MBM-XEM-002

Web GUI Guide

Revision 1.0

Super Micro Intelligent Switch

Release: **1.0**

Document status: Standard

Document release date: 8/30/2017

Contents

1 Introduction

1.1 Purpose

This document is designed to provide Supermicro Switch module MBM-XEM-002 users with the information required to configure the switch through the Web interface. The web pages have been presented as screenshots in this document to make the information more accessible.

1.2 Scope

This document explains in detail about all web pages and fields that are useful to configure the MBM-XEM-002 switch product.

1.3 Definitions and Acronyms

ACL	Access Control Lists
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common Internal Spanning Tree
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DLF	Destination Lookup Failure
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
IGMP	Internet Group Management Protocol
IGS	IGMP Snooping
IP	Internet Protocol
LA	Link Aggregation
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base

MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
PDU	Protocol Data Unit
QoS	Quality of Service
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLV	Type Length Value
TOS	Type Of Service
UDP	User Datagram Protocol
VLAN	Virtual LAN

2 Overview

MBM-XEM-002 can be configured through Web browsers like the Chrome, Firefox or Internet Explorer. For managing the switch through web browsers, type in the management IP address to start accessing the switch in browser address bar. For example, if the management IP address of the switch is 192.168.100.102, the switch can be accessed through the Web browser by typing **http://192.168.100.102** in the address bar of the web browser.

2.1 Management IP Address

MBM-XEM-002 comes with default DHCP settings for management IP address.

This default IP address can be changed to static in Management IP page in System Management section.

User can access switch management IP through CMM Ethernet connections. The internal management Ethernet ports of blade switches are connected with CMM Ethernet ports internally. Switch management IP is not reachable from the front panel of ports of switch module.

2.2 Login Page

Type in the switch IP address in the browser. The following **Login** page appears.

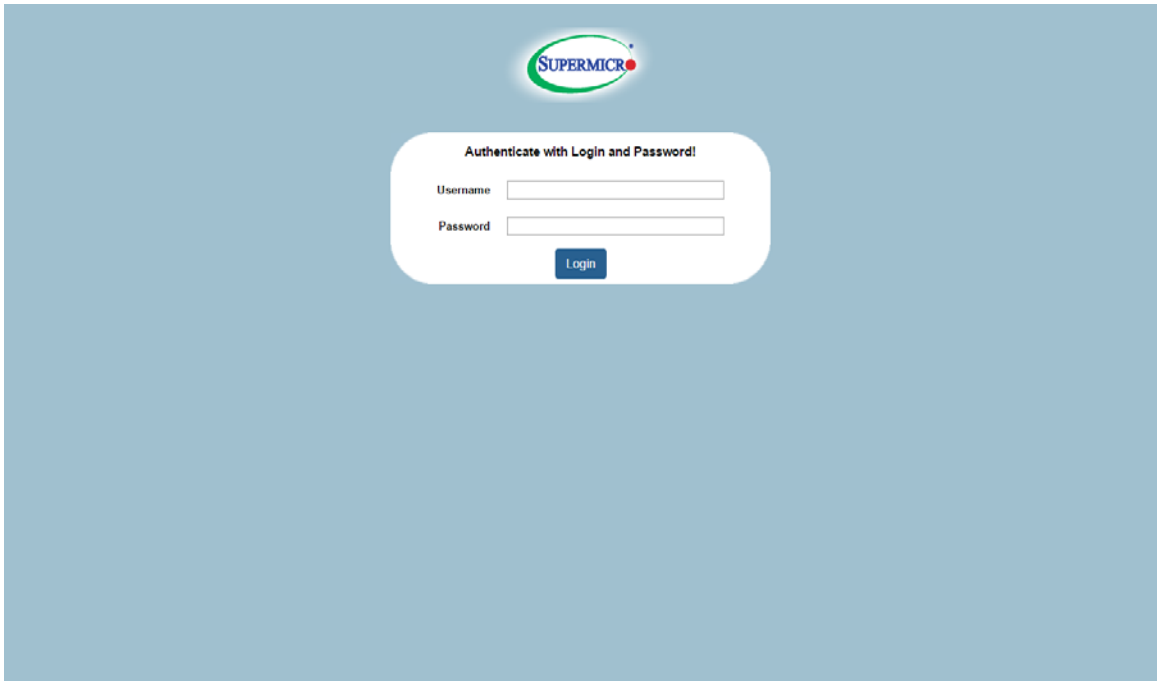
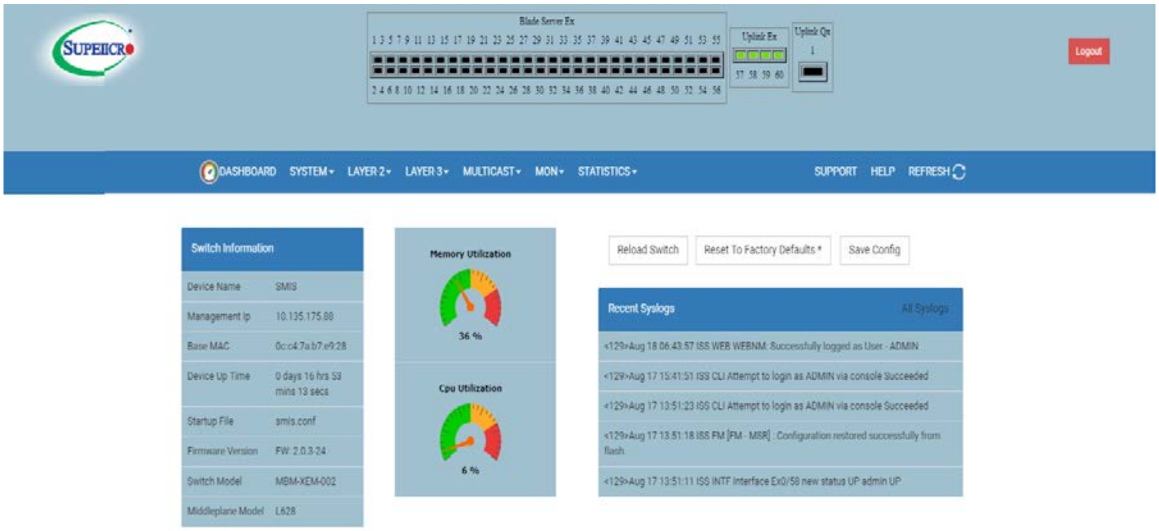


Fig: login page

Enter the **User Name** and **Password** and click the **Login** button. This **User Name** and **Password** are both used for accessing the Switch through the web for switch configuration. The user name and password entered are validated by Switch.

2.3 Home page

The Home page is displayed on successful validation of the user name and password. This page presents links to configurations of all the features of Switch. It has the following main components.



Switch Information	
Device Name	SMIS
Management Ip	10.135.175.88
Base MAC	0c:c4:7a:b7:e9:28
Device Up Time	0 days 16 hrs 53 mins 13 secs
Startup File	smis.conf
Firmware Version	FW: 2.0.3-24
Switch Model	MBM-XEM-002
Middleplane Model	L628

Recent Syslogs

```
<129>Aug 18 06:43:57 ISS WEB WEBNM: Successfully logged as User - ADMIN
<129>Aug 17 15:41:51 ISS CLI Attempt to login as ADMIN via console Succeeded
<129>Aug 17 13:51:23 ISS CLI Attempt to login as ADMIN via console Succeeded
<129>Aug 17 13:51:18 ISS FM [FM - MSR] : Configuration restored successfully from flash
<129>Aug 17 13:51:11 ISS INTF Interface Ex0/58 new status UP admin UP
```

Fig: Homepage

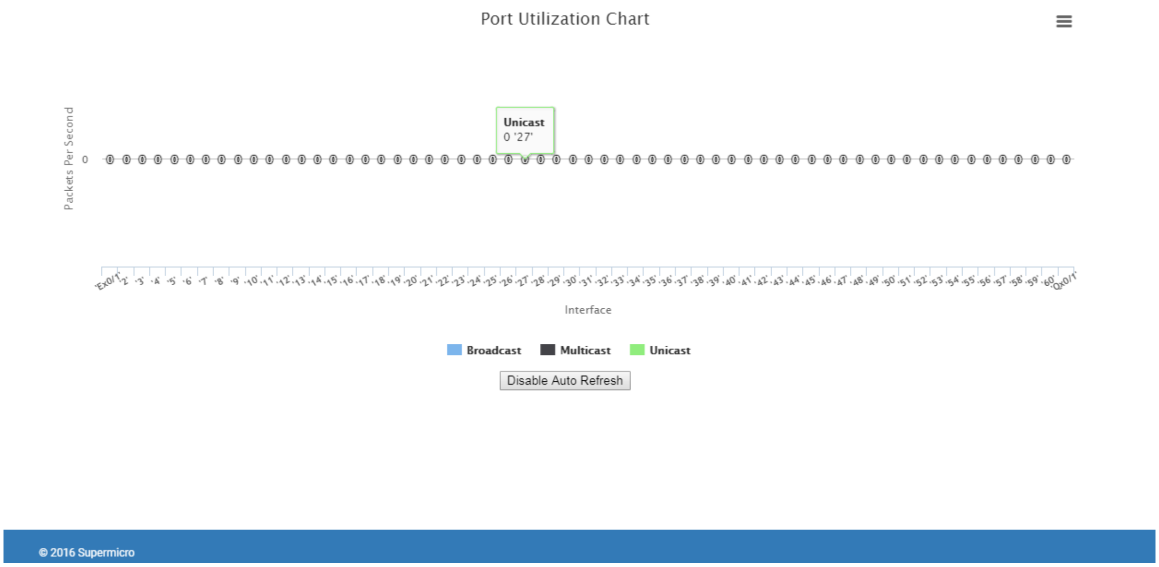

Port Utilization Chart
Unicast
0 '27'
Packets Per Second
0
Ex0/1' '2' '3' '4' '5' '6' '7' '8' '9' '10' '11' '12' '13' '14' '15' '16' '17' '18' '19' '20' '21' '22' '23' '24' '25' '26' '27' '28' '29' '30' '31' '32' '33' '34' '35' '36' '37' '38' '39' '40' '41' '42' '43' '44' '45' '46' '47' '48' '49' '50' '51' '52' '53' '54' '55' '56' '57' '58' '59' '60' 'Qx0/1'
Interface
Broadcast
Multicast
Unicast
Disable Auto Refresh
© 2016 Supermicro

Fig: Homepage Port Utilization

- Dashboard
- Page Top Links
- Top LED Display
- Menu - Configuration links for all sections

2.3.1 Dashboard

Dashboard page displays Switch information, Memory, Port and CPU utilization, System logs.

The **Switch Information** displays following details of Switch.

Device name - Displays the Switch name.

Management IP - Management IP Address of the Switch.

Switch Base MAC Address - The start address of MAC address block used in this switch.

Device Up Time - Displays the current duration of the Switch has been used.

Start Up file - Displays the name of the startup file while booting the switch.

Firmware Version - Displays the current version of firmware used in switch.

Switch model - Displays the model of the Switch.

Middleplane Model - Displays the model of the Middleplane inserted by the switch.

Memory Utilization - Displays the current usage of the memory used by the Switch in a gauge metre.

CPU Utilization - Displays the current usage the CPU used by the switch in a gauge metre.

Recent Syslogs - This table displays recent syslog messages from syslog buffers in memory.

Following buttons are used for quick configuration:

Reload Switch - Use this button to reload the switch.

Reset To Factory Defaults - This will set the switch to factory defaults. All stored configurations will be lost. Also all user names and passwords will be lost. Do necessary backups before resetting to factory defaults.

Write Startup Config - Use this button to write the configurations made in switch to the startup file.

Port Utilization - Displays the traffic rate of all the ports graphically. The chart displays Broadcast, Multicast and Unicast rates in packets/second. The displayed rate is the sum of the receive rate and transmit rate. It is refreshed every 10 seconds. User can disable refresh by using 'Disable Auto Refresh' button.

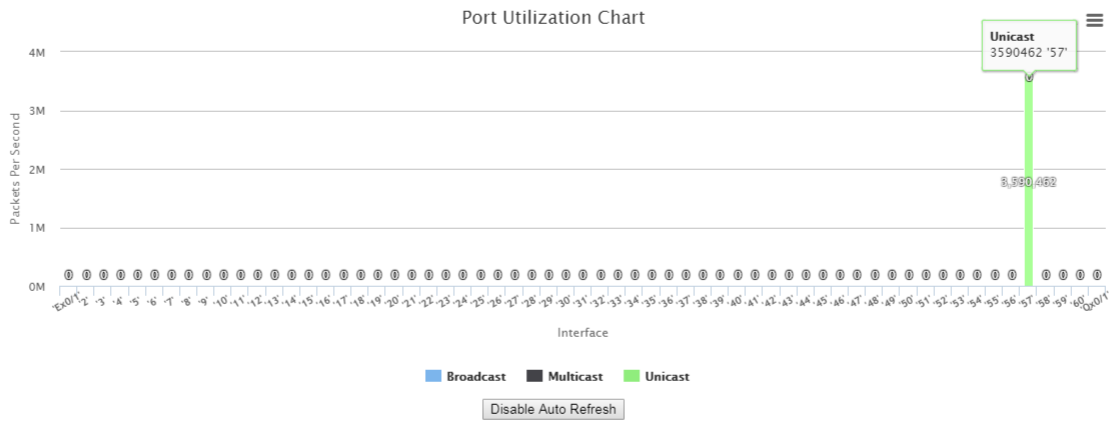


Fig : Port Utilization Chart

2.3.2 Page Top Links

This section provides the following links.

Refresh

Help

Support

Logout

Refresh link helps refreshing contents of the page. Unlike browser provided refresh button and refresh icon, these are refreshes only the contents of middle page which has active data.

Help link provides context specific help texts. This link opens a new help text page relevant to the configurations of current configuration page displayed.

Support link provides link to customer support help of Supermicro.

Logout link helps signing out of management web application. This link takes the user back to login screen requesting user name and password for login.

2.3.3 Top LED Display

This part of the screen displays the port status of Switch. It displays Speed and Link status for every port.

2.3.4 Menu

The menu displays the dropdown list to access configuration pages. This menu is organized based on the features supported in Switch. The main features are categorized in following groups.

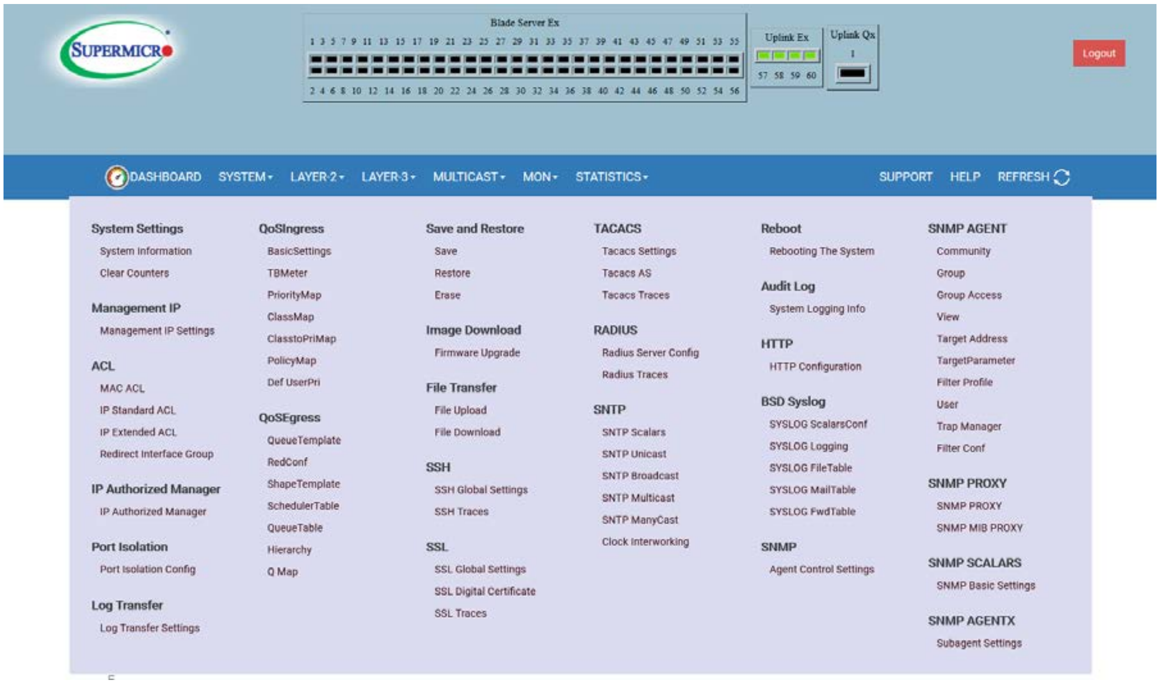


Fig: Menu List

- ❖ System Management – System based configurations
- ❖ Layer 2 Management – Layer 2 Protocols including VLAN, RSTP, MSTP, …
- ❖ Multicast Management – Multicast Protocols including IGMP Snooping and Dynamic Multicast.
- ❖ Statistics – Statistics and Counters for all the features.

This makes user to choose any configuration page directly without going back to home page every time.

3 System Management

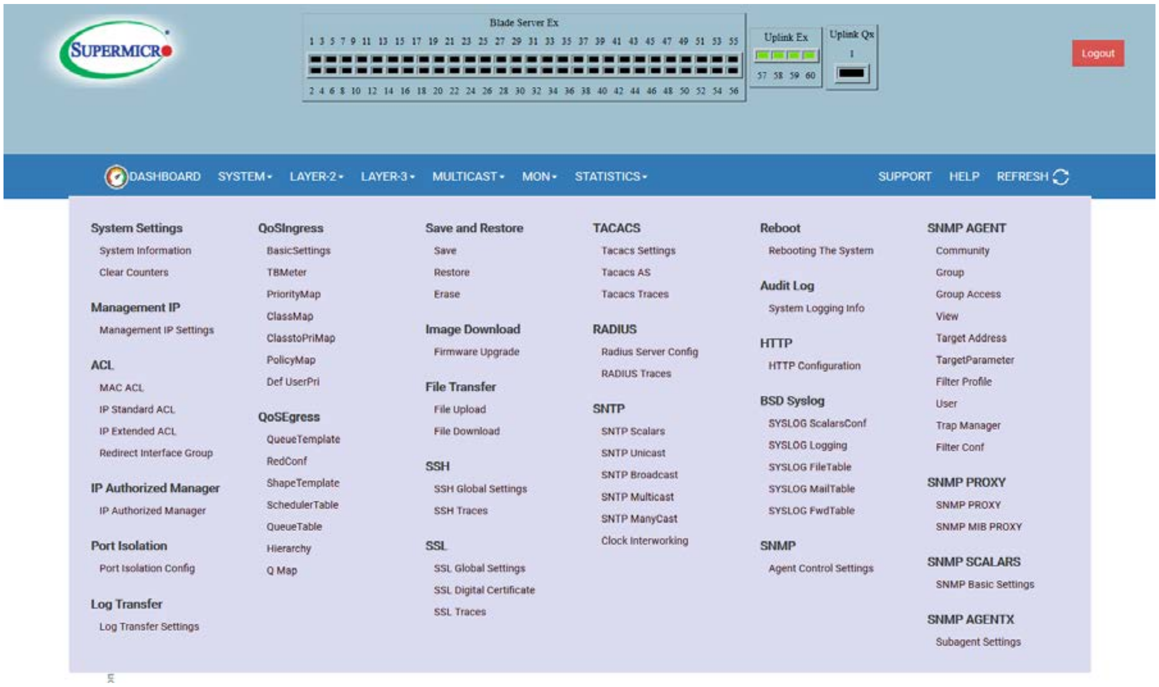


Fig: System Management

System Management covers the following features of Switch.

- System Settings
- Management IP
- ACL
- IP Authorized Manager
- Port Isolation
- Log Transfer
- QoSIngress
- QoSEgress
- Save and Restore
- Image Download
- File Transfer
- SSH
- SSL
- TACACS
- RADIUS
- SNTP

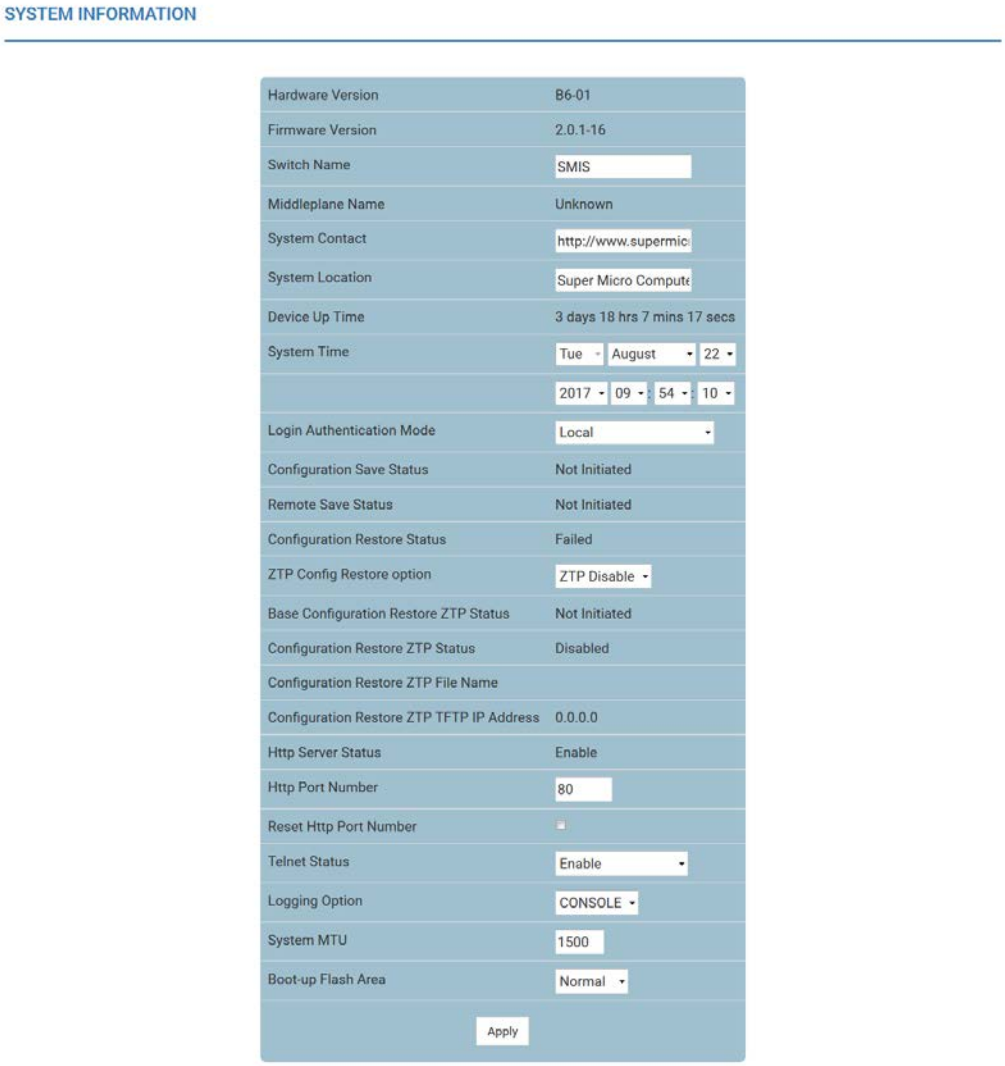
- Reboot
- Audit Log
- HTTP
- BSD Syslog
- SNMP
- SNMP AGENT
- SNMP PROXY
- SNMP SCALARS
- SNMP AGENTX

3.1 System Settings

The *System Settings* link allows you to configure the System Settings for switch. User can configure System Settings on the following two pages.

- System Information
- Clear Counters

3.1.1 System Information



SYSTEM INFORMATION

Hardware Version	B6-01
Firmware Version	2.0.1-16
Switch Name	SMIS
Middleplane Name	Unknown
System Contact	http://www.supermic
System Location	Super Micro Compute
Device Up Time	3 days 18 hrs 7 mins 17 secs
System Time	Tue August 22
	2017 09 : 54 : 10
Login Authentication Mode	Local
Configuration Save Status	Not Initiated
Remote Save Status	Not Initiated
Configuration Restore Status	Failed
ZTP Config Restore option	ZTP Disable
Base Configuration Restore ZTP Status	Not Initiated
Configuration Restore ZTP Status	Disabled
Configuration Restore ZTP File Name	
Configuration Restore ZTP TFTP IP Address	0.0.0.0
Http Server Status	Enable
Http Port Number	80
Reset Http Port Number	□
Telnet Status	Enable
Logging Option	CONSOLE
System MTU	1500
Boot-up Flash Area	Normal

Fig: System Information

The *System Information* link opens the **System Information** Page.

System Information page provides system related information and also helps configuration system specific parameters.

The table below lists the fields present in this page.

Hardware Version - Displays the hardware version number of the system.

Firmware Version - Displays the firmware version number of the system.

Switch Name - Enter the name of the device. The maximum length is 15.

Middleplane Name - Displays the middleplane name of the system.

System Contact - Enter the contact person details for this managed node. The maximum length is 50. If the contact information is not available, this value takes a zero-length string.

System Location - Enter the physical location of this node. The maximum length is 50. If the location is unknown, this value takes a zero-length string.

Device Up Time - Displays the time from which the device is up. The format is Days Hours, Minutes, Seconds. Example: 0 Days 1Hrs, 15Mins, 27 Secs

System Time - Select the current date and time. The format is Day Month Date Year Hours Minutes Seconds. Example: Fri May 07 2010 13: 40: 00

Login Authentication Mode - Select the login authentication mode. The list contains:

* Local - Sets locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.

* RADIUS - Sets the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

* Tacacs - Sets the TACACS server to be used as an authentication server. Communicates with the authentication server commonly used in networks.

* RADIUS fallback Local - The same with RADIUS, but fallback to Local authentication if the server fails.

* Tacacs fallback Local - The same with Tacacs, but fallback to Local authentication if the server fails.

Configuration Save Status - Displays the configuration save status. Once the configuration is done, the save status will be displayed as any of the following:

* Successful - System information is configured and saved successfully

* Failure - System information configuration save failed.

* Inprogress - System information configuration save is inprogress.

* Not Initiated - System information configuration save is not initiated.

Remote Save Status - Displays the remote save status. This status represents the status of save operation to the remote location as any of the following:

* Successful - Remote information is configured and saved successfully

* Failure - Remote information configuration save failed.

* Inprogress - Remote information configuration save is inprogress.

* Not Initiated - Remote information configuration save is not initiated.

Configuration Restore Status - Displays the configuration restoration status. The already configured parameter will be restored and the status will be displayed as any of the following

* Successful - Configuration is restored successfully.

* Failure - Configuration restoration failed.

* Inprogress - Configuration restoration is inprogress.

* Not Initiated - Configuration restoration is not initiated.

ZTP Config Restore option - Enable or disable ZTP (Zero Touch Provision) feature. ZTP is default to be disabled. If ZTP is enabled, the switch configuration will be coming from TFTP server. The switch configuration file name and tftp server IP address is provided by DHCP server option configuration. if ZTP is disabled, switch will use locally available configuration and ignore ZTP options in DHCP. The list contains:

* ZTP Enable - Get configuration from DHCP and TFTP server

* ZTP Disable - Use local configuration

Base Configuration Restore ZTP Status - Displays the ZTP base configuration restoration status. The base configuration is used for ZTP to access the network and the status will be displayed as any of the following:

* Successful - Base Configuration is restored successfully.

* Failed - Base Configuration restoration failed.

* In Progress - Base Configuration restoration is in progress.

* Not Initiated - Base Configuration restoration is not initiated.

Configuration Restore ZTP Status - Displays the ZTP configuration restoration status. The status will be displayed as any of the following:

* Disabled - ZTP is disabled

* Disabled : need DHCP - ZTP is enabled, but DHCP client feature is not enabled

* Disabled : need config restore - ZTP is enabled, but config restore feature is not enabled

* Disabled : Unknown - ZTP is enabled, but can not proceed for unknown reason

* Fallback - Download Failed - ZTP fallback to local configuration because download failed

* Fallback - Timeout or no option - ZTP fallback to local configuration because no needed DHCP options

* Successful - ZTP Configuration is restored successfully

* Downloading - ZTP Configuration is downloading

* Waiting - ZTP is waiting for needed DHCP options

Configuration Restore ZTP File Name - The name of the configuration file received from ZTP options (DHCP option 43 sub option 01) in DHCP ACK message.

Configuration Restore ZTP TFTP IP Address - The IP address of the TFTP server from which the ZTP provided configuration file need to be downloaded. This information is received in DHCP ACK message in option 66.

Http Server Status - Displays the status of the HTTP server as either enable or disable. By default the server is enabled.

Http Port Number - Displays the port to be used by the host to configure the router using the Web interface. This value ranges between 1 and 65535. Default value is 80.

> Once the port number is changed, the Http Server Statusis disabled and enabled. You should open the HTTP session with IP address and new port number. For example, you should enter as 12.0.0.1:100, where 12.0.0.1 represents the IP of the switch and 100 represents the port number.

Reset Http Port Number - Click the check box to reset the configured Http Port Status whose default value is 80. When this check box is enabled, the Http Port Status value is reset to the default value.

> Once the port number is set to default value, the Http Server Status is disabled and enabled. You should open the HTTP session with the IP address alone. For example, you should enter as 12.0.0.1, where 12.0.0.1 represents the IP of the switch.

Telnet Status - Select to set the status of TELNET in the system. The list contains the following;

* Enable - Sets the Telnet status as enabled.

* Disable - Sets the Telnet status as disabled.

* enableInProgress - Sets the Telnet status as enableInProgress.

* disableInProgress - Sets the Telnet status as disableInProgress.

Set operation of enable will move this object to the enableInProgress first then to the enable on successfull transition. Otherwise it will move back to the old state.

> enableInProgress and disableInProgress are not admin configurable values

The default value of Telnet Status is enabled.

Logging Option - Select the path to log the debug details, The list contains:

* Console - Logs the debug details in a console

* File - Logs the debug details in memory (system buffer)

* Flash - Logs the debug details in a file (flash)

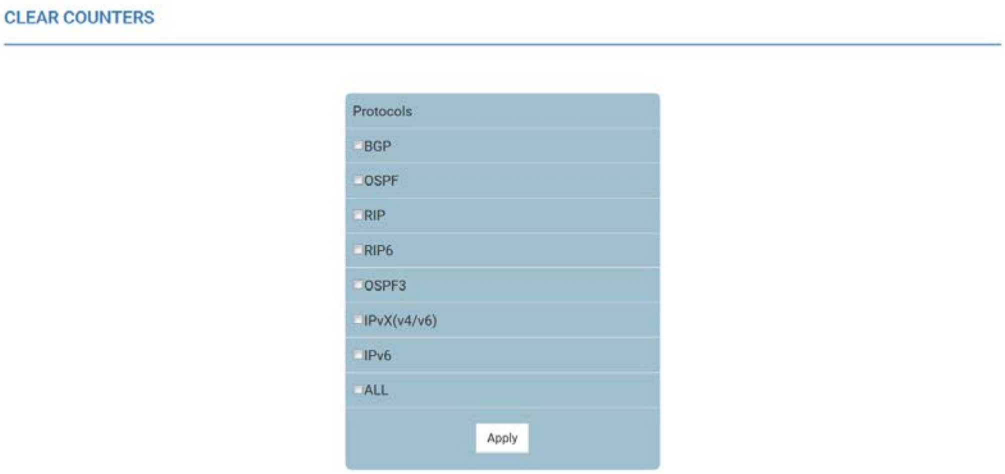
System MTU - Enter the MTU of the system. The interfaces will be brought to down for MTU update.

Boot-up Flash Area - Select boot up flash area. The list contains:

* Normal - boot up flash area on normal

* Fallback - boot up flash area on fallback.

3.1.2 Clear Counters



CLEAR COUNTERS

Protocols

□ BGP

□ OSPF

□ RIP

□ RIP6

□ OSPF3

□ IPvX(v4/v6)

□ IPv6

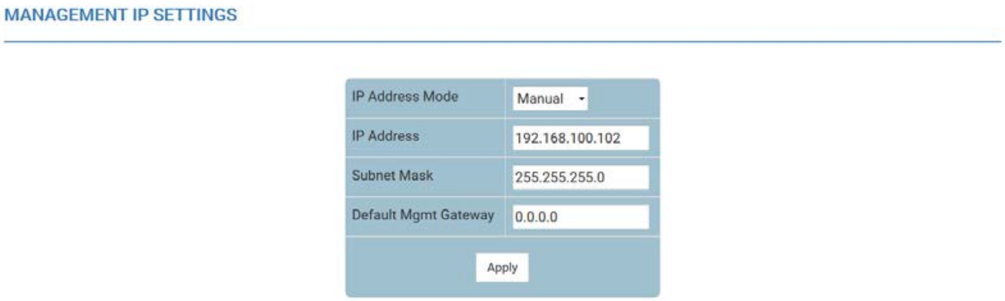
□ ALL

Fig: Clear Counters

The *Clear Counters* link opens the **Clear Counters** Page.
Clear Counters page allows the user to clear the counters.

The table below lists the fields present in this page.
BGP - Clear the BGP counters.
OSPF - Clear the OSPF counters.
RIP - Clear the RIP counters.
RIP6 - Clear the RIP6 counters.
OSPF3 - Clear the OSPF3 counters.
IPvX(v4/v6) - Clear the IPvX(v4/v6) counters.
IPv6 - Clear the IPv6 counters.
ALL - Clear ALL of the above counters

3.2 Management IP



MANAGEMENT IP SETTINGS

IP Address Mode	Manual
IP Address	192.168.100.102
Subnet Mask	255.255.255.0
Default Mgmt Gateway	0.0.0.0

Fig: Management IP settings

The *Management IP* link opens the **Management IP settings** Page.

The Management IP Settings page allows user to configure switch Management IP address details.

The default static management IP address for Supermicro Switch product is 192.168.100.102.

The table below lists the fields present in this page.

IP address mode - This can be either manual or dynamic. If manual mode is selected, then the management interface takes the configured IP address as Default IP Address. If dynamic mode is selected, the management interface gets the IP address through DHCP.

IP address - Configures the management IP address. This is configurable only if IP Address Mode is manual

Subnet Mask - Configures the management IP subnet mask. This is configurable only if IP Address Mode is manual

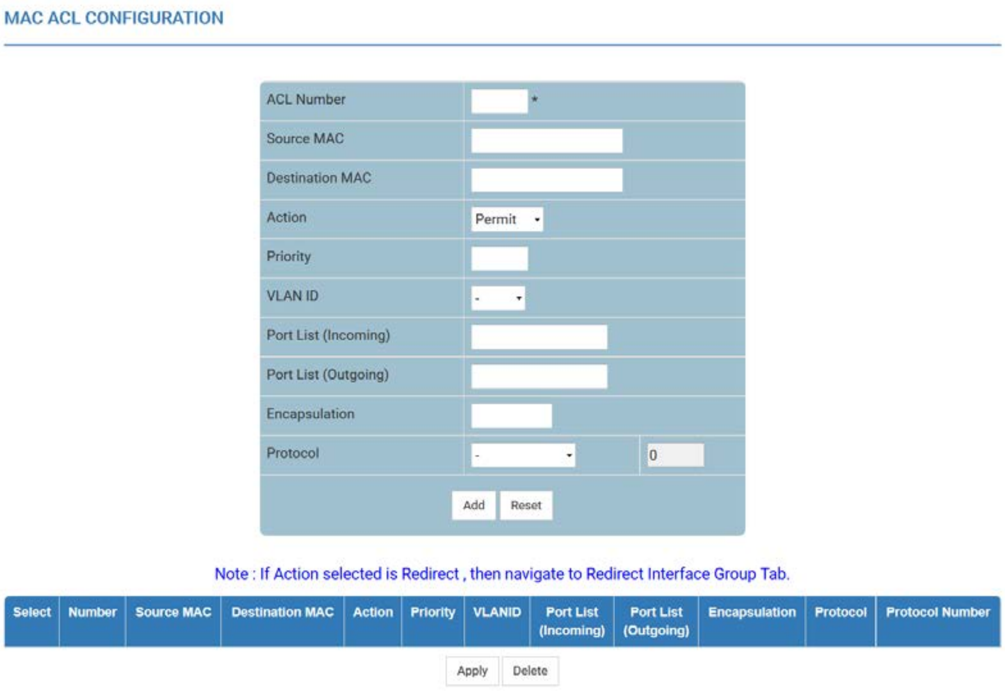
Default Mgmt Gateway - Configures the default gateway IP address in blade switches.

3.3 ACL

The *ACL* link allows you to configure the Access Control List for switch. User can configure ACL on the following four pages.

- ❖ MAC ACL
- ❖ IP Standard ACL
- ❖ IP Extended ACL
- ❖ Redirect Interface Group

3.3.1 MAC ACL



MAC ACL CONFIGURATION

ACL Number	*	
Source MAC		
Destination MAC		
Action	Permit	
Priority		
VLAN ID	-	
Port List (Incoming)		
Port List (Outgoing)		
Encapsulation		
Protocol	-	0

Note : If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Select	Number	Source MAC	Destination MAC	Action	Priority	VLANID	Port List (Incoming)	Port List (Outgoing)	Encapsulation	Protocol	Protocol Number

Fig: MAC ACL Configuration

The *MAC ACL* link opens the **MAC ACL Configuration** Page.

The MAC ACL Configuration page allows the user to configure the MAC(Media Access Control) access list.

The table below lists the fields present in this page.

ACL Number - Specifies the unique identifier for the access list. This value ranges between 1 and 65535.

Source MAC - Specifies the source MAC Address for which the access list must be applied.

Destination MAC - Specifies the destination MAC Address for which the access list must be applied.

> For making the status of the access list to be Active, both the source and destination MAC addresses must be configured.

Action - Specifies the action to be taken for the access list. Options are:

* Permit - Packet is forwarded according to the forwarding rules.

* Deny - Packet is discarded.

* Redirect - Packet is redirect according to the forwarding rules.

By default, Permit is selected.

If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Priority- Specifies the priority for the access list. This value ranges between 1 and 255. Default value is 1.

VLAN ID - Specifies the VLAN ID (Identifier) for which the access list has to be applied. This value ranges between 0 and 4094. Default value is 0.

Port List (Incoming) - Specifies the incomming port list for which the access list has to be applied.

Port List (Outgoing) - Specifies the outgoing port for which the access list has to be applied.

Encapsulation - Specifies the encapsulation type of the packet for which the access list has to be applied. This value ranges between 1 and 65535.

Protocol - Specifies the non-IP protocol type of the packet for which the access list has to be applied. Options are:

* aarp - Ethertype AppleTalk Address Resolution Protocol that maps a data-link
address to a network address

* amber - EtherType DEC-Amber

* dec-spanning - EtherType Digital Equipment Corporation (DEC) spanning tree

* decnet_iv - EtherType DECnet Phase IV protocol

* diagnostic - EtherType DEC-Diagnostic

* dsm - EtherType DEC-DSM/DDP

* etype-6000 - EtherType 0x6000

* etype-8042 - EtherType 0x8042

* lat - EtherType DEC-LAT

* lavc-sca - EtherType DEC-LAVC-SCA

* mop-consol - EtherType DEC-MOP Remote Console

* mop_dump - EtherType DEC-MOP Dump

* msdos - EtherType DEC-MSDOS

* mumps - EtherType DEC-MUMPS

* netbios - EtherType DEC- Network Basic Input/Output System (NETBIOS)

* vines-echo - EtherType Virtual Integrated Network Service (VINES) Echo from
Banyan Systems

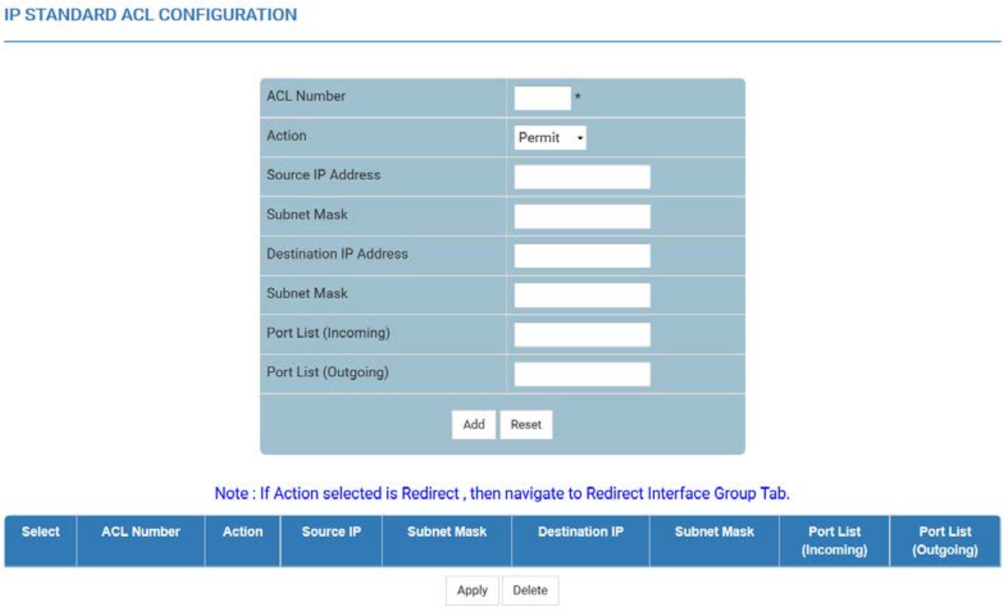
* vines-ip - EtherType VINES IP

* xns-id - EtherType Xerox Network Systems (XNS) protocol suite

* other

Protocol Number - Specifies the protocol number. This value ranges between 1 and 65535.

3.3.2 IP Standard ACL



IP STANDARD ACL CONFIGURATION

ACL Number	*
Action	Permit
Source IP Address	
Subnet Mask	
Destination IP Address	
Subnet Mask	
Port List (Incoming)	
Port List (Outgoing)	

Note : If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Select	ACL Number	Action	Source IP	Subnet Mask	Destination IP	Subnet Mask	Port List (Incoming)	Port List (Outgoing)

Fig: IP Standard ACL Configuration

The *IP Standard ACL link* opens the **IP Standard ACL Configuration** Page.

The IP Standard ACL Configuration page allows the user to configure the standard IP access lists.

The table below lists the fields present in this page.

ACL Number - Specifies the unique ID for the access list. This value ranges between 1 and 1000.

Action - Specifies whether the packets must be allowed or dropped when a match has been found. Options are:

* Permit - Allows the packets when a match has been found.

* Deny - Drops the packets when a match has been found.

* Redirect - Redirects the packets when a match has been found.

By default, Permit is selected.

If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Source IP Address - Specifies the source MAC Address for which the access list must be applied.

Destination IP Address - Specifies the destination MAC Address for which the access list must be applied.

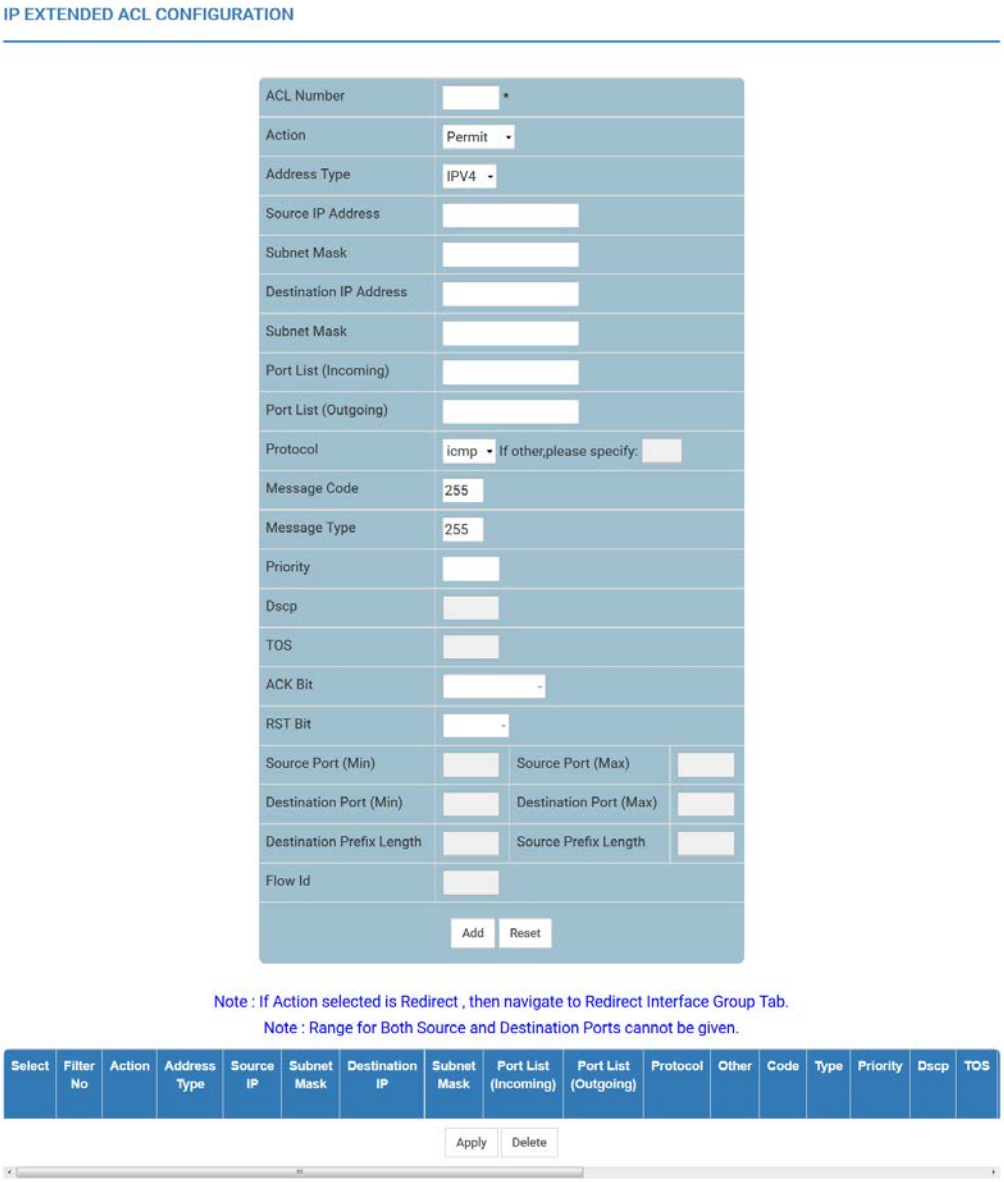
> For making the access list to be Active, both the source and destination MAC addresses must be configured.

Subnet Mask - Specifies the source and destination address mask corresponding to the IP Address.

Ports List (Incoming) - Specifies the incoming port list for which the access lists has to be applied.

Ports List (Outgoing) - Specifies the outgoing port for which the access lists has to be applied.

3.3.3IP Extended ACL



IP EXTENDED ACL CONFIGURATION

ACL Number	*		
Action	Permit		
Address Type	IPV4		
Source IP Address			
Subnet Mask			
Destination IP Address			
Subnet Mask			
Port List (Incoming)			
Port List (Outgoing)			
Protocol	icmp If other,please specify:		
Message Code	255		
Message Type	255		
Priority			
Dscp			
TOS			
ACK Bit			
RST Bit			
Source Port (Min)		Source Port (Max)	
Destination Port (Min)		Destination Port (Max)	
Destination Prefix Length		Source Prefix Length	
Flow Id			

Note : If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Note : Range for Both Source and Destination Ports cannot be given.

Select	Filter No	Action	Address Type	Source IP	Subnet Mask	Destination IP	Subnet Mask	Port List (Incoming)	Port List (Outgoing)	Protocol	Other	Code	Type	Priority	Dscp	TOS

Fig: IP Extended ACL Configuration

The *IP Extended ACL* link opens the **IP Extended ACL Configuration** Page.

The IP Extended ACL Configuration page allows the user to configure the extended IP access lists.

The table below lists the fields present in this page.

ACL Number - Specifies the unique ID for the access list. This value ranges between 1001 and 65535.

Action - Specifies whether the packets must be allowed or dropped when a match has been found. Options are:

* Permit - Allows the packets when a match has been found.

* Deny - Drops the packets when a match has been found.

* Redirect - Redirects the packets when a match has been found.

By default, Permit is selected.

If Action selected is Redirect , then navigate to Redirect Interface Group Tab.

Address Type - Specifies the type of IP address used by the entry. Options are:

* IPV4 - The entry uses the IPv4 addresses.

* IPV6 - The entry uses the IPv6 addresses.

Source IP Address - Specifies the IP Address for which the access list must be applied.

Subnet Mask - Specifies the address mask corresponding to the IP Address.

Destination IP Address - Specifies the IP Address for which the access list must be applied.

Ports List (Incoming) - Specifies the incoming port list for which the filter has to be applied.

Ports List (Outgoing) - Specifies the outgoing port for which the filter has to be applied.

Protocol - Specifies the type of protocol. Options are:

* icmp - Internet Control Message Protocol

* ip - Internet Protocol

* tcp - Transmission Control Protocol

* udp - User Datagram Protocol

* ospf - Open Shortest Path First

* pim - Protocol Independent Multicasting

* other - Any other protocol

By default, icmp is selected.

Other - Specifies the user defined protocol value.

Message Code - Specifies the message code to be checked for ICMP (Internet Control Message Protocol) Packets. This value ranges between 0 and 255. Default value is 255.

> Will be enabled, only if ICMP is chosen as the protocol.

Message Type - Specifies the message type to be checked for ICMP Packets. This value ranges between 0 and 255. Default value is 255.

> Will be enabled, only if ICMP is chosen as the protocol.

Priority- Specifies the priority for the filter. This value ranges between 1 and 255.

Dscp - Specifies the DSCP (Differentiated Services Code Point) value. This value ranges between 0 and 63.

TOS - Specifies the type of service for the access list. This value ranges between 0 and 7.

ACK Bit - Indicates the TCP Ack Bit to be checked against the incoming packet. Options are:

* Establish

* Not Establish

* Any

> Will be enabled, only if TCP is chosen as the protocol.

RST Bit - Indicates the TCP Reset Bit to be checked against the incoming packet. Options are:

* Set

* Not Set

* Any

> Will be enabled, only if TCP is chosen as the protocol.

Source Port (Min) - Specifies the TCP/UDP (User Datagram Protocol) source port from which the access list has to be applied. This value ranges between 0 and 65535.

Source Port (Max) - Specifies the TCP/UDP source ports to which the access list has to be applied. This value ranges between 0 and 65535.

Destination Port (Min) - Specifies the TCP/UDP destination port from which the access list has to be applied. This value ranges between 0 and 65535.

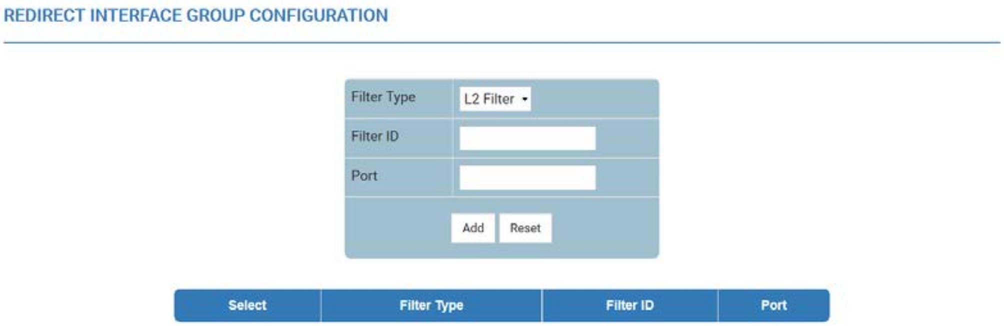
Destination Port (Max) - Specifies the TCP/UDP destination port to which the access list has to be applied. This value ranges between 0 and 65535.

Destination Prefix Length - Specifies the length of the CIDR (Classless Inter Domain Routing) prefix carried in the destination IP address.

Source Prefix Length - Specifies the length of the CIDR prefix carried in the source IP address.

Flow Id - Specifies the flow identifier in an IPv6 header. This value ranges between 0 and 1048575.

3.3.4 Redirect Interface Group



REDIRECT INTERFACE GROUP CONFIGURATION

Filter Type	L2 Filter
Filter ID	
Port	

Select	Filter Type	Filter ID	Port

Fig: Redirect Interface Group Configuration

The *Redirect Interface Group* link opens the **Redirect Interface Group Configuration** Page. This page allows the user to configure the details of Redirect Interface Group.

The table below lists the fields present in this page.

Filter Type - Select the filter type. By default this field is set as L2 Filter. The list contains

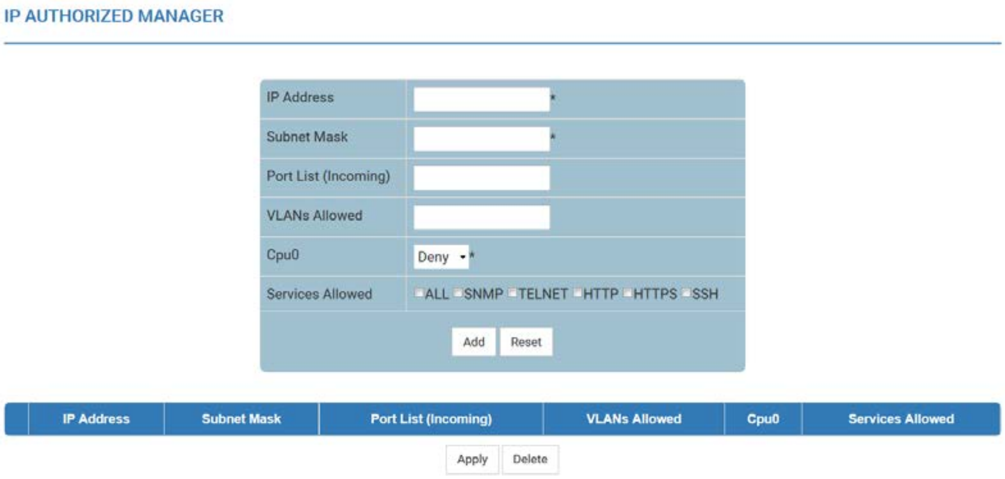
* L2 Filter - Configures L2 filter rules in the system

* L3 Filter - Configures L3 filter rules in the system

Filter ID - Enter the unique filter identifier.

Port - Enter the single port for which the access control has to be applied.

3.4 IP Authorized Manager



IP AUTHORIZED MANAGER

IP Address	*
Subnet Mask	*
Port List (Incoming)	
VLANs Allowed	
Cpu0	Deny *
Services Allowed	□ALL □SNMP □TELNET □HTTP □HTTPS □SSH

IP Address	Subnet Mask	Port List (Incoming)	VLANs Allowed	Cpu0	Services Allowed

Fig: IP authorized Manager

The *IP authorized Manager* link opens the **IP authorized Manager** Page.

This page allows the user to configure the IP authorized manager.

The table below lists the fields present in this page.

IP Address - Enter the Network or Host address from which the switch can be managed.

The maximum length of address is 15

An address 0.0.0.0 indicates Any Manager.

Subnet Mask - Enter the subnet mask for the configured IP address.

The maximum length of subnet mask is 15

> The configured subnet mask should be in the same subnet of the network in which the switch is placed.

Value 0.0.0.0 indicates mask for Any Manager.

Port List (Incoming) - Enter the port numbers through which the manager can access the switch.

> By default, the authorized manager is allowed to access the switch through all the ports. If a set of ports are configured in the Port List, the manager can access the switch only through the configured ports.

VLANs Allowed - Enter the VLANs in which the IP authorized manager can reside.

> By default, the manager is allowed to reside in any VLAN. If a set of VLANs are configured in the VLANs Allowed list, the manager can reside only in the configured VLAN set. Access to the switch will be denied from any other VLAN.

Cpu0 - Select access rights for the manager for the switch through OOB Port.

By default, Cpu0 is set as Deny. The list contains:

* Deny - Denies the OOB Interface access to the switch through the manager.

* Allow - Allows the OOB Interface access to the switch through the manager.

Services Allowed - Click the allowed services through which the manager can access the switch.

By default, the option ALL is selected. Options are:

* ALL - Supports all the services

* SNMP - SNMP (Simple Network Management Protocol),is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters

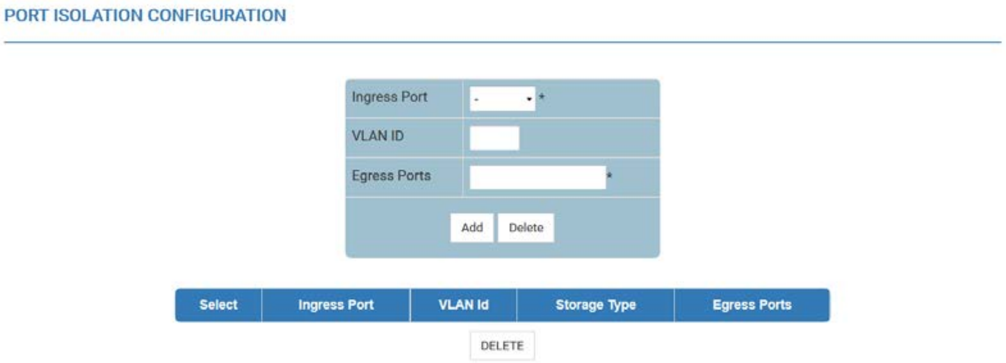
* TELNET - Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, the user can log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

* HTTP - HTTP (HyperText Transfer Protocol),is an underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page

* HTTPS - Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). S-HTTP is designed to transmit individual messages in a secured manner.

* SSH - Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

3.5 Port Isolation



Select	Ingress Port	VLAN Id	Storage Type	Egress Ports

Fig: Port Isolation Configuration

The *Port Isolation Config* link opens the **Port Isolation Configuration** Page.

This page allows the user to configure the list of allowed forwarding / egress ports, where the ingress packets for particular VLAN can be forwarded.

The table below lists the fields present in this page.

Ingress Port - Select the ingress port that should be mapped with the egress port. This is a combination of interface type and interface ID. The interface ID represents the port channel ID or is a combination of slot number and the port number (slot number/port number).

> This list contains only the available physical and link aggregated ports.

VLAN ID - Enter the VLAN ID that uniquely identifies a specific VLAN. The port isolation rule is applied only for the specified VLAN packets received on the configured ingress ports.

This value ranges between 1 and 4094.

Egress Ports - Enter the egress port or set of egress ports that should be mapped with the ingress port. Use comma as a separator between the ports while configuring a list of ports.

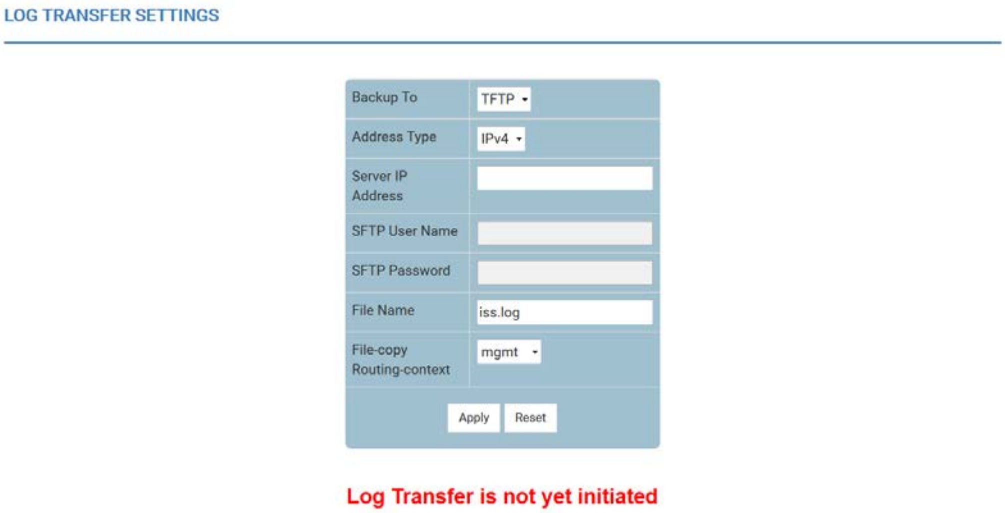
The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and 1 is port number)

3.6 Log Transfer



LOG TRANSFER SETTINGS

Backup To	TFTP
Address Type	IPv4
Server IP Address	
SFTP User Name	
SFTP Password	
File Name	iss.log
File-copy Routing-context	mgmt

Log Transfer is not yet initiated

Fig: Log Transfer Settings

The *Log Transfer Settings* link opens the **Log Transfer Settings** Page.
This page allows the user to configure log transfer parameters.

The table below lists the fields present in this page.

Backup To - Select the transfer mode for uploading log file to the remote system.
The default value is TFTP. The list contains:
* TFTP - Uploads the log file in TFTP (Trivial File Transfer Protocol) mode. It is used to transfer small amounts of data between hosts on a network.Any transfer begins with a request to read or write a file, which also serves to request a connection.
* SFTP - Uploads the log file in SFTP (SSH File Transfer Protocol) mode. It is a network protocol designed to provide secure file transfer and manipulation facilities over SSH.

Address Type - Select the address type.
By default, the Address type is set as IPv4. The list contains:
* IPv4 - Sets the Address type as IPv4.
* IPv6 - Sets the Address type as IPv6.

Server IP Address - Enter the IP address of the machine to which the log file is to be uploaded.

SFTP User Name - Enter the user name required for uploading log file in SFTP mode. This field is a string with size varying between 1 and 20.
> This field is disabled if the Transfer Mode is selected as TFTP.

SFTP Password - Enter the password for uploading log file in SFTP mode. This field is a string with size varying between 1 and 20.

> This field is disabled if the Transfer Mode is selected as TFTP.

File Name - Enter the file name in which the logs are saved in the remote system.

File-copy Routing-context - Select routing context for copy operation.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports.

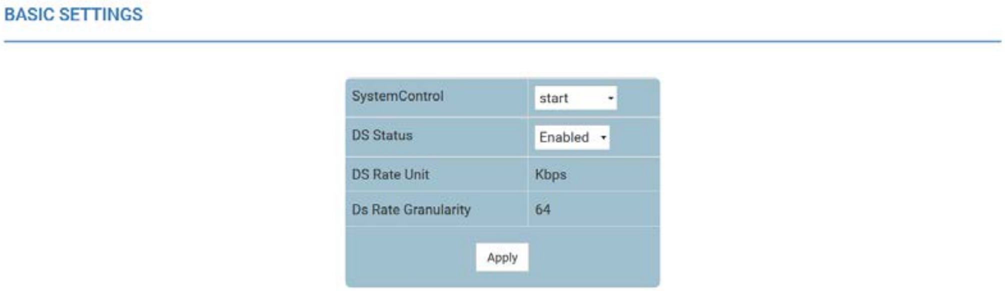
* mgmt - use the "mgmt VRF table for switch OOB port.

3.7 QoSIngress

The *QoSIngress* link allows you to configure the QoS Ingress settings for switch. User can configure QoSIngress on the following seven pages.

- BasicSettings
- TBMeter
- PriorityMap
- ClassMap
- ClasstoPriMap
- PolicyMap
- Def UserPri

3.7.1 Basic Settings



BASIC SETTINGS

SystemControl	start
DS Status	Enabled
DS Rate Unit	Kbps
Ds Rate Granularity	64

Fig: Basic Settings

The *BasicSettings* link opens the **Basic Settings** Page.

The page allows the user to configure the basic settings of QoS.

The table below lists the fields present in this page.

System Control - Select the status of the QoS module in the system.

By default System Control is set as start. The list contains:

* start - Resources required by QoS module are allocated and the QoS module starts running.

* shutdown - All the pools used by QoS module are released to the system.

DS Status - Select the status of the QoS module in the system.

By default, DS Status is set as Enabled. The list contains:

* Enabled - QoS module programs the hardware and starts protocol operation.

* Disabled - Stops protocol operation by deleting the hardware configuration.

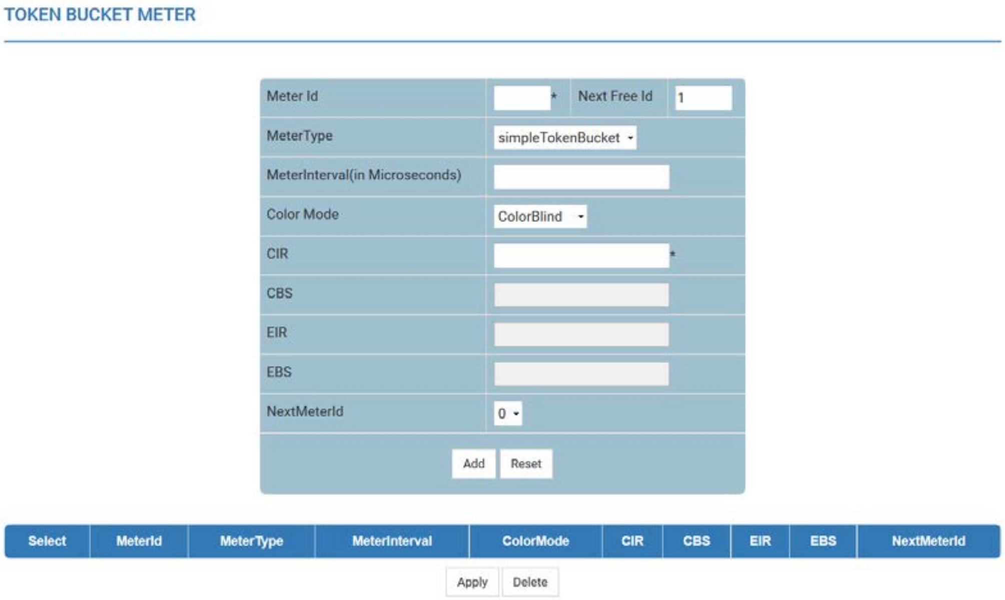
DS Rate Unit - Displays the unit for the information rate values based on target platform.

* Kbps - Kilobits per second.

Ds Rate Granularity - Displays the acceptable granularity level for configuring the information rate (CIR, EIR, PIR, PTR and CTR) values for a target platform.

By default Ds Rate Granularity value is set as 64.

3.7.2 TBMeter



TOKEN BUCKET METER

Meter Id	*	Next Free Id	1
MeterType	simpleTokenBucket		
MeterInterval(in Microseconds)			
Color Mode	ColorBlind		
CIR	*		
CBS			
EIR			
EBS			
NextMeterId	0		

Select	MeterId	MeterType	MeterInterval	ColorMode	CIR	CBS	EIR	EBS	NextMeterId

Fig: Token Bucket Meter

The *TBMeter* link opens the **Token Bucket Meter** Page.

The Token Bucket Meter page allows the user to configure the token bucket parameters.

The table below lists the fields present in this page.

Meter Id - Specifies the index that enumerates the token bucket parameter entries. This value ranges between 1 and 65535.

Next Free Id - Specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field.

MeterType - Specifies the metering algorithm associated with the token bucket parameters. Options are:

* simpleTokenBucket - Token Bucket Meter.

* avgRate - Average Rate Meter.

* srTCM - Single Rate Three Color Marker Metering as defined by RFC 2697.

* trTCM - Two Rate Three Color Marker Metering as defined by RFC 2698.

* tswTCM - Time Sliding Window Three Color Marker Metering as defined by RFC 2859.

* mefDecoupleMeter - Dual bucket meter as defined by RFC 4115.

* mefCoupledMeter - Dual bucket meter as defined by RFC 2697 and MEF coupling Flag.

> Note there are rules for different meter type:

- Interval and CIR Should not be NULL for Simple Token Bucket Meter

- Interval and CIR Should not be NULL for Avg Rate Meter

- CIR, CBS and EBS Should not be NULL for Single Rate Three Color Meter (srTCM)

- CIR, CBS, EIR and EBS Should not be NULL for Two Rate Three Color Meter (trTCM)

- CIR, EIR and Interval Should not be NULL for Time Sliding Window Three Colour Marker (tswTCM)

MeterInterval(in Microseconds) - Specifies the time interval used with the token bucket. This value ranges between 1 and 10000.

Color Mode - Specifies the color mode. Options are:

* ColorBlind

* ColorAware

Default color mode is ColorBlind.

CIR - Specifies the committed information rate as per MEF (Metro Ethernet Forum). This value ranges between 0 and 65535.

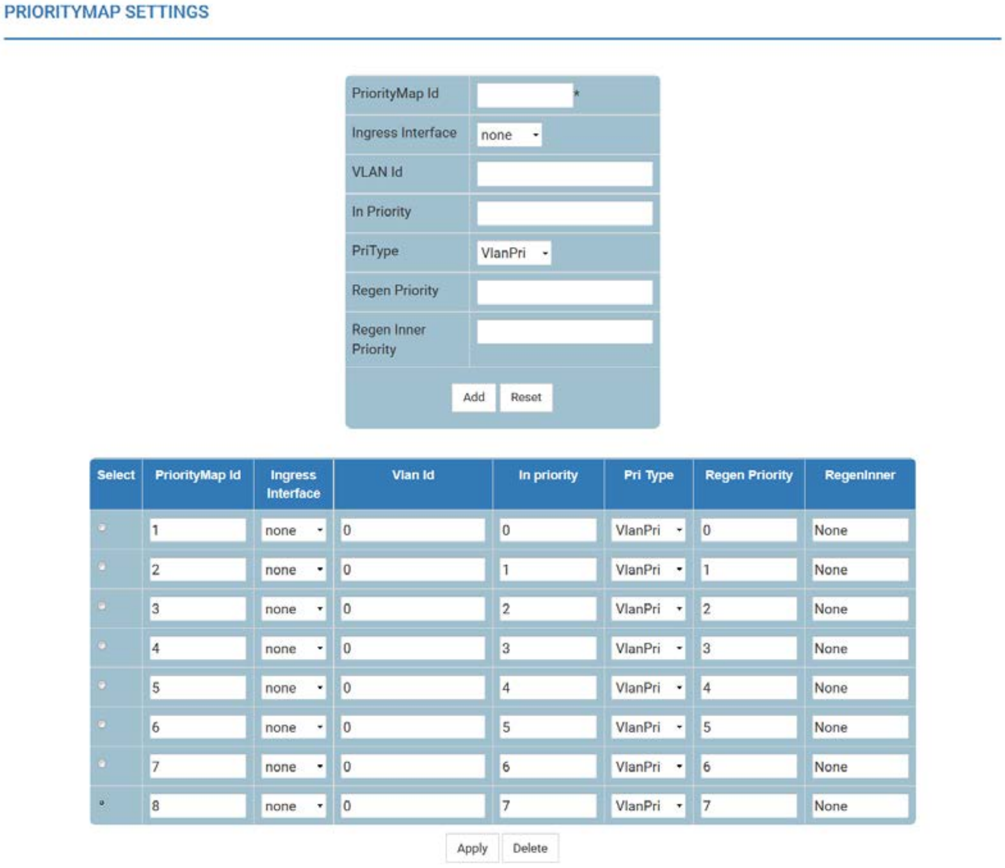
CBS - Specifies the committed burst size as per MEF. This value ranges between 0 and 65535.

EIR - Specifies the excess information rate as per MEF. This value ranges between 0 and 65535.

EBS - Specifies the excess burst size as per MEF. This value ranges between 0 and 65535.

NextMeterId - Specifies the meter entry ID to be used for applying the second/next level of conformance on the incoming packet.

3.7.3 PriorityMap



PRIORITYMAP SETTINGS

PriorityMap Id	*
Ingress Interface	none
VLAN Id	
In Priority	
PriType	VlanPri
Regen Priority	
Regen Inner Priority	

Select	PriorityMap Id	Ingress Interface	Vlan Id	In priority	Pri Type	Regen Priority	RegenInner
○	1	none	0	0	VlanPri	0	None
○	2	none	0	1	VlanPri	1	None
○	3	none	0	2	VlanPri	2	None
○	4	none	0	3	VlanPri	3	None
○	5	none	0	4	VlanPri	4	None
○	6	none	0	5	VlanPri	5	None
○	7	none	0	6	VlanPri	6	None
●	8	none	0	7	VlanPri	7	None

Fig: Prioritymap Settings

The *PriorityMap* link opens the **Prioritymap Settings** Page.

The Prioritymap Settings page allows the user to configure the priority map settings.

The table below lists the fields present in this page.

PriorityMap Id - Specifies a unique ID for priority map. This value ranges between 1 and 65535.

Ingress Interface - Specifies the incoming port number:

VLAN Id - Specifies the VLAN identifier for priority regeneration. The default value is 0.

In Priority - Specifies the incoming priority value determined for the received frame. This value ranges between 0 and 63.

> Note there are rules for different priority types:

- For PriType VlanPri, range should be Min 0 - Max 7
- For PriType IpTos, range should be Min 0 - Max 7
- For PriType IpDscp, range should be Min 0 - Max 63
- For PriType MplsExp, range should be Min 0 - Max 7

PriType - Specifies the incoming priority type. Options are:

* VlanPri

* IpTos

* IpDscp

* MplsExp

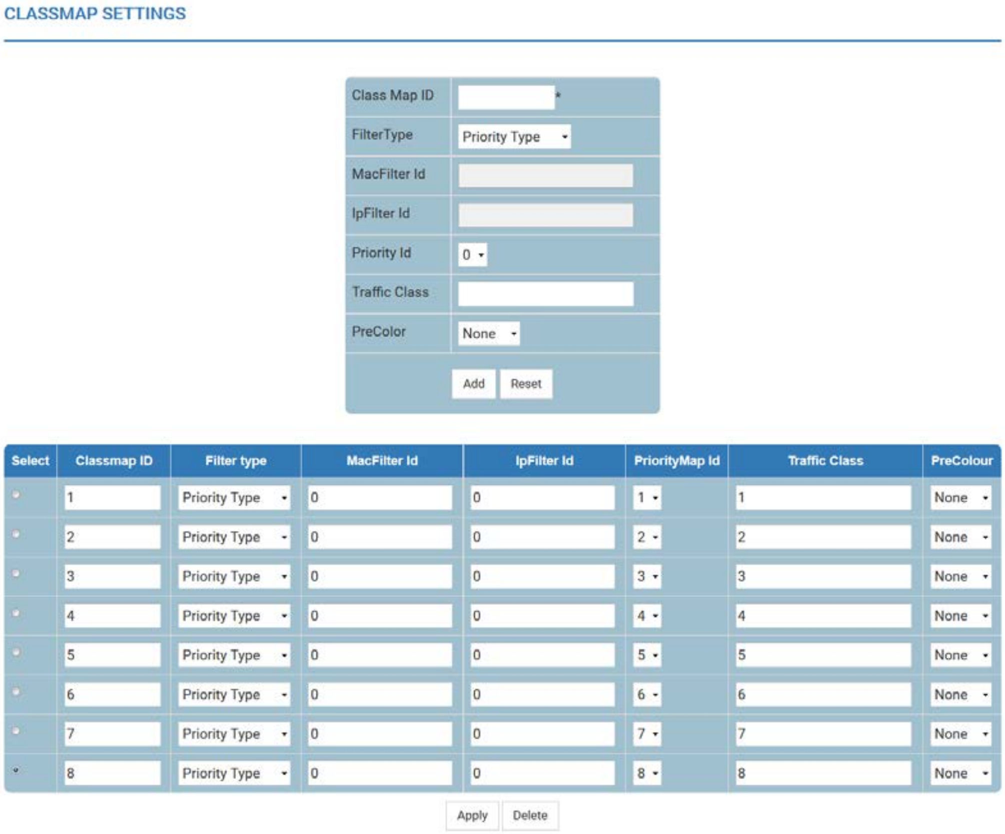
Default option is VlanPri

Regen Priority - Specifies the regenerated priority value determined for the received frame. This value ranges between 0 and 63. Default value is 0.

> Note there are rules for different priority types. Reference to 'In Priority'.

Regen Inner Priority - Specifies the regenerated inner priority value determined for the received frame. This value ranges between zero and seven.

3.7.4 ClassMap



CLASSMAP SETTINGS

Class Map ID	*
FilterType	Priority Type
MacFilter Id	
IpFilter Id	
Priority Id	0
Traffic Class	
PreColor	None

Select	Classmap ID	Filter type	MacFilter Id	IpFilter Id	PriorityMap Id	Traffic Class	PreColour
○	1	Priority Type	0	0	1	1	None
○	2	Priority Type	0	0	2	2	None
○	3	Priority Type	0	0	3	3	None
○	4	Priority Type	0	0	4	4	None
○	5	Priority Type	0	0	5	5	None
○	6	Priority Type	0	0	6	6	None
○	7	Priority Type	0	0	7	7	None
●	8	Priority Type	0	0	8	8	None

Fig: ClassMap Settings

The *ClassMap* link opens the **ClassMap Settings** Page.

The Classmap Settings page allows the user to classify the stream of traffic.

The table below lists the fields present in this page.

Class Map ID - Specifies a unique ID for classmap. This value ranges between 1 and 65535.

FilterType - Specifies the filter type associated with the classmap. Options are:

* Priority Type

* Mac or Ip type

MacFilter Id - Specifies the MAC filter ID associated with this classmap. This value ranges between 0 and 65535. Default value is 0.

IpFilter Id - Specifies the IP filter ID associated with this classmap. This value ranges between 0 and 65535. Default value is 0.

Priority Id - Specifies the priority map ID associated with this classmap. Default value is 0.

Traffic Class - Specifies the traffic class associated with the classmap. This value ranges between 1 and 65535.

PreColor - Specifies the color of the packet prior to metering. Options are:

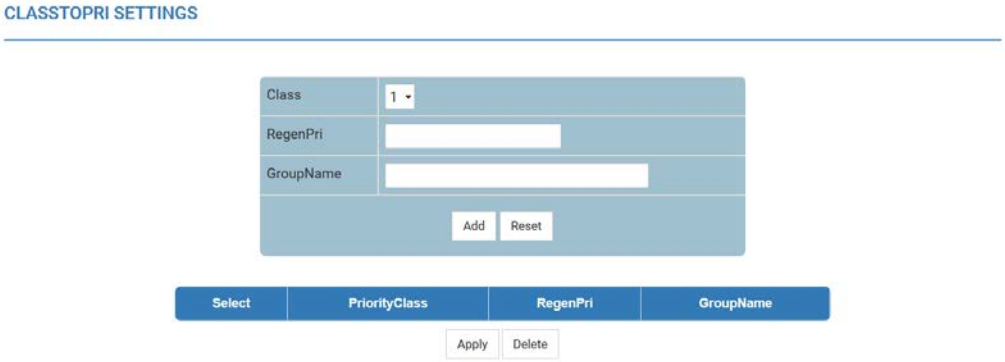
* None - Traffic is not pre-colored.

* Green - Traffic conforms to SLAs.

* Yellow - Traffic exceeds the SLAs.

* Red - Traffic violates the SLAs.

3.7.5 ClasstoPriMap



CLASSTOPRI SETTINGS

Class	1
RegenPri	
GroupName	

Select	PriorityClass	RegenPri	GroupName

Fig: ClasstoPri Settings

The *ClasstoPriMap* link opens the **ClasstoPri Settings** Page.

The ClasstoPri Settings page allows the user to configure the class to priority settings.

The table below lists the fields present in this page.

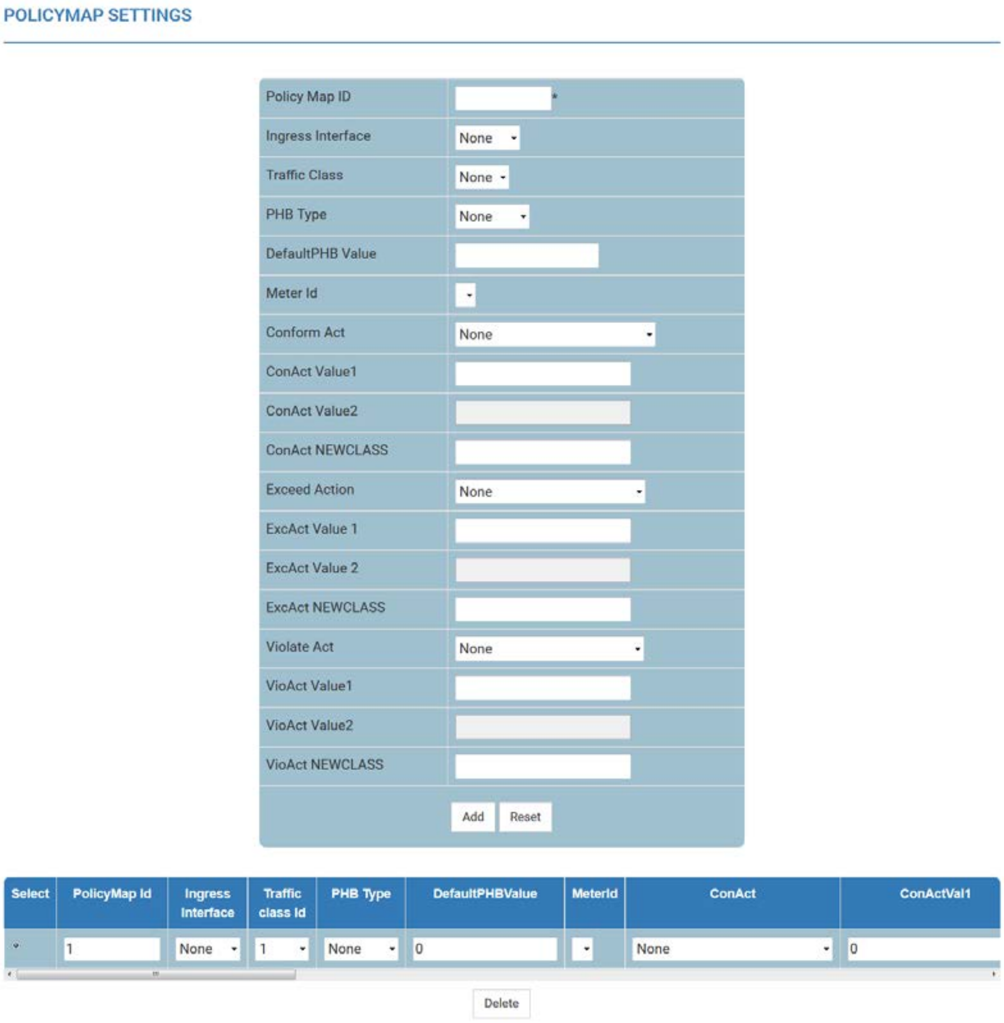
Class - Select the traffic class from existing ClassMap Settings.

To add a new class, go to ClassMap Settings and add a ClassMap with the class.

RegenPri - Specifies the regenerated priority value determined for the input class. This value ranges between zero and seven.

GroupName - Unique identification of the group to which an input class belongs.

3.7.6 PolicyMap



POLICYMAP SETTINGS

Policy Map ID	*
Ingress Interface	None
Traffic Class	None
PHB Type	None
DefaultPHB Value	
Meter Id	
Conform Act	None
ConAct Value1	
ConAct Value2	
ConAct NEWCLASS	
Exceed Action	None
ExcAct Value 1	
ExcAct Value 2	
ExcAct NEWCLASS	
Violate Act	None
VioAct Value1	
VioAct Value2	
VioAct NEWCLASS	

Select	PolicyMap Id	Ingress Interface	Traffic class Id	PHB Type	DefaultPHBValue	MeterId	ConAct	ConActVal1
○	1	None	1	None	0		None	0

Fig: PolicyMap Settings

The *PolicyMap* link opens the **PolicyMap Settings** Page.

The PolicyMap Settings page allows the user to configure action for a specified classmap.

The table below lists the fields present in this page.

Policy Map ID - Specifies the unique ID for policy map. This value ranges between 1 and 65535.

Ingress Interface - Specifies the incoming port number:

Traffic Class - Specifies the traffic class for which the policy map needs to be applied.

PHB Type - Indicates the PHB (Per Hop Behavior) type to be used for filling the default PHB for the policy map entry. Options are:

* None

* VlanPri

* ipTos

* ipDscp

* mplsExp

DefaultPHB Value - Indicates the default outgoing PHB values for the policy map. This value ranges between 0 and 63.

Meter Id - Specifies to a meter table ID which is the index for the meter table. Default value is 0.

Conform Act - Specifies the action to be performed on the packet, when the packets are found to be in profile. Options are:

* None - None.

* ActionIPsetPort - Sets the new port value.

* ConformActionIPTos - Sets the new IP TOS value.

* ConformActionDSCP - Sets the new DSCP value.

* ConformActionVlanPriandDE - Sets the VLAN priority and VLAN Drop Eligible indicator of the outgoing packet.

* ConformActionInnerVlanPri - Sets the Inner VLAN priority of the outgoing packet.

* ConformActionMplsEXP - Sets the MPLS Experimental bits of the outgoing packet.

ConAct Value 1 - Specifies the conform action value for either VlanPri or VlanDe.

ConAct Value 2 - Specifies the conform action value for either VlanPri or VlanDe.

ConAct NEWCLASS - Represents the traffic class to which an incoming frame pattern is classified after metering.

Exceed Action - Specifies the action to be performed on the packet, when the packets are found to be in profile. Options are:

* Drop - Drops the packet.

* ExceedActionIPTos - Sets the new IP TOS value.

* ExceedActionDSCP - Sets the new DSCP value.

* ExceedActionVlanPriandDE - Sets the VLAN priority and VLAN Drop Eligible indicator of the outgoing packet.

* ExceedActionInnerVlanPri - Sets the Inner VLAN priority of the outgoing packet.

* ExceedActionMplsEXP - Sets the MPLS Experimental bits of the outgoing packet.

ExcAct Value1 - Specifies the exceed action value for either VlanPri or VlanDe.

ExcAct Value2 - Specifies the exceed action value for either VlanPri or VlanDe.

ExcAct NEWCLASS - Represents the traffic class to which an incoming frame pattern is classified after metering.

Violate Act - Specifies the action to be performed on the packet when the packets are found to be out of profile. Options are:

* Drop - Drops the packet.

* ViolateActionIPTos - Sets the new IP TOS value.

* ViolateActionDSCP - Sets the new DSCP value.

* ViolateActionVlanPriandDE - Sets the VLAN priority and VLAN Drop Eligible indicator of the outgoing packet.

* ViolateActionInnerVlanPri - Sets the Inner VLAN priority of the outgoing packet.

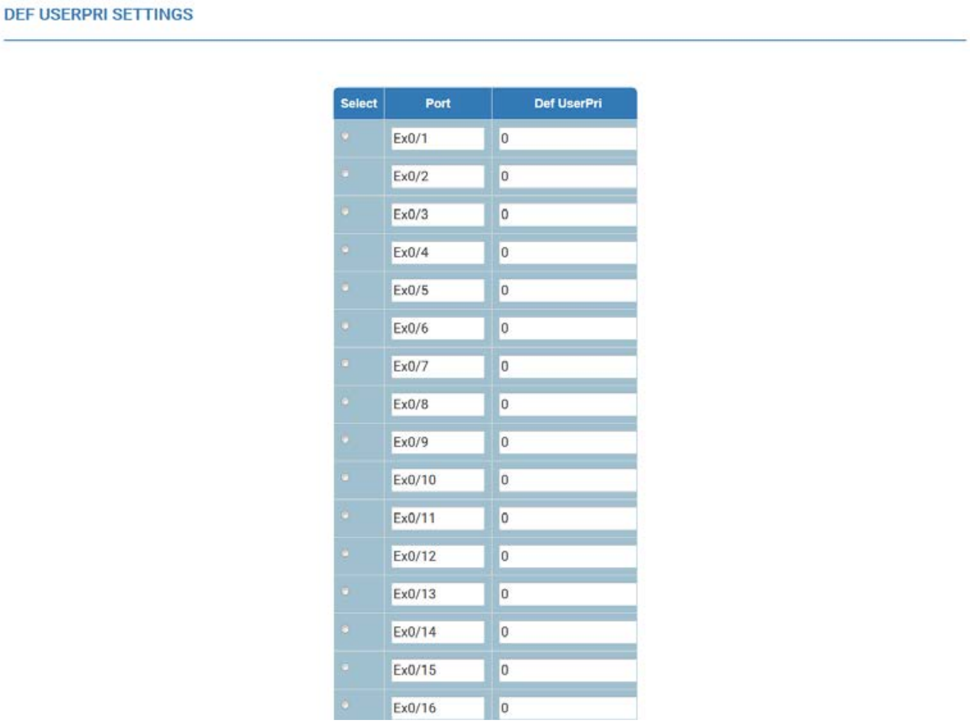
* ViolateActionMplsEXP - Sets the MPLS Experimental bits of the outgoing packet.

VioAct Value1 - Specifies the violate action value for either VlanPri or VlanDe.

VioAct Value2 - Specifies the violate action value for either VlanPri or VlanDe.

VioAct NEWCLASS - Represents the traffic class to which an incoming frame pattern is classified after metering.

3.7.7 Def UserPri



DEF USERPRI SETTINGS

Select	Port	Def UserPri
○	Ex0/1	0
○	Ex0/2	0
○	Ex0/3	0
○	Ex0/4	0
○	Ex0/5	0
○	Ex0/6	0
○	Ex0/7	0
○	Ex0/8	0
○	Ex0/9	0
○	Ex0/10	0
○	Ex0/11	0
○	Ex0/12	0
○	Ex0/13	0
○	Ex0/14	0
○	Ex0/15	0
○	Ex0/16	0

Fig: Def UserPri Settings

The *Def UserPri* link opens the **Def UserPri Settings** Page.

The Def UserPri Settings page allows the user to configure the default user priority settings.

The table below lists the fields present in this page.

Port - Specifies the port number.

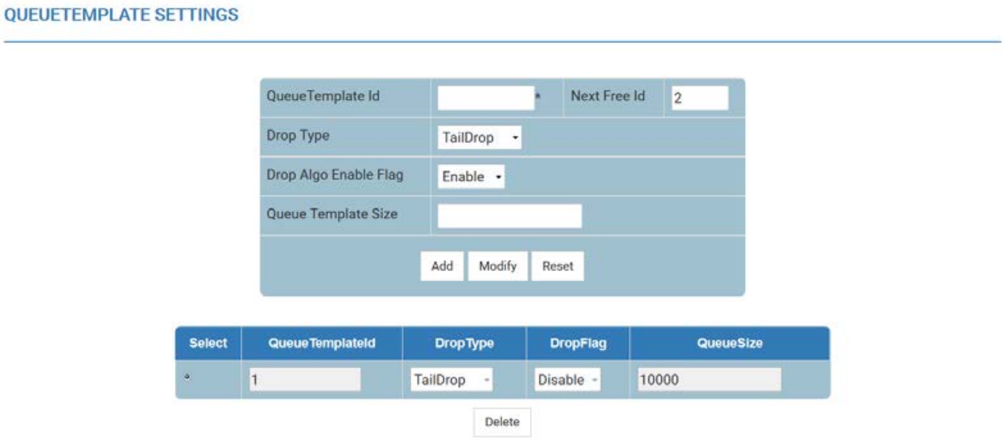
Def UserPri - Specifies the default user priority. This value ranges between zero and seven.

3.8 QoSEgress

The *QoSEgress* link allows you to configure the QoS Egress settings for switch. User can configure QoSEgress on the following seven pages.

- QueueTemplate
- RedConf
- ShapeTemplate
- SchedulerTable
- QueueTable
- Hierarchy
- Q Map

3.8.1 QueueTemplate


QUEUETEMPLATE SETTINGS

QueueTemplate Id	*	Next Free Id	2
Drop Type	TailDrop		
Drop Algo Enable Flag	Enable		
Queue Template Size			

Select	QueueTemplateId	DropType	DropFlag	QueueSize
○	1	TailDrop	Disable	10000

Fig: QueueTemplate Settings

The *QueueTemplate* link opens the **QueueTemplate Settings** Page.

The QueueTemplate Settings page allows the user to configure the queue template settings.

The table below lists the fields present in this page.

QueueTemplate Id - Specifies the index that enumerates the queue entries. This value ranges between 1 and 65535.

Next Free Id - Specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field.

Drop Type - Specifies the type of drop algorithm used by this queue template. Options are:

* TailDrop - Queue template size represents the maximum depth of the queue, beyond which all newly arriving packets are dropped.

* HeadDrop - If a packet arrives, when the current depth of the queue is at queue template size, packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue.

* RED - On packet arrival, an active queue management algorithm is executed which may randomly drop a packet. This algorithm may be proprietary, and it may drop either the arriving packet or another packet in the queue.

* WRED - On packet arrival, an active queue management algorithm is executed which may randomly drop a packet. This algorithm may be proprietary, and it may drop either the arriving packet or another packet in the queue.

Drop Algo Enable Flag - Enables/disables drop algorithm for congestion management. Options are:

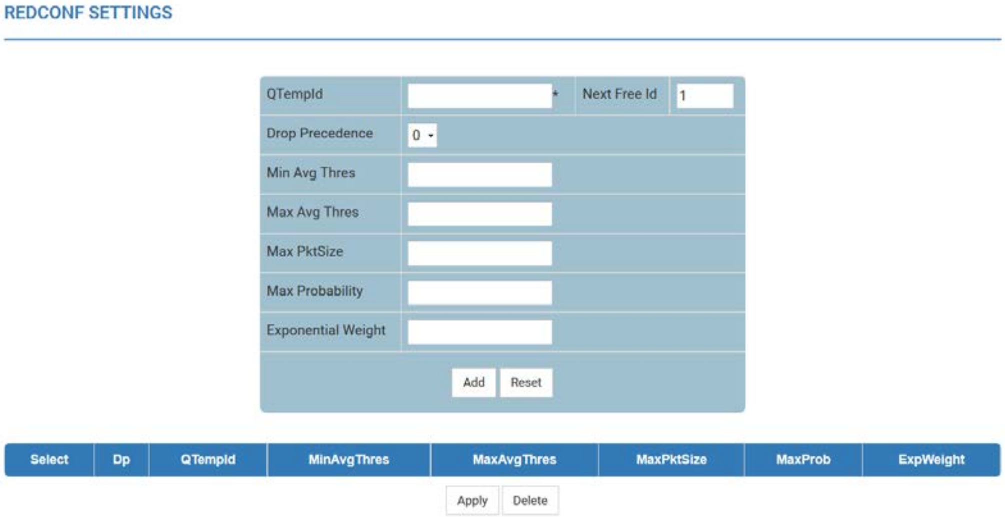
* Enable - Enables drop algorithm for congestion management.

* Disable - Disables drop algorithm for congestion management.

By default, this is enabled.

Queue Template Size - Specifies the queue size. This value ranges between 1 and 65535.

3.8.2 RedConf


REDCONF SETTINGS

QTempId	*	Next Free Id	1
Drop Precedence	0		
Min Avg Thres			
Max Avg Thres			
Max PktSize			
Max Probability			
Exponential Weight			

Select	Dp	QTempId	MinAvgThres	MaxAvgThres	MaxPktSize	MaxProb	ExpWeight

Fig: RedConf Settings

The *RedConf* link opens the **RedConf Settings** Page.

The RedConf Settings page allows the user to configure parameters for Random Detect Algorithm.

The table below lists the fields present in this page.

QTempId - Specifies the index that enumerates the queue entries. This value ranges between 1 and 65535.

Next Free Id - Specifies an integer which may be used as a new index in the table. The value of zero indicates that no more new entries can be created in the relevant table. This is a read only field.

Drop Precedence - Specifies the drop precedence. Options are:

* 0 **-** Low drop precedence.

* 1 - Medium drop precedence.

* 2 - High drop precedence.

Min Avg Thres - Specifies the minimum average threshold for the random detect algorithm. Below this threshold, packets are admitted into the queue. This value ranges between 1 and 65535.

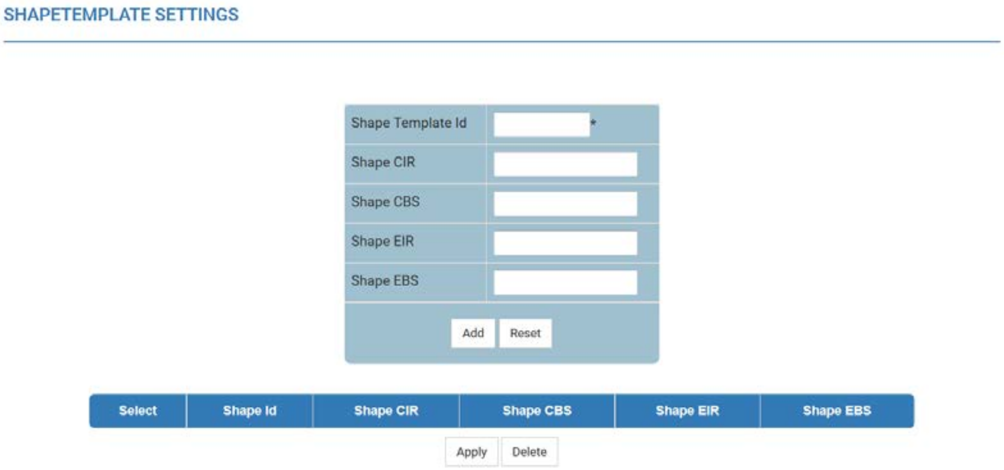
Max Avg Thres - Specifies the maximum average threshold for the random detect algorithm. Above this threshold, packets are discarded before entering the queue. This value ranges between 1 and 65535.

Max PktSize - Specifies the maximum allowed packet size. This value ranges between 1 and 65535.

Max Probability - Specifies the maximum probability of discarding a packet in units of percentage. This value ranges between 1 and 100. Default value is 100.

Exponential Weight - Specifies the exponential weight for determining the average queue size. This value ranges between 0 and 31. Default value is 0.

3.8.3 ShapeTemplate



SHAPETEMPLATE SETTINGS

Shape Template Id	*
Shape CIR	
Shape CBS	
Shape EIR	
Shape EBS	

Select	Shape Id	Shape CIR	Shape CBS	Shape EIR	Shape EBS

Fig: ShapeTemplate Settings

The *ShapeTemplate* link opens the **ShapeTemplate Settings** Page.

The ShapeTemplate Settings page allows the user to configure the shaper attributes.

The table below lists the fields present in this page.

Shape Template Id - Specifies the shape template table index. This value ranges between 1 and 65535.

Shape CIR - Specifies the committed information rate for packets through this queue. This value ranges between 1 and 10485760. The default value is 10000.

CIR should be less than or equal to EIR.

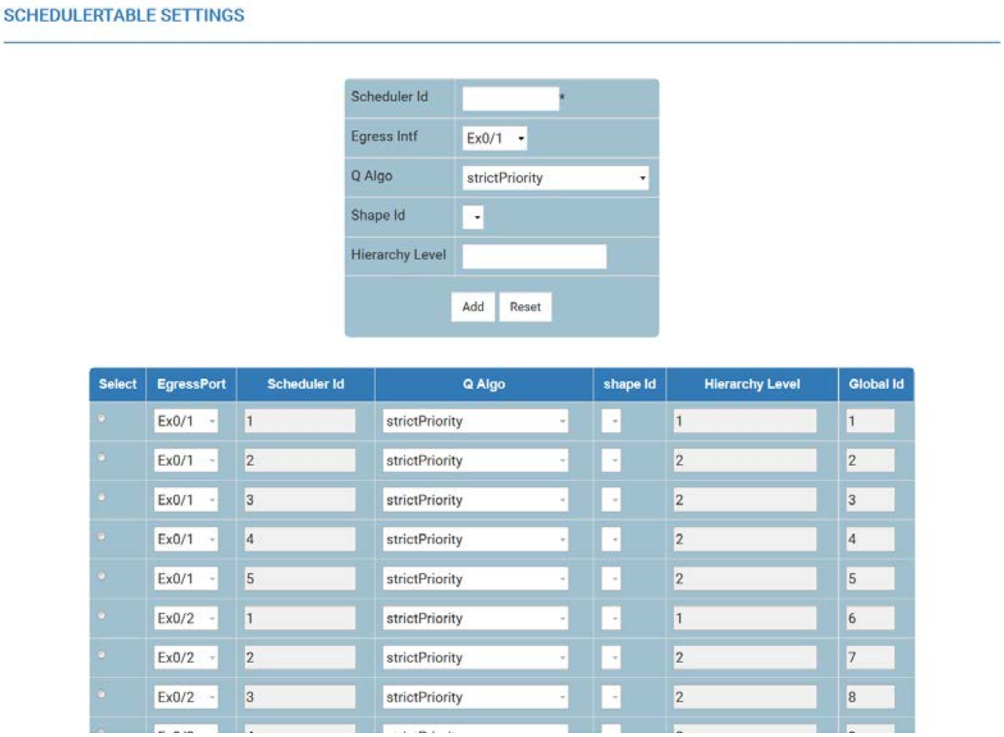
Shape CBS - Specifies the committed burst size for packets through this queue. This value ranges between 0 and 10485760. The default value is 10000.

Shape EIR - Specifies the excess information rate for packets through this hierarchy. This value ranges between 0 and 10485760. The default value is 10000.

EIR should be more than CIR.

Shape EBS - Specifies the excess burst size for packets through this hierarchy. This value ranges between 0 and 10485760. The default value is 10000.

3.8.4 SchedulerTable



SCHEDULERTABLE SETTINGS

Scheduler Id	*
Egress Intf	Ex0/1
Q Algo	strictPriority
Shape Id	
Hierarchy Level	

Select	EgressPort	Scheduler Id	Q Algo	shape Id	Hierarchy Level	Global Id
○	Ex0/1	1	strictPriority		1	1
○	Ex0/1	2	strictPriority		2	2
○	Ex0/1	3	strictPriority		2	3
○	Ex0/1	4	strictPriority		2	4
○	Ex0/1	5	strictPriority		2	5
○	Ex0/2	1	strictPriority		1	6
○	Ex0/2	2	strictPriority		2	7
○	Ex0/2	3	strictPriority		2	8

Fig: SchedulerTable Settings

The *SchedulerTable* link opens the **SchedulerTable Settings** Page.

The SchedulerTable Settings page allows the user to configure the scheduler settings.

The table below lists the fields present in this page.

Scheduler Id - Specifies the scheduler identifier that uniquely identifies the scheduler in the system/egress interface. This value ranges between 1 and 65535.

Egress Interface - Specifies the outgoing port number.

Q Algo - Sets the packet scheduling algorithm for the port. Options are:

* strictPriority

* roundRobin

* weightedRoundRobin

* weightedFairQueing

* strictRoundRobin

* strictWeightedRoundRobin

* strictWeightedFairQueing

* deficitRoundRobin

Default option is strictPriority.

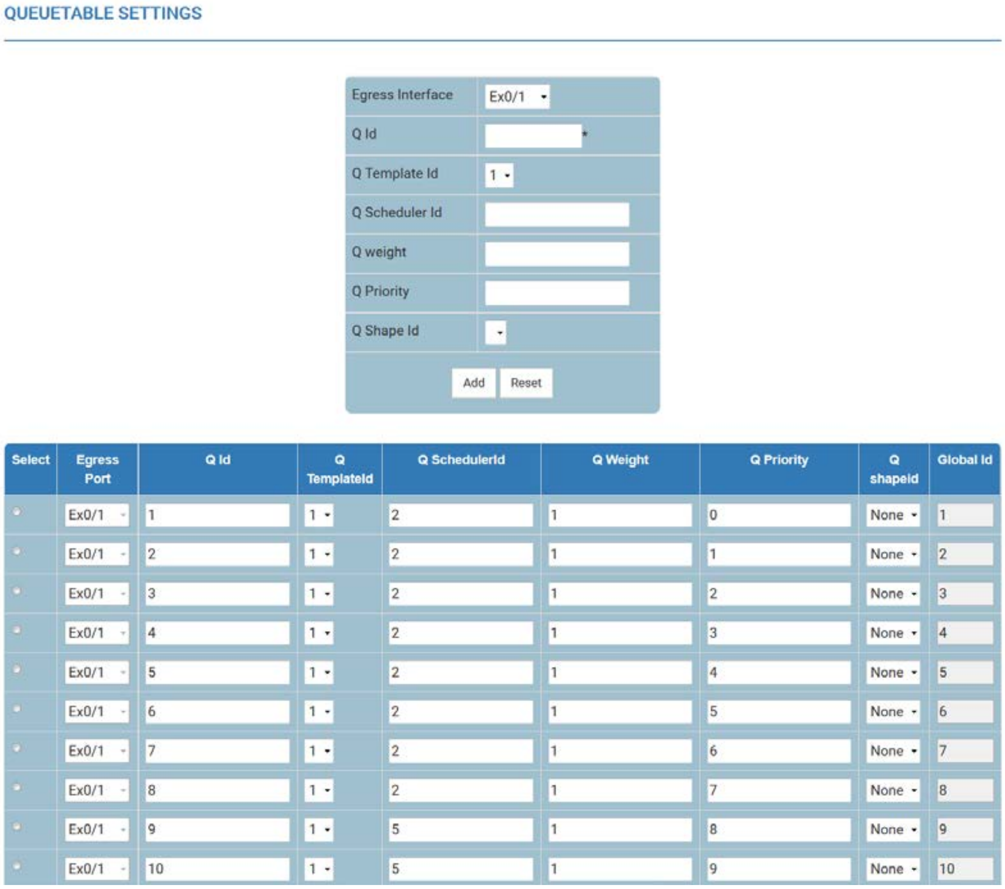
Shape Id - Specifies the shaper identifier that specifies the bandwidth requirements for the scheduler. This value ranges between 0 and 65535.

Hierarchy Level - Indicates the depth of the queue/scheduler hierarchy. This value ranges between 0 and 10. Default value is 0.

> For BCM hardware, it only supports 1, 2 and 3.

Global Id - Specifies the scheduler identifier that uniquely identifies the scheduler in the system / egress interface. This value ranges between 0 and 65535.

3.8.5 QueueTable


QUEUETABLE SETTINGS

Egress Interface	Ex0/1
Q Id	*
Q Template Id	1
Q Scheduler Id	
Q weight	
Q Priority	
Q Shape Id	

Select	Egress Port	Q Id	Q TemplateId	Q SchedulerId	Q Weight	Q Priority	Q shapeId	Global Id
○	Ex0/1	1	1	2	1	0	None	1
○	Ex0/1	2	1	2	1	1	None	2
○	Ex0/1	3	1	2	1	2	None	3
○	Ex0/1	4	1	2	1	3	None	4
○	Ex0/1	5	1	2	1	4	None	5
○	Ex0/1	6	1	2	1	5	None	6
○	Ex0/1	7	1	2	1	6	None	7
○	Ex0/1	8	1	2	1	7	None	8
○	Ex0/1	9	1	5	1	8	None	9
○	Ex0/1	10	1	5	1	9	None	10

Fig: QueueTable Settings

The *QueueTable* link opens the **QueueTable Settings** Page.

The QueueTable Settings page allows the user to configure the queue parameters.

The table below lists the fields present in this page.

Egress Interface - Specifies the outgoing port number.

Q Id - Specifies the queue identifier that uniquely identifies the queue in the system/port. This value ranges between 1 and 65535.

Q Template Id - Specifies the queue template ID applied for configuring queue attributes. This value ranges between 1 and 65535.

Q Scheduler Id - Specifies the scheduler identifier that manages the specified queue. This identifier is unique relative to an egress interface. This value ranges between 1 and 65535.

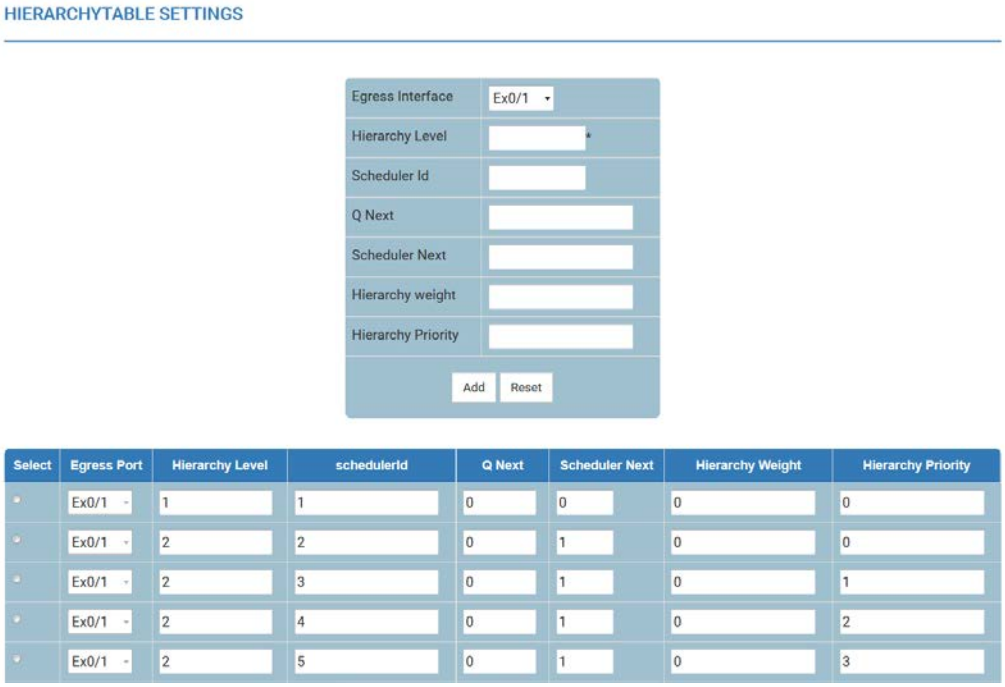
Q weight - Specifies the user assigned weight to the CoS queue. The assigned weights are used only when the scheduling algorithm is a weighted scheduling algorithm. This value ranges between 1 and 1000.

Q Priority - Specifies the user assigned priority for the CoS queue. The assigned priority is used only when the scheduler uses a priority based scheduling algorithm. This value ranges between 0 and 15. Default value is 0.

Q Shape Id - Specifies the shaper identifier that specifies the bandwidth requirements for the queue. This value ranges between 0 and 65535.

Global Id - Specifies the queue identifier that uniquely identifies the queue in the system / egress interface. This field is read only. This value ranges between 0 and 192.

3.8.6 Hierarchy



HIERARCHYTABLE SETTINGS

Egress Interface	Ex0/1
Hierarchy Level	*
Scheduler Id	
Q Next	
Scheduler Next	
Hierarchy weight	
Hierarchy Priority	

Select	Egress Port	Hierarchy Level	schedulerId	Q Next	Scheduler Next	Hierarchy Weight	Hierarchy Priority
○	Ex0/1	1	1	0	0	0	0
○	Ex0/1	2	2	0	1	0	0
○	Ex0/1	2	3	0	1	0	1
○	Ex0/1	2	4	0	1	0	2
○	Ex0/1	2	5	0	1	0	3

Fig: HierarchyTable Settings

The *Hierarchy* link opens the **HierarchyTable Settings** Page.

The HierarchyTable Settings page allows the user to specify the hierarchy details.

The table below lists the fields present in this page.

Egress Interface - Specifies the outgoing port number.

Hierarchy Level - Indicates the depth of the queue/scheduler hierarchy. This value ranges between 1 and 10.

Scheduler Id - Specifies the scheduler identifier that uniquely identifies the scheduler in the system/egress interface.

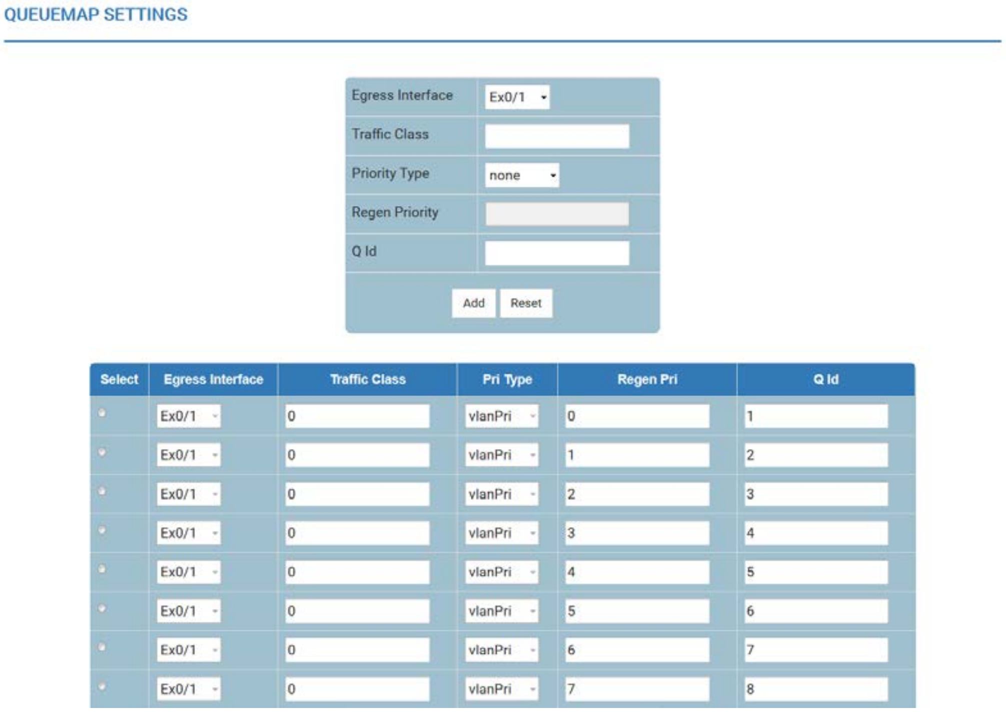
Q Next - Specifies the next-level queue to which the scheduler output needs to be sent. The value of this object could be unique in the system/port.

Scheduler Next - Specifies the next-level scheduler to which the scheduler output needs to be sent. The value of this object could be unique in the system/port.

Hierarchy weight - Specifies the weight if the scheduler is connecting to a WFQ of another scheduler. This value ranges between 0 and 1000.

Hierarchy Priority - Specifies the priority when the scheduler is connecting to any of the priorities (EF, AF, BE) of the next level strict-priority scheduler. This value ranges between 0 and 15. Default value is 0.

3.8.7 Q Map



QUEUEMAP SETTINGS

Egress Interface	Ex0/1
Traffic Class	
Priority Type	none
Regen Priority	
Q Id	

Select	Egress Interface	Traffic Class	Pri Type	Regen Pri	Q Id
○	Ex0/1	0	vlanPri	0	1
○	Ex0/1	0	vlanPri	1	2
○	Ex0/1	0	vlanPri	2	3
○	Ex0/1	0	vlanPri	3	4
○	Ex0/1	0	vlanPri	4	5
○	Ex0/1	0	vlanPri	5	6
○	Ex0/1	0	vlanPri	6	7
○	Ex0/1	0	vlanPri	7	8

Fig: QueueMap Settings

The *Q Map* link opens the **QueueMap Settings** Page.

The QueueMap Settings page allows the user to map an egress port, CLASS of service to a queue.

The table below lists the fields present in this page.

Egress Interface - Specifies the outgoing port number.

Traffic Class - Specifies the input class (associated with an incoming packet) that needs to be mapped to an outbound queue. This value ranges between 0 and 65535.

Priority Type - Specifies the regenerated-priority type to interpret the value of RegenPriority object. Options are:

* none

* vlanPri

* ipTos

* ipDscp

* mplsExp

* vlanDEI

Regen Priority - Specifies the regenerated-priority (for an incoming packet) that needs to be mapped to an outbound queue. This is mutually exclusive to the CLASS configuration. This value ranges between 0 and 63.

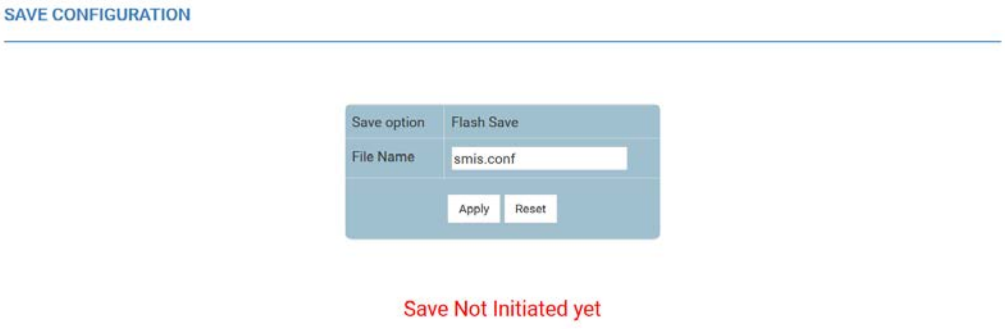
Q Id - Specifies the queue identifier that uniquely identifies a queue relative to an interface. It could be configured with a unique value in the system. This value ranges between 1 and 65535.

3.9 Save and Restore

The *Save and Restore* link allows you to configure the file management settings for switch. User can configure Save and Restore on the following three pages.

- Save
- Restore
- Erase

3.9.1 Save


SAVE CONFIGURATION

Save option	Flash Save
File Name	smis.conf

Save Not Initiated yet

Fig: Save Configuration

The *Save* link opens the **Save Configuration** Page.

This page allows the user to save the current configuration of the switch in a file

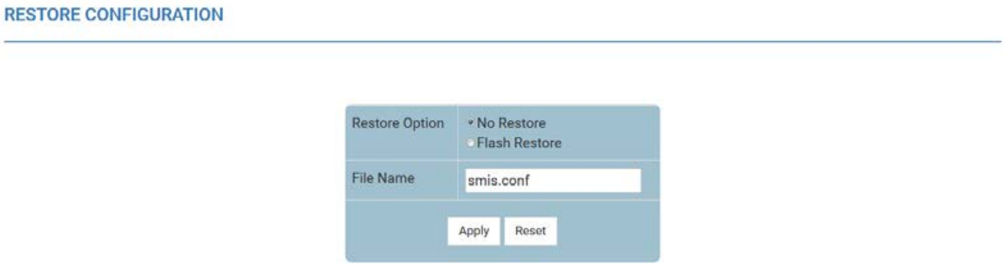
The table below lists the fields present in this page.

Save option - Click one of the option buttons to specify the save option to be used for the Switch. The options are:

* Flash Save - Saves the configurations in the specified file name of the Flash

File Name - Enter the name of the file in which the Switch configurations are to be saved. The default file name where the Switch configurations are saved is smis.conf. All configurations are saved in a single configuration file only.

3.9.2 Restore


RESTORE CONFIGURATION

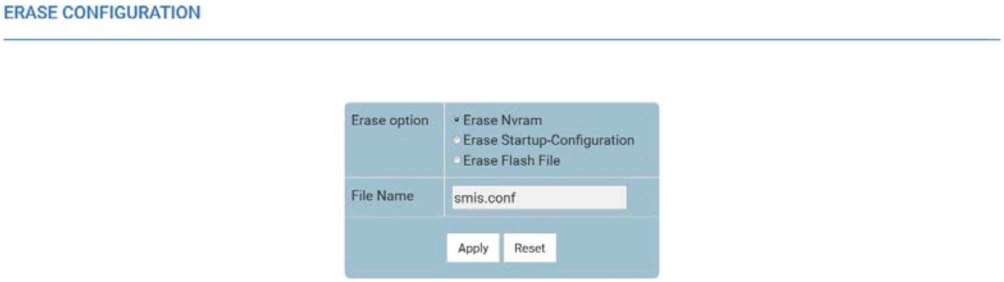
Restore Option	● No Restore ○ Flash Restore
File Name	smis.conf

Fig: Restore configuration

The *Restore* link opens the **Restore configuration** Page.
This page allows the user to restore the previously saved configurations of the switch from the Startup Configuration File.

The table below lists the fields present in this page.
Restore option - Click one of the option buttons to specify whether the Switch configurations have to be restored. The list contains:
* No Restore - Specifies that the switch configurations need not be restored when
the system is restarted
* Flash Restore - Restores the configurations from the Startup Configuration File in the Flash, when the system is restarted.
File Name - Enter the configuration file name available in the remote system. The default file name is smis.conf.

3.9.3 Erase



ERASE CONFIGURATION

Erase option: ● Erase Nvram ○ Erase Startup-Configuration ○ Erase Flash File

File Name: smis.conf

Fig: Erase configuration

The *Erase* link opens the **Erase configuration** Page.

This page allows the user to:

* Reset the system startup configurations present in the issnvram.txt file.

The default system startup configuration takes effect after the system reboot.

* Erase or delete the saved configuration from Flash.

* Delete any file present in the Flash.

The table below lists the fields present in this page.

Erase option - Click one of the option buttons to specify the erase or delete configuration or file. Options are:

* Erase Nvram - Resets the System startup parameter values present in the issnvram.txt file to default values. These default values take effect only after the system reboot.

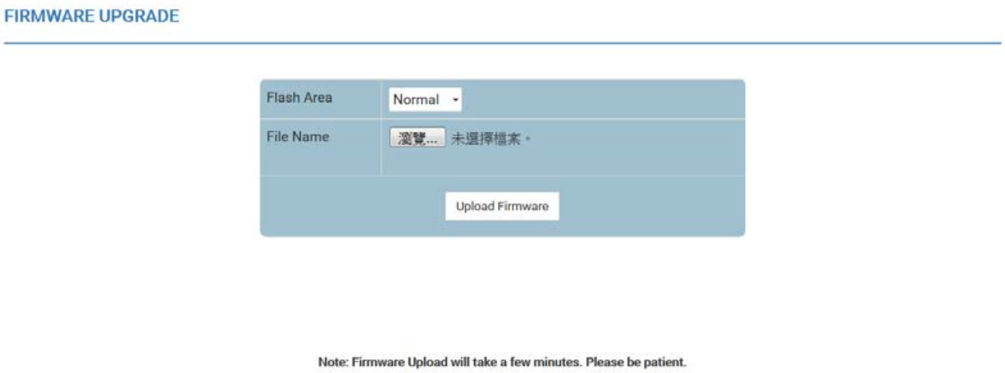
* Erase Startup-Configuration - Erases the earlier saved configurations of the entire system, from Flash. Whenever the Switch reboots, the system comes up with default parameters upon next Switch restart.

* Erase Flash File - Deletes any file from Flash specified in the File Name field of this screen.

File Name - Enter the configuration file name to be erased. The default file name is smis.conf. Any other file which needs to be deleted from Flash can also be specified.

> This field is configurable only if the Erase option is set as Erase Flash File.

3.10Image Download



Flash Area: Normal

File Name: 未選擇檔案。

Note: Firmware Upload will take a few minutes. Please be patient.

Fig: Firmware Upgrade

The *Firmware Upgrade* link opens the **Firmware Upgrade** Page.
This page allows the user to perform an image download operation on a standalone switch to download a new image from the user's local file system to the switch.

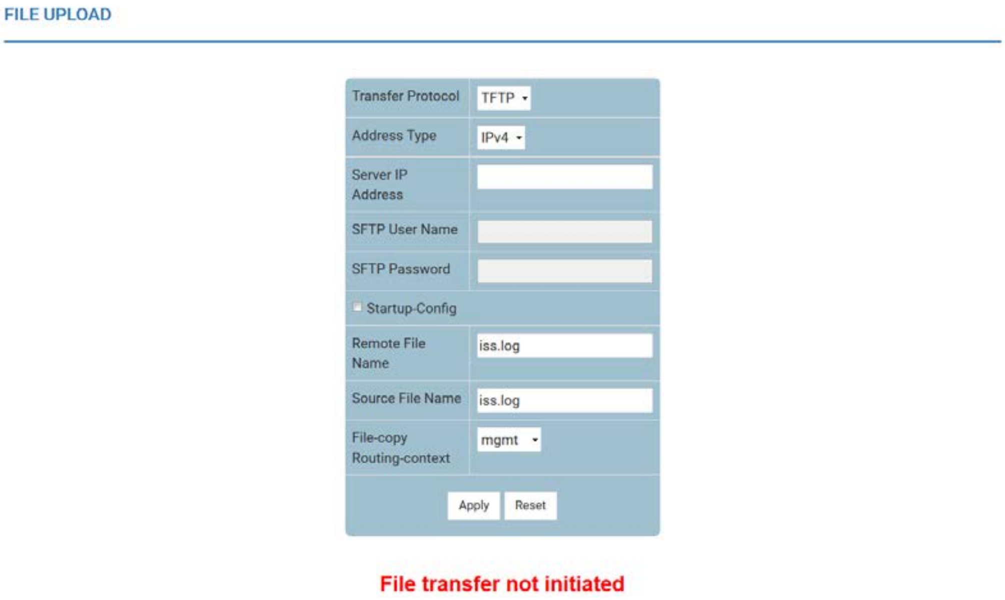
The table below lists the fields present in this page.
Flash Area - Select the boot area for the image to be downloaded.
* Normal - The normal boot area.
* Fallback - The fallback boot area.
File Name - Open a dialog to browse user's local file system and choose the image file to be downloaded.

3.11File Transfer

The *File Transfer* link allows you to configure the file upload / download settings for switch. User can configure File Transfer on the following two pages.

- File Upload
- File Download

3.11.1 File Upload



FILE UPLOAD

Transfer Protocol	TFTP
Address Type	IPv4
Server IP Address	
SFTP User Name	
SFTP Password	
□ Startup-Config	
Remote File Name	iss.log
Source File Name	iss.log
File-copy Routing-context	mgmt

File transfer not initiated

Fig: File Upload

The *File Upload* link opens the **File Upload** Page.

This page allows the user to upload file from remote server.

The table below lists the fields present in this page.

Transfer Protocol - Select the transfer mode for uploading file to the remote system.

By default it as set as TFTP. The list contains:

* TFTP **-** Uploads the file in TFTP (Trivial File Transfer Protocol) mode.

* SFTP **-** Uploads the file in SFTP (SSH File Transfer Protocol) mode.

Address Type - Select the IP Address type of the machine to which the file is to be uploaded.

By default it as set as IPv4. The list contains:

* IPv4 **-** Sets the Address type as IPv4.

* IPv6 **-** Sets the Address type as IPv6.

Server IP Address - Enter the IP address of the machine to which the file is to be uploaded.

SFTP User Name - Enter the user name required for uploading file in SFTP mode. This field is a string with size varying between 1 and 20.

> This field is disabled if the Transfer Protocol is selected as TFTP.

SFTP Password - Enter the password required for uploading file in SFTP mode. This field is a string with size varying between 1 and 20.

> This field is disabled if the Transfer Protocol is selected as TFTP.

Startup config - Select the function Startup configuration. A startup configuration contains configuration information that is used at reboot. This command takes a backup of the initial configuration in flash or at a remote location.

Remote File Name - Enter the name of the remote file after uploaded to the remote system.

Source File Name - Enter the name of the source file to be uploaded to the remote system.

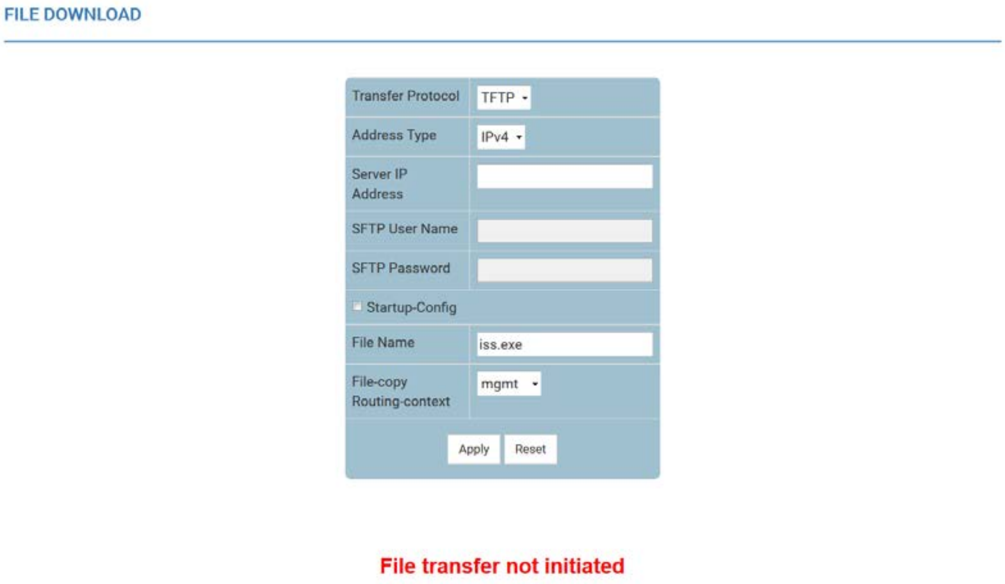
File-copy Routing-context - Select routing context for copy operation.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

3.11.2 File Download



FILE DOWNLOAD

Transfer Protocol	TFTP
Address Type	IPv4
Server IP Address	
SFTP User Name	
SFTP Password	
□ Startup-Config	
File Name	iss.exe
File-copy Routing-context	mgmt

File transfer not initiated

Fig: File Download

The *File Download* link opens the **File Download** Page.

This page allows the user to configure the file download details.

The table below lists the fields present in this page.

Transfer Protocol - Select the transfer mode for downloading file from the remote system. The default value is TFTP. The list contains:

* TFTP - Downloads the file in TFTP (Trivial File Transfer Protocol) mode.

* SFTP - Downloads the file in SFTP (SSH File Transfer Protocol) mode.

Address Type - Select the IP Address type of the machine to which the file is to be downloaded. By default it as set as IPv4. The list contains:

* IPv4 - Sets the Address type as IPv4.

* IPv6 - Sets the Address type as IPv6.

Server IP Address - Enter the IP address of the machine from which the file is to be downloaded.

SFTP User Name - Enter the user name required for downloading file in SFTP mode. This field is a string with size varying between 1 and 20.

> This field is disabled if the Transfer Protocol is selected as TFTP.

SFTP Password - Enter the password required for downloading file in SFTP mode. This field is a string with size varying between 1 and 20.

> This field is disabled if the Transfer Protocol is selected as TFTP.

Startup config - Select the function Startup configuration. A startup configuration contains configuration information that is used at reboot. This command retrieves a backup of the initial configuration from flash or a remote location to use it for restoration.

File Name - Enter the name of the file to be downloaded from the remote system.

File-copy Routing-context - Select routing context for copy operation.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports

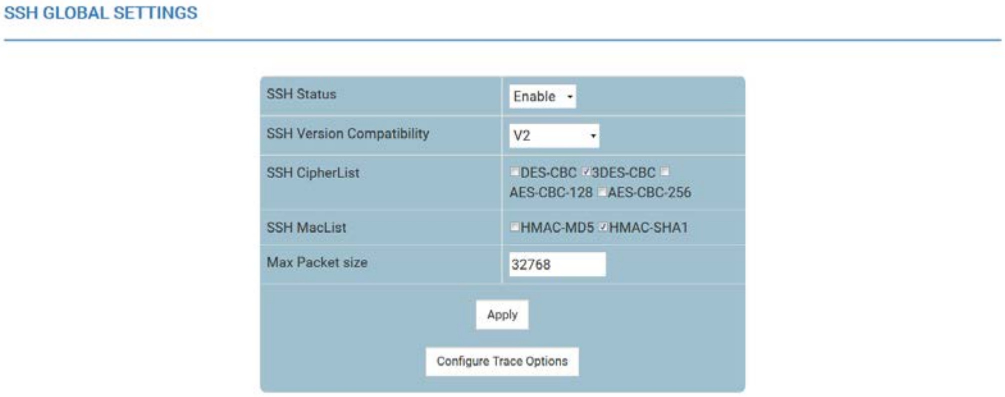
* mgmt - use the "mgmt VRF table for switch OOB port

3.12 SSH

The *SSH* link allows you to configure the SSH settings for switch. User can configure SSH on the following two pages.

- SSH Global Settings
- SSH Traces

3.12.1 SSH Global Settings



SSH GLOBAL SETTINGS

SSH Status	Enable
SSH Version Compatibility	V2
SSH CipherList	□DES-CBC ☑3DES-CBC □AES-CBC-128 □AES-CBC-256
SSH MacList	□HMAC-MD5 ☑HMAC-SHA1
Max Packet size	32768

Fig: SSH Global Settings

The *SSH Global Settings* link opens the **SSH Global Settings** Page.

The table below lists the fields present in this page.

SSH Status - Select the status of the SSH module.

By default, SSH status is set as Enabled. The list contains:

* Enable - Enables the SSH feature in the switch. SSH feature enables the user to log into a remote machine and execute commands.

* Disable - Disables the SSH feature in the switch. This action disconnects the secure channel.

SSH version Compatibility - Select the version of the SSH.

By default, the SSH version compatibility is set as V2. The list contains:

* Both V1,V2 - Supports both SSH version-1 and version-2.

* V2 - Supports only the SSH version-2.

SSH CipherList - Select the Cipher-List. The cipher list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list will be used for Encryption. DES-CBC is the default algorithm in NON-FIPS mode and 3DES-CBC is the default algorithm in FIPS mode. The options are:

* DES-CBC - This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key.

* 3DES-CBC - This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.

* AES-CBC-128 - This is a 2 bit cipherlist. It is based on symmetric-key algorithm that uses a 128-bit key with cipher-block chaining (CBC) as mode of operation.

* AES-CBC-256 - This is a 3 bit cipherlist. It is based on symmetric-key algorithm that uses a 256-bit key with cipher-block chaining (CBC) as mode of operation.

SSH MacList - Select the MAC list. The MAC list takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication. Both can be selected.

By default, the option HMAC-SHA1 is selected. The options are:

* HMAC-MD5 - HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code involving a cryptographic hash function in combination with a secret key

* HMAC-SHA1 - is a similar version to MD5 and works on 512 bit blocks

Max Packet size - Enter the maximum number of bytes allowed in an SSH transport connection. The SSH connection is allowed only if the packet size does not exceed the value configured, else it will be dropped. By default the maximum packet size is set as 32768. This value ranges between 1 and 32768.

3.12.2 SSH Traces

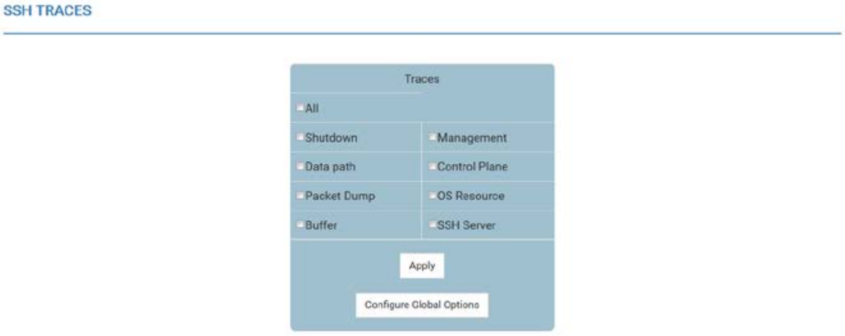


Fig: SSH Traces

The *SSH Traces* link opens the **SSH Traces** Page.
This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.
A 4 byte integer is used for enabling the level of tracing. Each bit in the 4 byte integer represents a particular level of trace.
System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages.

The debug messages are saved in the flash for technical support.
But the configuration in this page will be reset after reboot.

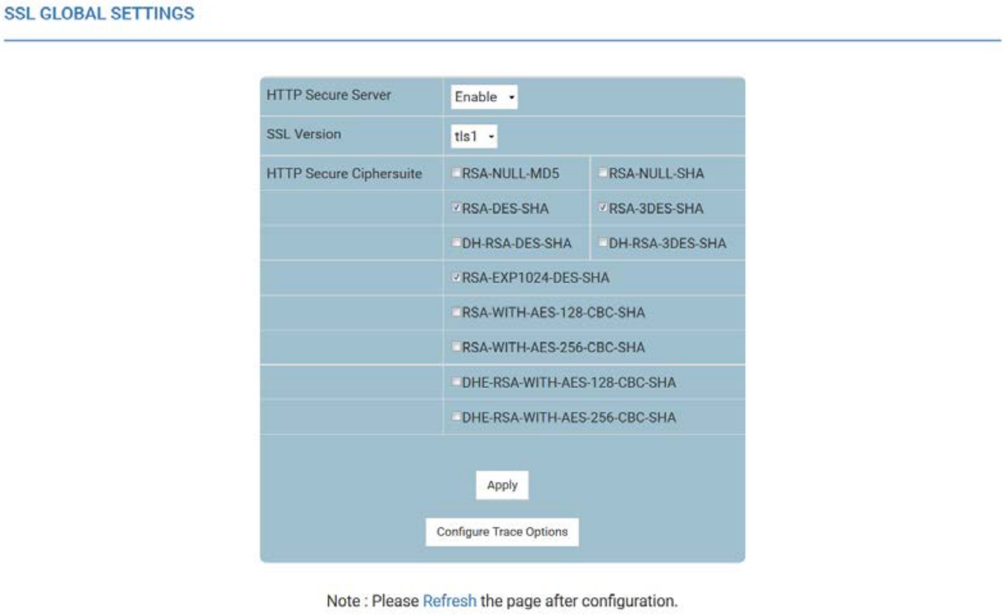
The table below lists the fields present in this page.
Traces - Select the traces for which debug statements is to be generated. The options are
* All - Generates debug statements for all traces
* Shutdown - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory
* Data Path - Generates debug statements for datapath.
* Packet Dump - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
* Buffer - Generates debug statements for traces with respect to allocation and freeing of Buffer.
* Management - Generates debug statements for management plane functionality traces.
* Control Plane - Generates debug statements for Control Plane functionality traces.
* OS Resource - Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers
* SSH Server - Generates debug statements while creating/openin/closing SSH server sockets and any failures to wake up SSH server sockets. Also during enabling /disbling of SSH server.

3.13 SSL

The *SSL* link allows you to configure the SSL settings for switch. User can configure SSL on the following three pages.

- SSL Global Settings
- SSL Digital Certificate
- SSL Traces

3.13.1 SSL Global Settings



SSL GLOBAL SETTINGS

HTTP Secure Server	Enable	
SSL Version	tls1	
HTTP Secure Ciphersuite	□ RSA-NULL-MD5	□ RSA-NULL-SHA
	☑ RSA-DES-SHA	☑ RSA-3DES-SHA
	□ DH-RSA-DES-SHA	□ DH-RSA-3DES-SHA
	☑ RSA-EXP1024-DES-SHA	
	□ RSA-WITH-AES-128-CBC-SHA	
	□ RSA-WITH-AES-256-CBC-SHA	
	□ DHE-RSA-WITH-AES-128-CBC-SHA	
	□ DHE-RSA-WITH-AES-256-CBC-SHA	

Note : Please Refresh the page after configuration.

Fig: SSL Global Settings

The *SSL Global Settings* link opens the **SSL Global Settings** Page.
This page allows the user to configure the local server and set initial default values for all virtual hosts running on this server.

The table below lists the fields present in this page.
HTTP Secure Server - Select the status of the HTTP secure server.
By default, Secure Server is set as Disable. The list contains:
* Enable - Enables secure HTTP in the system. When the server status is enabled, it establishes the secure layer in the network.
* Disable - Disables secure HTTP in the system.
SSL Version - Configure the SSL version.
By default, SSL version is set as tls1. The list contains:
* all - Allows configuration to both SSL3 and TLS1 SSL protocols. Server accepts all the connection and the https session is established.
* ssl3 - Configures SSL version 3 protocol.
* tls1 - Configures Transport Layer Security version 1 protocol.
HTTP Secure Ciphersuite - Select the cipher suite for providing the input. When an SSL connection is established, the client and server exchange information about which cipher suites they have in common.

By default the options RSA_3DES_SHA, RSA_DES_SHA and RSA_EXP1024_DES_SHA are selected. The options are:

* RSA-NULL-MD5 - cipher suites using RSA key exchange and offering no authentication combined with cipher suites using MD5.

* RSA-NULL-SHA - cipher suites using RSA key exchange and offering no authentication combined with cipher suites using SHA1.

* RSA-DES-SHA - cipher suites using RSA key exchange. and cipher suites using DES combined with cipher suites using SHA1.

* RSA-3DES-SHA - cipher suites using RSA key exchange and cipher suites using triple DES combined with cipher suites using SHA1.

* DH-RSA-DES-SHA - cipher suites using DH, including anonymous DH with cipher suites using RSA key exchange and cipher suites using DES combined with cipher suites using SHA1.

* DH-RSA-3DES-SHA - cipher suites using DH, including anonymous DH with cipher suites using RSA key exchange and cipher suites using triple DES combined with cipher suites using SHA1.

* RSA-EXP-1024-DES-SHA - cipher suites using RSA key exchange with export encryption algorithms. Including 40 and 56 bits algorithms and cipher suites using DES combined with cipher suites using SHA1.

* RSA-WITH-AES-128-CBC-SHA - cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard(AES) algorithms and cipher suites using SHA1.

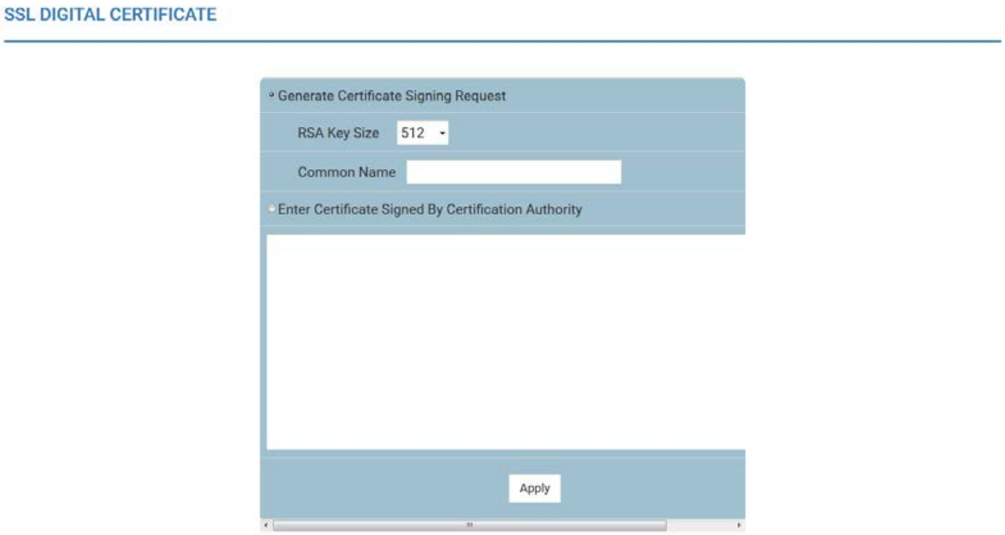
* RSA-WITH-AES-256-CBC-SHA - cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard(AES) algorithms and cipher suites using SHA1.

* DHE-RSA-WITH-AES-128-CBC-SHA - cipher suites using dhe, and cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard(AES) algorithms combined with cipher suites using SHA1.

* DHE-RSA-WITH-AES-256-CBC-SHA - cipher suites using dhe, and cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard(AES) algorithms combined with cipher suites using SHA1.

> The encryptions use these combinations to send /receive data in a secure manner.

3.13.2 SSL Digital Certificate



SSL DIGITAL CERTIFICATE

● Generate Certificate Signing Request

RSA Key Size 512

Common Name

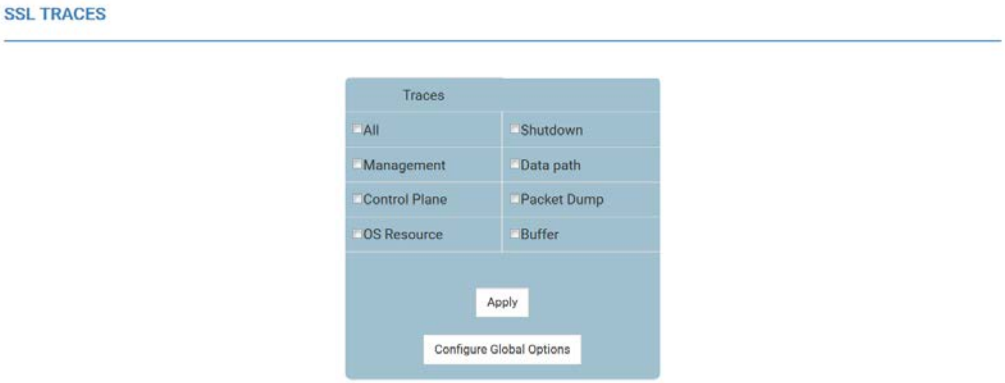
○ Enter Certificate Signed By Certification Authority

Fig: SSL Digital Certificate

The *SSL Digital Certificate* link opens the **SSL Digital Certificate** Page.
SSL digital certificates are offered to merchants, banks and organizations that collect personal information from their clients. These SSL Certificates ensure a safe transportation of data on the inter network in a remote location. SSL has encouraged E-commerce, which has grown many folds in the short period of time.
SSL Digital Certificate can be configured using auto-generation or manually enter the certificate details to obtain a certificate signed by certification authority.

The table below lists the fields present in this page.
Generate Certificate signing Request - Select to generate certificate based on the RSA key size and common name. The certificate is awarded to users who utilize the HTTPS protocol.
RSA Key Size - Select the desired Key size. The list contains:
* 512 - The key size is set as 512.
* 1024 - The key size is set as 1024.
> The RSA key size is enabled only if the Generate Certificate signing Request option is selected. Else, it is grayed out and cannot be configured.
Common Name Enter the details of the user requesting for the Digital Certificate.
> The Common name is enabled only if the Generate Certificate signing Request option is selected. Else, it is grayed out and cannot be configured.
Enter Certificate Signed by Certification Authority - Select to enter Certificate Signed by Certification Authority. The user manually enters the details of the certificate.

3.13.3 SSL Traces


SSL TRACES

Traces	
□ All	□ Shutdown
□ Management	□ Data path
□ Control Plane	□ Packet Dump
□ OS Resource	□ Buffer

Fig: SSL Traces

The *SSL Traces* link opens the **SSL Traces** Page.

This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.

A 4 byte integer is used for enabling the level of tracing. Each bit in the 4 byte integer represents a particular level of trace.

System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.

Traces - Select the traces for which debug statements is to be generated. The options are

* All - Generates debug statements for all traces.

* Management - Generates debug statements for Management Plane functionality traces.

* Control Plane - Generates debug statements for Control Plane functionality traces.

* OS Resource - Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers.

* Shut down - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory.

* Data Path - Generates debug statements for data path.

* Packet Dump - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.

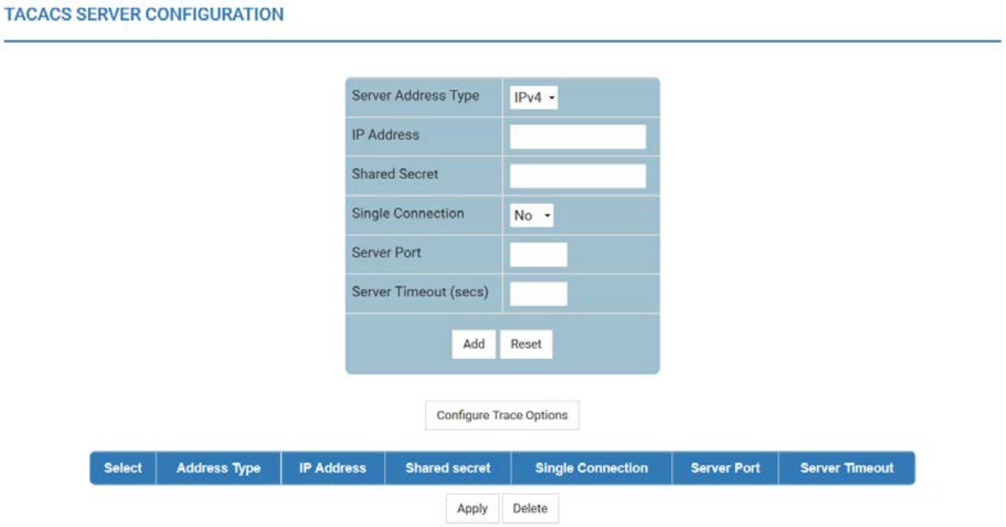
* Buffer - Generates debug statements for traces with respect to allocation and freeing of Buffer.

3.14TACACS

The *TACACS* link allows you to configure the TACACS settings for switch. User can configure TACACS on the following three pages.

- Tacacs Settings
- Tacacs AS
- Tacacs Traces

3.14.1 Tacacs Settings



TACACS SERVER CONFIGURATION

Server Address Type	IPv4
IP Address	
Shared Secret	
Single Connection	No
Server Port	
Server Timeout (secs)	

Select	Address Type	IP Address	Shared secret	Single Connection	Server Port	Server Timeout

Fig: TACACS Server Configuration

The *Tacacs Settings* link opens the **TACACS Server Configuration** Page.
This page allows the user to configure the TACACS server configuration.

The table below lists the fields present in this page.

Server Address Type - Select the address type of the TACACS+ server. By default, the server address type is set as IPV4.The list contains:

* IPV4 - Sets the address type of the server as Internet Protocol Version 4.

* IPV6 - Sets the address type of the server as Internet Protocol Version 6.

IP Address - Enter the IPv4 or IPv6 address of the TACACS+ server. The TACACS+ client interacts with the server having this IP address.

> This software allows maximum of 5 server information (IPv4 or IPv6) to be configured.

Shared Secret - Enter the secret key shared between the client and server (IPv4 or IPv6) for encryption and decryption.

Single Connection - Select whether single connect support is enabled/ disabled for the server. By default, Single Connection is set to No. The list contains:

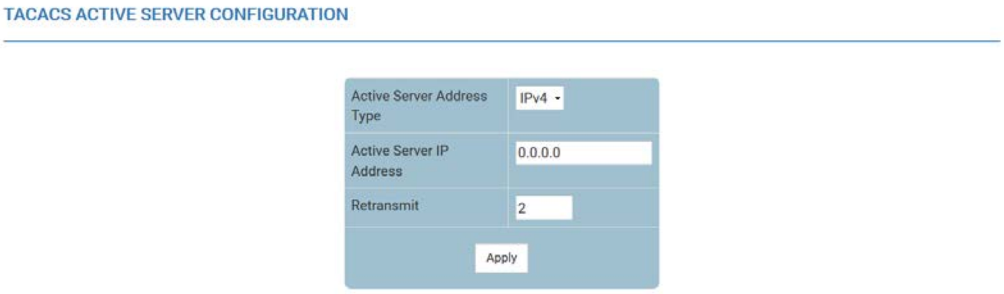
* Yes - Allows multiple sessions over a single TCP connection. Thus the authentication, authorization and accounting process are carried out in a single TCP connection.

* No - Does not allow the multiple sessions to handle over a single TCP connection. Thus the authentication, authorization and accounting are carried out in separate TCP connection.

Server Port - Enter the server port number for TACACS protocol. This value ranges between 0 and 65535. Default value for Server Port is 49 for IPv4 and 4949 for IPv6.

Server Timeout (secs) - Enter the timeout value within which the TACACS client expects a response from server. This value ranges between 1 and 255. The default value for Server Time out is 5 seconds. The TACACS client assumes that the primary server is down and gets connected with secondary server, after the expiry of this time.

3.14.2 Tacacs AS



TACACS ACTIVE SERVER CONFIGURATION

Active Server Address Type	IPv4
Active Server IP Address	0.0.0.0
Retransmit	2

Fig: TACACS Active Server Configuration

The *Tacacs AS* link opens the **TACACS Active Server Configuration** Page.
This page allows the user to set the TACACS server that should be used as primary server.

The table below lists the fields present in this page.
Active Server Address Type - Select the address type of the active server. The list contains:
* IPV4 - Sets the address type of the active server as Internet Protocol Version 4.
* IPV6 - Sets the address type of the active server as Internet Protocol Version 6.
Active Server IP Address - Enter the IP address of the TACACS server that should be set as primary server. Address 0.0.0.0 disables the configured active server.
Retransmit - Enter the number of times the TACACS client remote server searches the list of TACACS servers.
This value ranges between 1 and 5. Default value of retransmit is 2
If the TACACS client does not receive any response from the server for the given retransmit time, it searches and gets connected with the next server.

3.14.3 Tacacs Traces

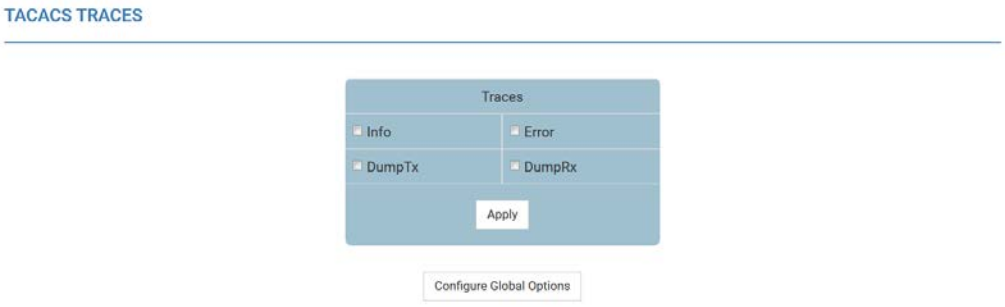


Fig: Tacacs Traces

The *Tacacs Traces* link opens the **Tacacs Traces** Page.

This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.

Traces - Select the traces for which debug statements is to be generated. The list contains:

* Info - Generates debug statements for informational messages

* Error - Generates debug statements for error messages

* DumpTx - Generates debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets.

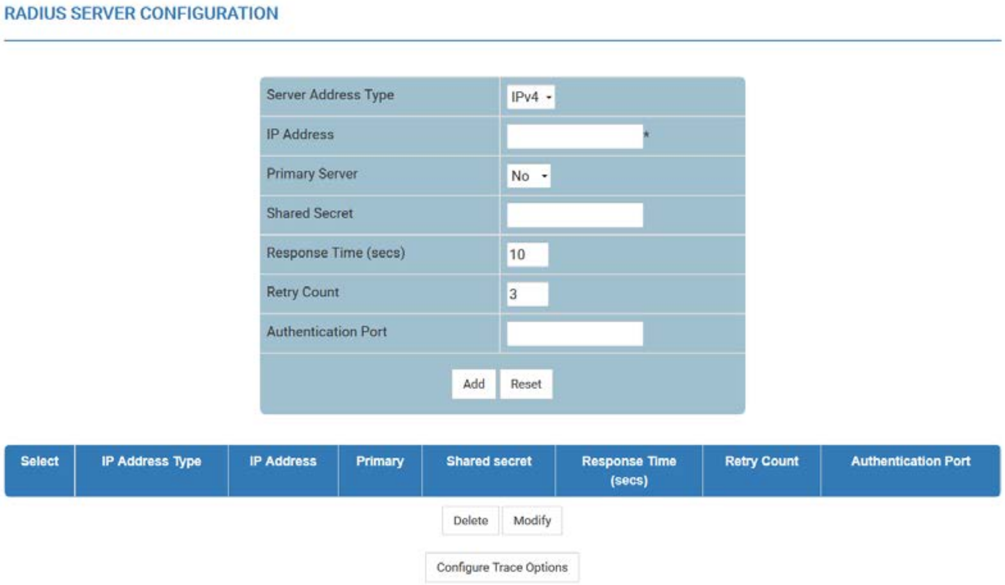
* DumpRx - Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets.

3.15 RADIUS

The *RADIUS* link allows you to configure the RADIUS settings for switch. User can configure RADIUS on the following two pages.

- Radius Server Config
- Radius Traces

3.15.1 Radius Server Config



RADIUS SERVER CONFIGURATION

Server Address Type	IPv4
IP Address	*
Primary Server	No
Shared Secret	
Response Time (secs)	10
Retry Count	3
Authentication Port	

Select	IP Address Type	IP Address	Primary	Shared secret	Response Time (secs)	Retry Count	Authentication Port

Fig: Radius Server Configuration

The *Radius Server Config* link opens the **Radius Server Configuration** Page.

This page allows the user to configure the Radius Server settings.

The table below lists the fields present in this page.

Server Address Type - Specifies the Radius server address type. Options are:

* IPV4 - Radius server address type is set as Internet Protocol Version 4, where a 32 bit address is used.

* IPV6 - Radius server address type is set as Internet Protocol Version 6, where a 128 bit address is used.

IP Address - Enter the IP Address of the Radius Server.

Primary Server - Select server type. is a primary server or not. Only one server can be configured as the primary server. Options are:

* Yes - Indicates the server type as primary server.

* No - Indicates the server type is not primary server.

Shared Secret - Enter the secret string, which is to be shared between the Radius Server and the Radius Client. The shared secret is the secret of the server to which the request was sent and from which the response was received.

Response Time (secs) - Enter the maximum time within which the Radius Server is expected to respond for a request from the Radius Client.

This value ranges between 1 and 120 seconds.

Retry Count - Enter the maximum number of times a request can be re-transmitted before getting response from the Radius Server. If the retransmit count has exceeded the configured maximum retransmissions, the packet and the user entry are deleted from the user request table and the error condition is logged.

This value ranges between 1 and 254.

Authentication Port - Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535.

3.15.2 Radius Traces

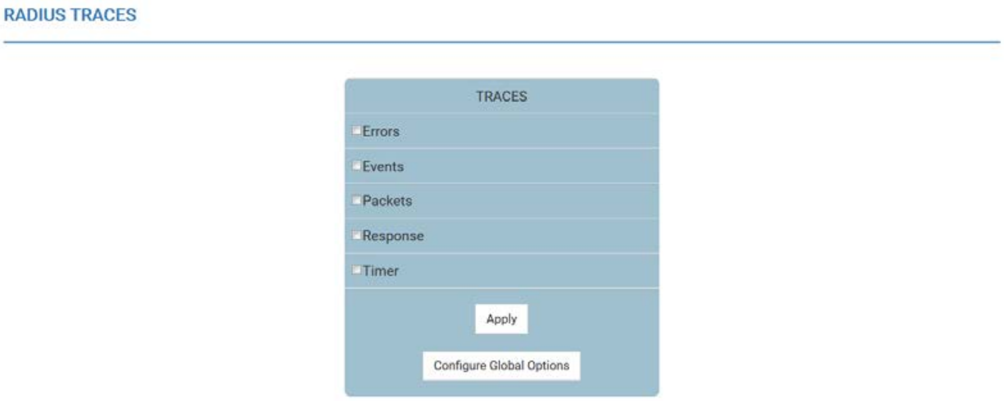


Fig: Radius Traces

The *Radius Traces* link opens the **Radius Traces** Page.

This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.

A FOUR BYTE integer is used for enabling the level of tracing. Each BIT in the four byte integer represents a particular level of Trace. Combination of levels is also allowed.

System errors such as memory allocation failures are notified by means of LOG messages and TRACE messages. Interface errors and protocol errors are notified by means of TRACE messages.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.

Traces Select the traces for which debug statements is to be generated. The options are

* Errors - Generates debug statements for all failure traces of the below mentioned traces.

* Events - Generates event debug statements. Generates debug statements for event handling traces. This trace is generated for event processing or response occurring with respect to radius.

* Packets - Generates packet debug statements. Generates debug statements for packets handling traces. This trace is generated for packet transmission or reception scenarios.

* Response - Generates response debug statements. This trace provides information about the response from the Radius server.

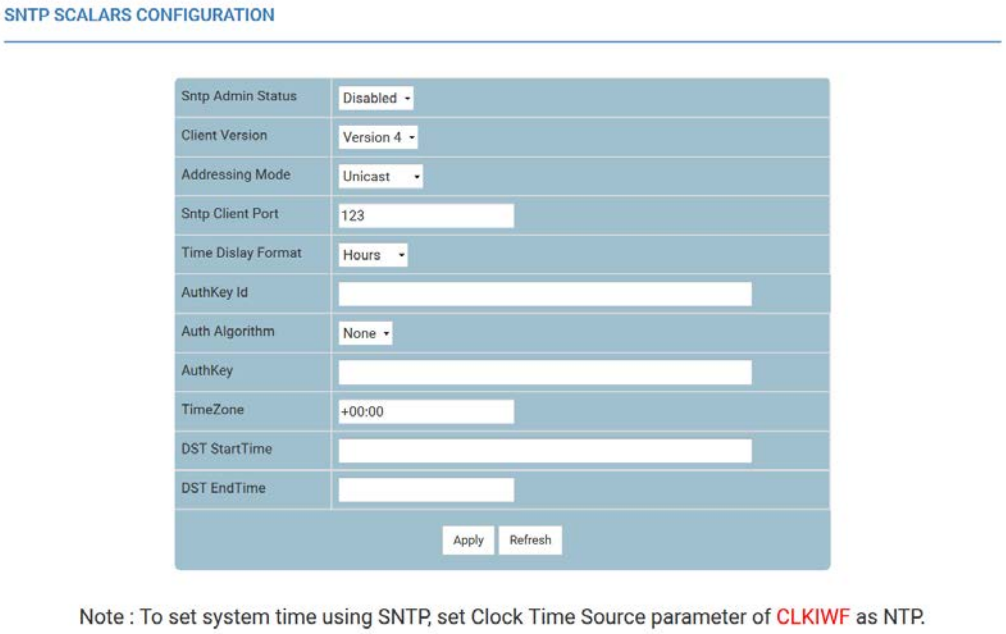
* Timer - Generates timer debug statements. This trace is generated for timer functionality.

3.16 SNTP

The *SNTP* link allows you to configure the SNTP settings for switch. User can configure SNTP on the following six pages.

- SNTP Scalars
- SNTP Unicast
- SNTP Broadcast
- SNTP Multicast
- SNTP AnyCast
- Clock Interworking

3.16.1 SNTP Scalars



SNTP SCALARS CONFIGURATION

Sntp Admin Status	Disabled
Client Version	Version 4
Addressing Mode	Unicast
Sntp Client Port	123
Time Dislay Format	Hours
AuthKey Id	
Auth Algorithm	None
AuthKey	
TimeZone	+00:00
DST StartTime	
DST EndTime	

Note : To set system time using SNTP, set Clock Time Source parameter of CLKIWF as NTP.

Fig: SNTP Scalars Configuration

The *SNTP Scalars* link opens the **SNTP Scalars Configuration** Page.
This page allows the user to configure the details of SNTP scalars.

The table below lists the fields present in this page.

Sntp Admin Status - Select the SNTP client module status

By default, this is Disabled. The list contains:

* Enabled - Enables the SNTP client module. On enabling, the server starts sending the request to the host for synchronisation.

* Disabled - Disables the SNTP client module.

> All the configurations are active only when the SNTP module is enabled.

Client Version - Select the SNTP client module version.

By Default it is set as Version 4. The list contains:

* Version 3 - Sets the SNTP client version as Version 3

* Version 4 - Sets the SNTP client version as Version 4

> All the SNTP requests are sent out with the current configured version number.

When required, the administrator can change the current version number.

Addressing Mode - Select the SNTP client addressing mode.

The default addressing mode is Unicast. The list contains:

* Unicast - SNTP client operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.

* Broadcast - SNTP client operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.

* Multicast -SNTP client operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.

* Anycast. - SNTP client operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses

Sntp Client Port - Enter the SNTP client port number. This value ranges between 1025 and 65535. The default value is 123.

Time Display Format - Select the time display format.

The default format is Hours. The list contains:

* Hours - Sets the time display as 24 hours format.

* Am/Pm - Sets the time display as 12 hours AM/PM format.

AuthKey Id - Enter the key identifier identifying the cryptographic key used to generate the message-authentication code.

Auth Algorithm - Select the SNTP authentication algorithm.

The default authentication algorithm is None. The list contains:

* None - The communication will be opened and no authorisation will be provided.

* md5 - MD5(Message Digest-5) verifies data integrity. MD5 is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.

AuthKey - Enter the authentication key that is used to implement NTP authentication.

TimeZone - Enter the system time zone with respect to UTC.

The format is (+/-)HH:MM. Where:

* +/- denotes the difference with the Greenwich Mean Time. + indicates forward time zone and - indicates backward time zone.

* HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.

* mm denotes the minutes. The value ranges from 00 to 59.

For example, the valid value is +05:30.

DST StartTime - Enter the DST (Daylight Saving Time) start time. The format is weekofmonth-weekofday-month,HH:MM. Where:

* weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.

* weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.

* month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

* HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.

* mm denotes the minutes. The value ranges from 00 to 59.

For example, the valid value is First-Sun-Jan,23:45.

> DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year.

DST EndTime - Enter the DST end time. The valid format is [weekofmonth-weekofday-month, HH:MM].

The format is weekofmonth-weekofday-month,HH:MM. Where:

* weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.

* weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.

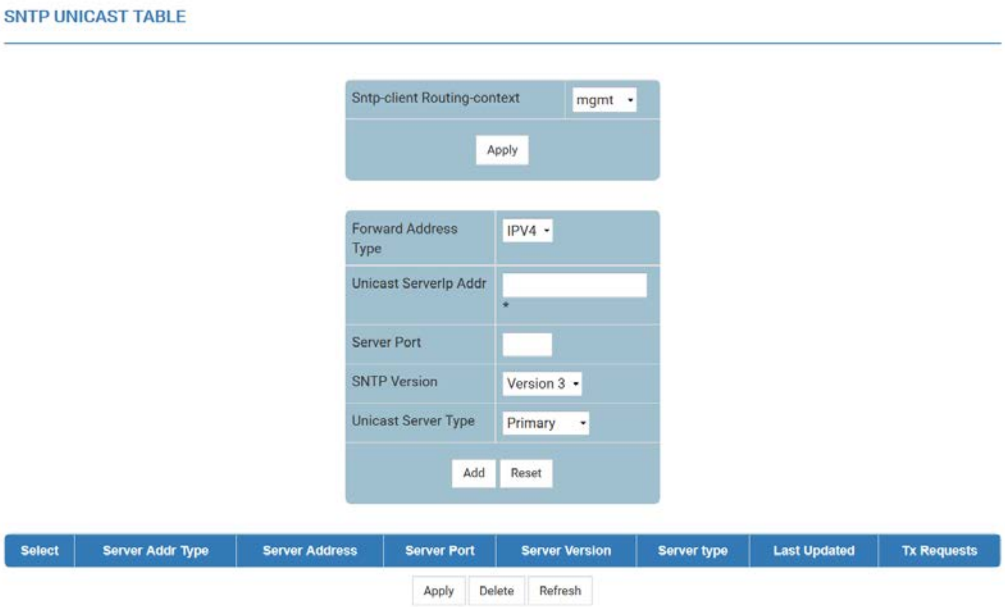
* month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

* HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.

* mm denotes the minutes. The value ranges from 00 to 59.

For example, the valid value is First-Mon-Jan,23:45.

3.16.2 SNTP Unicast



SNTP UNICAST TABLE

Sntp-client Routing-context	mgmt

Forward Address Type	IPV4
Unicast ServerIp Addr	*
Server Port	
SNTP Version	Version 3
Unicast Server Type	Primary

Select	Server Addr Type	Server Address	Server Port	Server Version	Server type	Last Updated	Tx Requests

Fig: SNTP Unicast Table

The *SNTP Unicast* link opens the **SNTP Unicast Table** Page.

This page allows the user to configure the SNTP unicast parameter.

The table below lists the fields present in this page.

Sntp-client Routing-context - Select routing context for Sntp-client.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Forward Address Type - Select the address type of the unicast server in the Unicast addressing mode. The list contains:

* IPV4 - Sets the address type of the unicast server as Internet Protocol Version 4

* IPV6 - Sets the address type of the unicast server as Internet Protocol Version 6

Unicast ServerIp Addr - Enter the unicast IPv4/IPv6 server address in the Unicast addressing mode.

Server Port - Enter the SNTP port on which the server is UP. The value ranges between 1025 and 65535. The default value is 123.

SNTP Version Select the SNTP version supported by the server. The list contains:

* Version 3 - Sets the SNTP version as version 3.

* Version 4- Sets the SNTP version as version 4.

Unicast Server Type - Select the Unicast server type. This flag is to distinguish between primary and secondary server. SNTP client sends request to different servers until it receives successful response. This flag tells the order in which to query the servers The list contains:

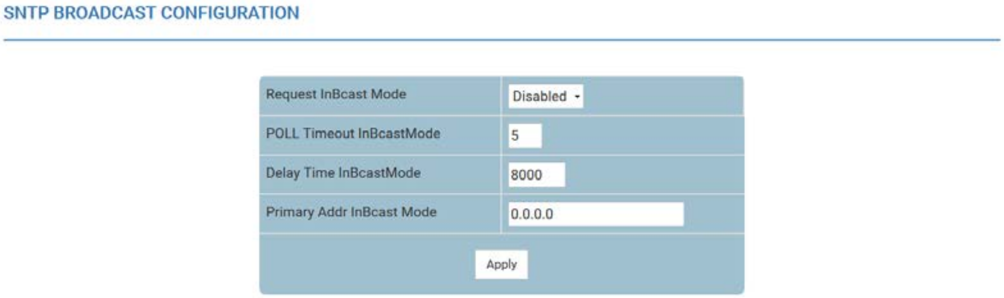
* Primary - Sets the unicast server typer as primary server.

* Secondary - Sets the unicast server typer as secondary server.

Last Updated - Specifies the local time when the system time was successful.

Tx Requests - Specifies the number of SNTP requests sent in the Unicast addressing mode.

3.16.3 SNTP Broadcast


SNTP BROADCAST CONFIGURATION

Request InBcast Mode	Disabled
POLL Timeout InBcastMode	5
Delay Time InBcastMode	8000
Primary Addr InBcast Mode	0.0.0.0

Fig: SNTP Broadcast Configuration

The *SNTP Broadcast* link opens the **SNTP Broadcast Configuration** Page.
This page allows the user to configure the SNTP Broadcast parameters.

The table below lists the fields present in this page.

Request InBcast Mode - Select the SNTP send request status in Broadcast mode.
By default, this is set as Disabled. The list contains:

* Enabled - Sents the SNTP request to the broadcast server to calculate the delay time.

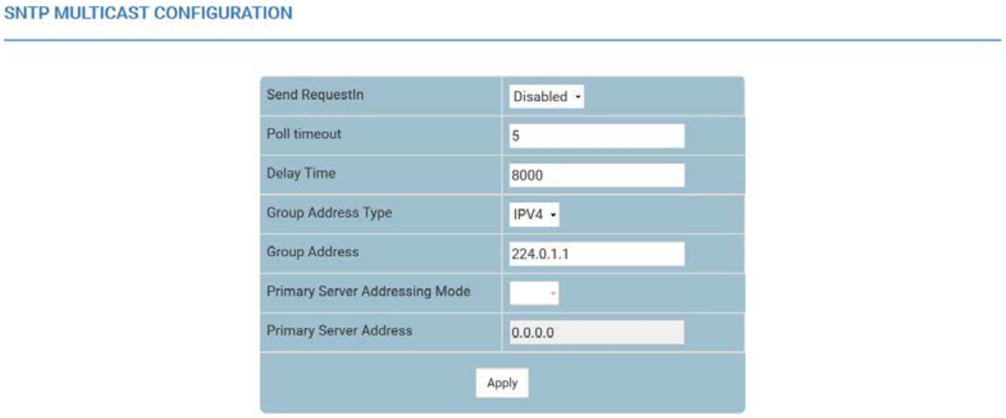
* Disabled - Does not send the SNTP request.

POLL Timeout InBcast Mode - Enter the number of seconds to wait for a response from a SNTP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds. The default value is 5 seconds.

Delay Time InBcast Mode - Enter the delay time when there is no response from the broadcast server. This value ranges between 1000 and 15000 microseconds. The default value is 8000 microseconds.

Primary Addr InBcast Mode - The primary server IP address learnt in Broadcast addressing mode. It is ready-only.

3.16.4 SNTP Multicast



SNTP MULTICAST CONFIGURATION

Send RequestIn	Disabled
Poll timeout	5
Delay Time	8000
Group Address Type	IPV4
Group Address	224.0.1.1
Primary Server Addressing Mode	
Primary Server Address	0.0.0.0

Fig: SNTP Multicast Configuration

The *SNTP Multicast* link opens the **SNTP Multicast Configuration** Page.
This page allows the user to configure the SNTP multicast parameters.

The table below lists the fields present in this page.

Send RequestIn - Select the SNTP send request status in Multicast mode.
By default, this is Disabled. The list contains:

* Enabled - Sends the SNTP request to the multicast server to calculate the delay time.

* Disabled - Does not send the SNTP request.

Poll timeout - Enter the number of seconds to wait for a response from a SNTP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds. The default value is 5 seconds.

Delay Time - Enter the delay time when there is no response from the multicast server. This value ranges between 1000 and 15000 microseconds. The default value is 8000 microseconds.

Group Address Type - Select the multicast group address type that can be configured by the administrator. The list contains:

* IPV4 - Sets the multicast group address type as Internet Protocol Version 4

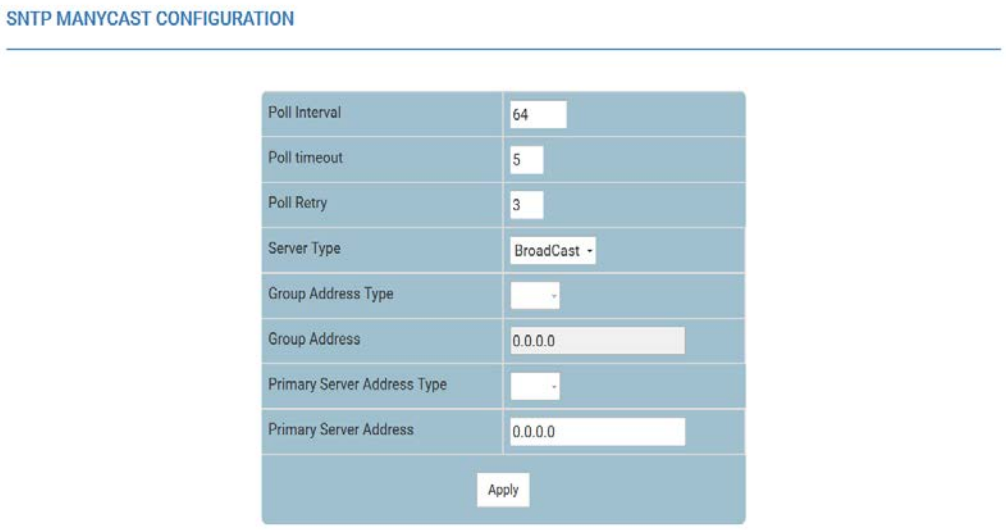
* IPV6 - Sets the multicast group address type as Internet Protocol Version 6

Group Address - Enter the multicast group address that can be configured by the administrator.

Primary Server Addressing Mode - Displays the address type of the primary server learnt in Multicast addressing mode. The list contains: IPV4 and IPV6.
This is a read-only field.

Primary Server Address - Displays the primary server IP address learnt in Multicast addressing mode. This is a read-only field. The default address is 0.0.0.0.

3.16.5 SNTP ManyCast



SNTP MANYCAST CONFIGURATION

Poll Interval	64
Poll timeout	5
Poll Retry	3
Server Type	BroadCast
Group Address Type	
Group Address	0.0.0.0
Primary Server Address Type	
Primary Server Address	0.0.0.0

Fig: SNTP Manycast Configuration

The *SNTP Manycast* link opens the **SNTP Manycast Configuration** Page.
This page allows the user to configure the SNTP manycast parameters.

The table below lists the fields present in this page.

Poll Interval - Configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 16 and 16284 in seconds.

Poll timeout - Configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds.

Poll Retry - Configures SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in seconds.

Server Type - Configures SNTP multicast or broadcast server address in manycast mode.
The list contains:
* broadcast - Configures SNTP broadcast server address in manycast mode.
* multicast - Configures SNTP multicast server address in manycast mode.

Group Address Type - Select the multicast group address type that can be configured by the administrator. The list contains:
* IPV4 - Sets the multicast group address type as Internet Protocol Version 4
* IPV6 - Sets the multicast group address type as Internet Protocol Version 6

Group Address - Enter the multicast group address that can be configured by the administrator.

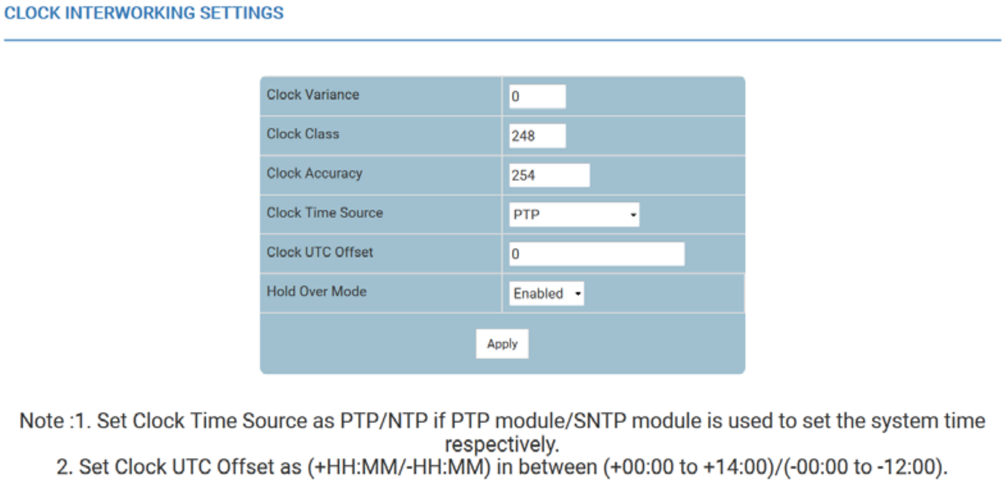
Primary Server Addressing Mode - Select the address type of the primary server learnt in Manycast addressing mode. The list contains:

* IPV4 - Sets primary server address type as Internet Protocol Version 4

* IPV6 - Sets primary server address type as Internet Protocol Version 6

Primary Server Address - Displays the primary server IP address learnt in Manycast addressing mode. The default address is 0.0.0.0.

3.16.6 Clock Interworking



CLOCK INTERWORKING SETTINGS

Clock Variance	0
Clock Class	248
Clock Accuracy	254
Clock Time Source	PTP
Clock UTC Offset	0
Hold Over Mode	Enabled

Note :1. Set Clock Time Source as PTP/NTP if PTP module/SNTP module is used to set the system time respectively.
2. Set Clock UTC Offset as (+HH:MM/-HH:MM) in between (+00:00 to +14:00)/(-00:00 to -12:00).

Fig: Clock Interworking Settings

The *Clock Interworking* link opens the **Clock Interworking Settings** Page.
The clock IWF module acts as a layer between the system clock and the protocol which synchronizes the system clock. This module selects the time source to set the system clock and maintains the information about the clock quality such as clock accuracy, class, and variance and so on. The Clock Interworking Settings page allows configuring the clock IWF parameters.

The table below lists the fields present in this page.
Clock Variance - Specifies the variance of the primary clock. This object reflects the value provisioned by the external source (NTP/SNTP/GPS) that synchronizes the system clock. Default value is 0 (minimum variance).
Clock Class - Specifies the class of the primary clock. This object reflects the value provisioned by the external source (NTP/SNTP/GPS) that synchronizes the system clock.
This value ranges between 0 and 255. Default value is 248.
Clock Accuracy - Specifies the accuracy of the primary clock. Clock accuracy is the mean of the time or frequency error between the clock under test and a perfect reference clock, over an ensemble of measurements.
This object reflects the value provisioned by the external source (NTP/SNTP/GPS) that synchronizes the system clock.
This value ranges between 0 and 255. Default value is 254.
Clock Time Source - Specifies the time source of the primary clock. The system clock is synchronized only through the specified source. Options are:
* None
* Atomic Clock

* GPS - Global Positioning System

* PTP - Precision Time Protocol

* NTP - Network Time Protocol

* Internal Oscillator

Default option is PTP.

Clock UTC Offset - Specifies the current UTC (Coordinated Universal Time) offset in scaled nanoseconds with respect to the system time.

This value ranges between 0 and 65535. Default value is 0.

Hold Over Mode - Specifies whether the system clock is in hold over specification. Options are:

* Enabled - The clock is in holdover mode.

* Disabled - The clock is in not in holdover mode.

Default option is Disabled.

A clock previously synchronized/syntonized to another clock (normally a primary reference or a master clock) but now free-running based on its own internal oscillator, whose frequency is being adjusted using data acquired while it had been synchronized/syntonized to the other clock. Such a clock is said to be in holdover mode.

3.17 Reboot

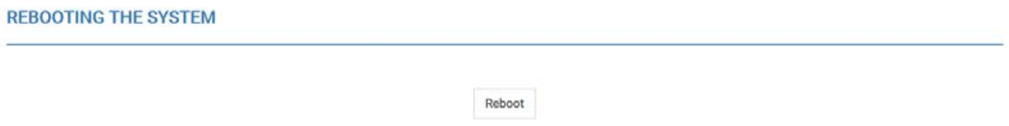
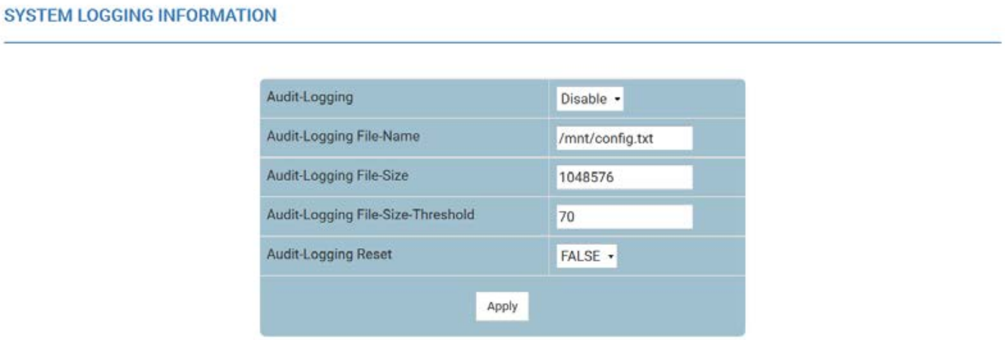

REBOOTING THE SYSTEM

Fig: Rebooting the System

The *Rebooting the System* link opens the **Rebooting the System** Page.

This page allows the user to reboot the target.

3.18 Audit Log



SYSTEM LOGGING INFORMATION

Audit-Logging	Disable ▾
Audit-Logging File-Name	/mnt/config.txt
Audit-Logging File-Size	1048576
Audit-Logging File-Size-Threshold	70
Audit-Logging Reset	FALSE ▾

Fig: System Logging information

The *System Logging info* link opens the **System Logging information** Page.

This page allows the user to configure the logging information. The Audit logs are used for creation and update of confidential information.

The table below lists the fields present in this page.

Audit Logging - Select the status of the module.

By default the Audit logging is set as Disable. The list contains:

* Enable - Enables the Audit logging and email alert features in the system

* Disable - Disables the Audit logging feature.

Audit Logging File name - Enter the name of the file that captures the log information. Default file name is /mnt/config.txt.

Audit Logging File Size - Enter the size of the log file that captures the information. Default file size is 1048576 bytes.

Audit Logging File Size Threshold - Enter the threshold value of the log storage space with respect to the maximum storage space size. The threshold value in percentage ranges between 1 and 99. Default threshold is 70.

Audit Logging Reset - Select the reset option in the module.

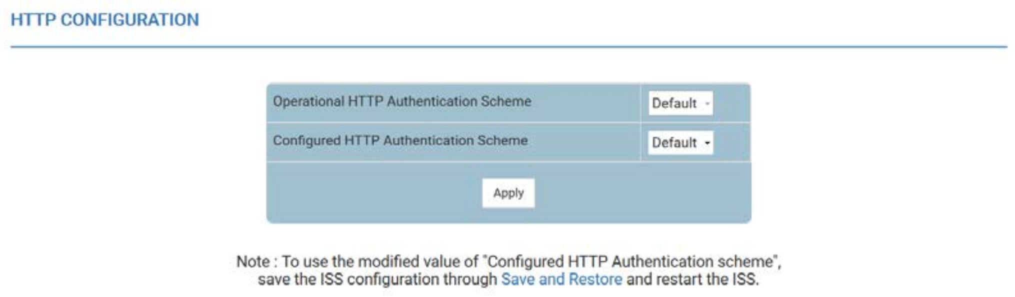
By default, the logging reset is set as False. The Syslog server IP Address and log level information are captured during configuration and stored in log file. The list contains:

* True - The syslog server IP address and log level information are flushed.

* False - Disables the Audit logging reset.

> The logging reset automatically reverts back to False, once the configuration is applied to the switch.

3.19HTTP



HTTP CONFIGURATION

Operational HTTP Authentication Scheme	Default
Configured HTTP Authentication Scheme	Default

Note : To use the modified value of "Configured HTTP Authentication scheme", save the ISS configuration through Save and Restore and restart the ISS.

Fig: HTTP Configuration

The *HTTP Configuration* link opens the **HTTP Configuration** Page.
This page allows the user to configure the HTTP related information.

The table below lists the fields present in this page.

Operational HTTP Authentication Scheme - Displays the Operational HTTP Authentication scheme which is used to authenticate all the HTTP client requests. By default, the Operational HTTP Authentication Scheme is set as Default.

Configured HTTP Authentication Scheme - Select the configurable HTTP Authentication scheme. By default, the Configured HTTP Authentication Scheme is set as Default.

* Default - Specifies Form-Based authentication mechanism

* Basic - Specifies the Basic HTTP Authentication scheme

* Digest - Specifies the Digest HTTP Authentication scheme

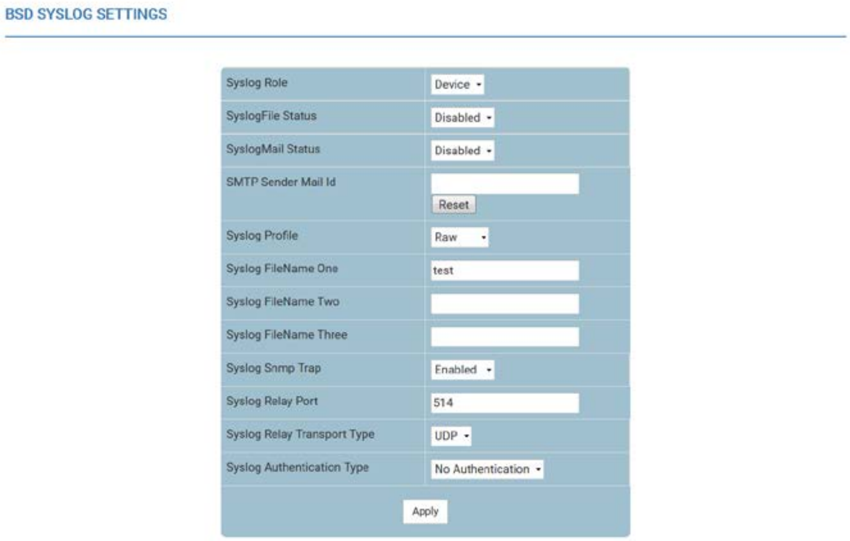
> To use the modified value of Configured HTTP
Authentication scheme, save the configuration through Save and Restore link and restart the switch. Also restart the browser and clear all the private data, saved session information and cache from the browser.

3.20BSD Syslog

The *BSD Syslog* link allows you to configure the Syslog settings for switch. User can configure BSD Syslog on the following five pages.

- SYSLOG ScalarsConf
- SYSLOG Logging
- SYSLOG FileTable
- SYSLOG MailTable
- SYSLOG FwdTable

3.20.1 SYSLOG ScalarsConf



BSD SYSLOG SETTINGS

Syslog Role	Device
SyslogFile Status	Disabled
SyslogMail Status	Disabled
SMTP Sender Mail Id	
Syslog Profile	Raw
Syslog FileName One	test
Syslog FileName Two	
Syslog FileName Three	
Syslog Snmp Trap	Enabled
Syslog Relay Port	514
Syslog Relay Transport Type	UDP
Syslog Authentication Type	No Authentication

Fig: BSD Syslog Settings

The *SYSLOG ScalarsConf* link opens the **BSD Syslog Settings** Page.

This page allows the user to configure the BSD syslog settings.

The table below lists the fields present in this page.

Syslog Role - Select the syslog role.

By default it is set as Device. The list contains:

* Device - Generates and forwards the syslog message.

* Relay - Receives, generates and forwards the syslog messages. Checks whether the received packet is as per BSD Syslog format. If not, makes the message to BSD Syslog format and forwards.

SyslogFile Status - Select the syslog file storage to log the status in the local storage path.

By default, the status is Disabled. This list contains are:

* Enabled - Sets the syslog local storage as enabled.

* Disabled - Sets the syslog local storage as disabled.

SyslogMail Status - Select the syslog mail storage.

By default, the status is Disabled. The list contains:

* Enabled - Enables the syslog mail storage.

* Disabled - Disables the syslog mail storage.

SMTP Sender Mail Id - Enter the sender mail ID to which email alerts should be sent using SMTP (Simple Mail Transfer Protocol). The user can customize it to add support for specific event for which email alerts should be sent.

This value is a string of size varying between 1 and 100.

Syslog Profile - Select the syslog profile for beep.

By default, the beep profile is Raw. The list contains.

* Raw - Raw syslog profile.

* Cooked - Cooked syslog profile.

Syslog FileName One - Enter the first file where the syslog can store the messages locally. This is a string of maximum size 32.

Syslog FileName Two - Enter the second file where the syslog can store the messages locally. This is a string of maximum size 32.

Syslog FileName Three - Enter the third file where the syslog can store the messages locally. This is a string of maximum size 32.

Syslog Snmp Trap - Select the Syslog SNMP server up or down traps to be generated when connectivity fails. By default syslog SNMP trap is selected as Enabled. The list contains:

* Enabled - Generates trap whenever connectivity to the external server collecting logs is lost.

* Disabled - Does not generate Syslog SNMP server up or down traps.

Syslog Relay Port - Enter the port in which the relay listens irrespective of the transport type. The relay opens the socket and listens on the configured port. This value ranges between 0 and 65535. Default value is 514.

Syslog Relay Transport Type - Select the transport protocol to be used by the relay for receiving syslog messages.

By default, transport type is set as UDP. The list contains:

* UDP - Relay receives syslog messages through UDP socket.

* TCP - Relay receives syslog messages through TCP socket.

Syslog Authentication Type - Select the authentication mode to be used for sending E-mail alerts to the mail server configured.

The list contains:

* No Authentication - E-mail alerts are sent without authentication.

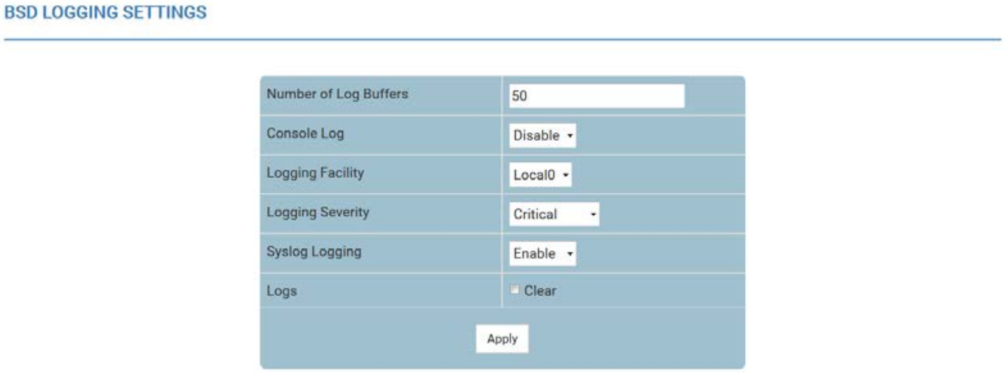
* AUTH LOGIN - E-mail alerts are sent after authenticating the user. The authentication is done by sending the BASE64 encoded username and password.

* AUTH PLAIN - E-mail alerts are sent after authenticating the user. The authentication is done by sending the BASE64 encoded username and password in a single statement.

* CRAM MD5 - E-mail alerts are sent after authenticating the user. The authentication is done by sending the BASE64 encoded username and a 32 byte HMAC MD5 digest.

* DIGEST MD5 - E-mail alerts are sent after authenticating the user. The authentication is done by sending the BASE64 encoded digest response calculated using the username, password, realm string and the nonce.

3.20.2 SYSLOG Logging



BSD LOGGING SETTINGS

Number of Log Buffers	50
Console Log	Disable
Logging Facility	Local0
Logging Severity	Critical
Syslog Logging	Enable
Logs	□ Clear

Fig: BSD Logging Settings

The *SYSLOG Logging* link opens the **BSD Logging Settings** Page.
This page log only particular kind of syslog messages and group those messages under respective facilities for audit purpose allows the user to configure the BSD syslog settings.

The table below lists the fields present in this page.
Number of Log Buffers - Enter the number of logs and email alert messages that can be stored in a local buffer for the syslog messages. This value ranges between 1 and 200. Default value is 50.
Console Log - Select whether the logs and email alert messages should be displayed in the console while being sent to the server.
By default, console log option is set as Enable. The list contains:
* Enable - Sends the log and email alert messages to the server and it will be displayed in the console also.
* Disable - Sends the log and email alert messages to the server alone and it will not be displayed in the console.
Logging Facility - Select the facility level used for storing the logs and email alert messages.
The facility refers to different general classification of the messages.
By default, the facility is set as Local0. The list contains:
* Local0 - Reserved local use facility
* Local1 - Reserved local use facility
* Local2 - Reserved local use facility
* Local3 - Reserved local use facility
* Local4 - Reserved local use facility
* Local5 - Reserved local use facility
* Local6 - Reserved local use facility

* Local7 - Reserved local use facility

Logging Severity - Select the severity level for the syslog messages to be logged. The list contains:

* Emergency - Log messages that represent panic condition.
* Alert - Log messages that require immediate attention.
* Critical - Log messages that represent critical error.
* Error - Log error messages.
* Warning - Log warning messages.
* Notice - Log messages that represent significant condition but not errors.
* Info - Log informational messages.
* Debug - Log debug messages

Syslog Logging - Select whether the syslog service is to be enabled.

By default, syslog service is set as Enable. The list contains:

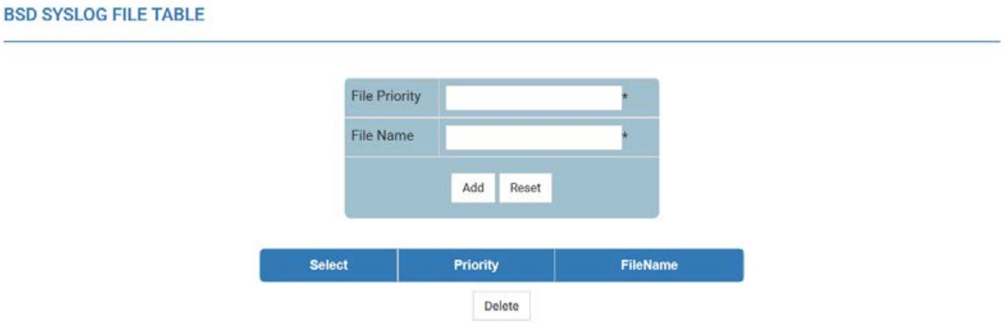
* Enable - Enables the syslog feature in the system. The syslog messages and email alert messages are logged in the system.
* Disable - Disables the syslog feature in the system. The syslog messages and email alert messages are not logged in the system.

Logs - Select the Clear facility to delete the logs buffered in the system.

By default, the check box is not selected.

> Once the buffered logs are cleared, the check box changes to the default status (this is, the check box is not selected).

3.20.3 SYSLOG FileTable


BSD SYSLOG FILE TABLE

File Priority	*
File Name	*

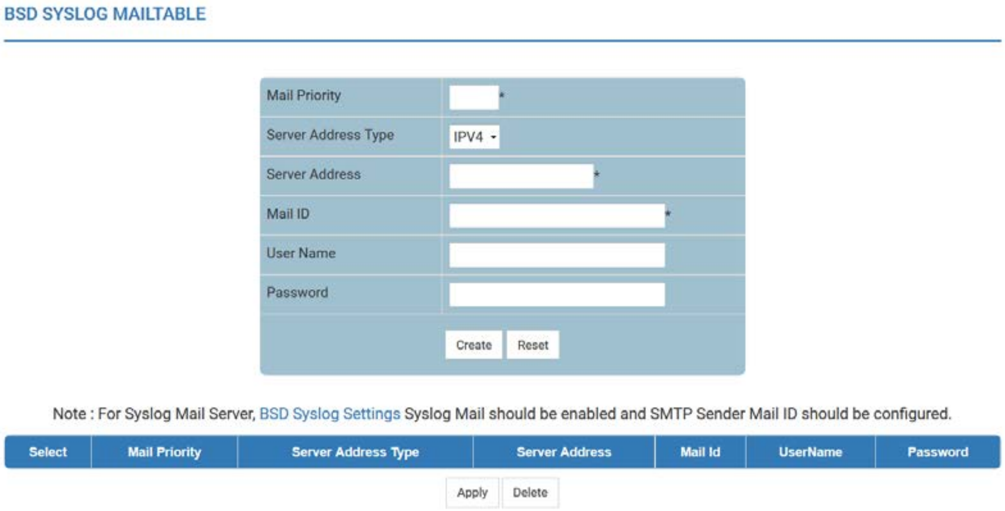
Select	Priority	FileName

Fig: BSD Syslog File Table

The *SYSLOG FileTable* link opens the **BSD Syslog File Table** Page.
This page allows the user to configure the BSD syslog file table settings.

The table below lists the fields present in this page.
File Priority - Enter the priority for which the log messages should be written in file. This value ranges between 0 and 191.
File Name - Enter the file name to which the syslog message is written.

3.20.4 SYSLOG MailTable


BSD SYSLOG MAILTABLE

Mail Priority	*
Server Address Type	IPV4
Server Address	*
Mail ID	*
User Name	
Password	

Note : For Syslog Mail Server, BSD Syslog Settings Syslog Mail should be enabled and SMTP Sender Mail ID should be configured.

Select	Mail Priority	Server Address Type	Server Address	Mail Id	UserName	Password

Fig: BSD Syslog MailTable

The *SYSLOG MailTable* link opens the **BSD Syslog MailTable** Page.

This page allows the user to configure the BSD syslog Mail Table settings.

The table below lists the fields present in this page.

Mail Priority - Enter the priority which is to be mailed. This value ranges between 0 and 191.

Server Address Type - Select the mail server address type. The list contains:

* IPV4 - Sets the Server Address Type as Internet Protocol Version 4

* IPV6 - Sets the Server Address Type as Internet Protocol Version 6

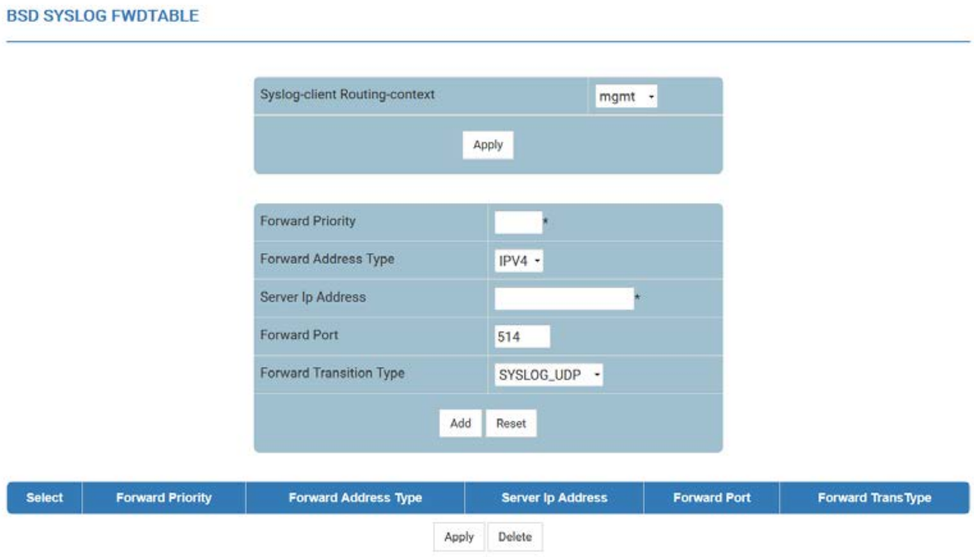
Server Address - Enter the mail server IP.

Mail ID - Enter the receiver mail ID.

User Name - Enter the user name of the account in the mail server to which the mails to be sent. The user name is used only if an authentication method is configured for the system. The user name is not used for sending mails, if Syslog Authentication Type is set as No Authentication. The maximum allowed size in 64 characters.

Password - Enter the password to authenticate the user name in the mail server. The password is used only if a valid authentication method is configured for the system. The password is not used for sending mails, if Syslog Authentication Type is set as No Authentication. The maximum allowed size in 64 characters.

3.20.5 SYSLOG FwdTable



BSD SYSLOG FWDTABLE

Syslog-client Routing-context	mgmt

Forward Priority	*
Forward Address Type	IPV4
Server Ip Address	*
Forward Port	514
Forward Transition Type	SYSLOG_UDP

Select	Forward Priority	Forward Address Type	Server Ip Address	Forward Port	Forward TransType

Fig: BSD Syslog FwdTable

The *SYSLOG FwdTable* link opens the **BSD Syslog FwdTable** Page.

This page allows the user to configure the syslog forward table settings.

The table below lists the fields present in this page.

Syslog-client Routing-context - Select routing context for Syslog-client.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Fwd Priority - Enter the priority which is to be forwarded to the desired server. This value ranges between 0 and 191.

Forward Address Type - Select the address type of the server. The list contains:

* IPV4 - Sets the forward address type as Internet Protocol Version 4

* IPV6 - Sets the forward address type as Internet Protocol Version 6.

Server Ip Address - Enter the server IP to which the syslog messages is to be forwarded.

Forward Port - Enter the port through which it can send the syslog message. This value ranges between 0 and 65535. Default value is 514.

Forward Transition Type - Select the transport type using which it can send syslog message. The default transition type is SYSLOG_UDP. The list contains:

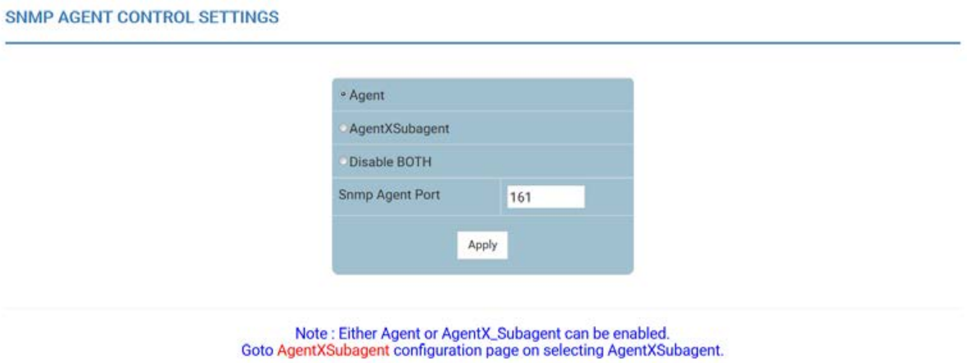
* SYSLOG_UDP - Sets the forward transition type as SYSLOG_UDP.

* SYSLOG_TCP- Sets the forward transition type as SYSLOG_TCP.

* SYSLOG_BEEP- Sets the forward transition type as SYSLOG_BEEP.

3.21SNMP

The SNMP is a widely deployed protocol that is commonly used to monitor and manage network devices. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.



SNMP AGENT CONTROL SETTINGS

● Agent

○ AgentXSubagent

○ Disable BOTH

Snmp Agent Port: 161

Note : Either Agent or AgentX_Subagent can be enabled.
Goto AgentXSubagent configuration page on selecting AgentXSubagent.

Fig: SNMP Agent Control Settings

The *Agent Control Settings* link opens the **SNMP Agent Control Settings** Page.
This page allows the user to configure SNMP Agent Control Settings.

The table below lists the fields present in this page.

Agent - Select Agent to enable the SNMP Agent. This allows the software to directly interface with the managed modules to configure and monitor them.
By default, this is enabled.

AgentXSubagent - Select AgentXSubagent to enable the SNMP Agent X Subagent.
* If this is enabled, the sub-agent registers and communicates with the master agent.
* If this is disabled, the sub-agent de-registers with the master agent and does not communicate with the master agent at all
By default, this is disabled
> On selecting this option, click on the link AgentXSubagent at the bottom of the form to view the Agent X Subagent Configuration page.

Disable BOTH - Select Disable BOTH to disable both SNMP Agent and Agent X Subagent.

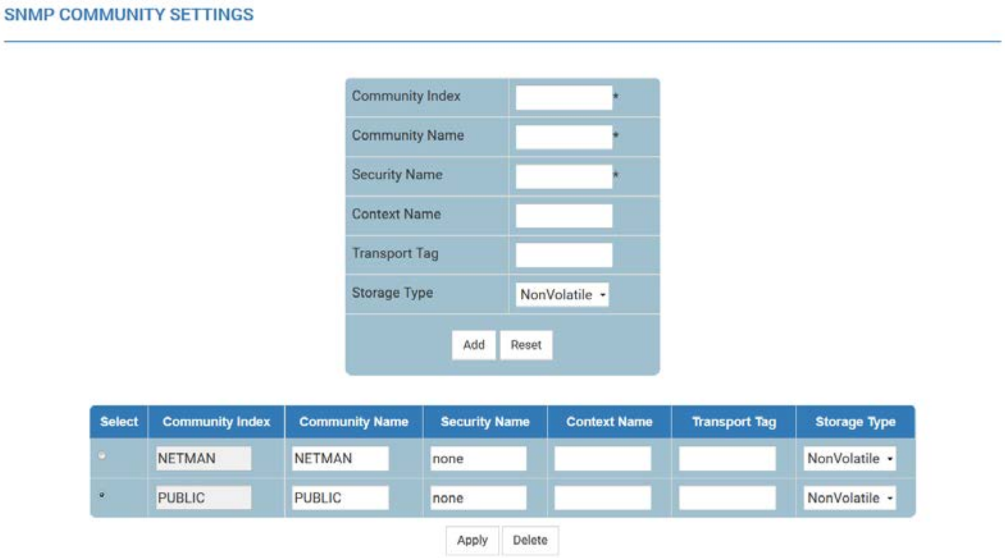
Snmp Agent Port - Enter the SNMP Agent Port number on which snmp agent listens. This value ranges between 1 and 65535.
This value can be entered only if Agent is selected.
This field is greyed out for AgentXsubagent and Disable Both option.
The default value is 161.

3.22 SNMP AGENT

The *SNMP AGENT* link allows you to configure the SNMP AGENT settings for switch. User can configure SNMP AGENT on the following ten pages.

- Community
- Group
- Group Access
- View
- Target Address
- TargetParameter
- Filter Profile
- User
- Trap Manager
- Filter Conf

3.22.1 Community


SNMP COMMUNITY SETTINGS

Community Index	*
Community Name	*
Security Name	*
Context Name	
Transport Tag	
Storage Type	NonVolatile

Select	Community Index	Community Name	Security Name	Context Name	Transport Tag	Storage Type
○	NETMAN	NETMAN	none			NonVolatile
●	PUBLIC	PUBLIC	none			NonVolatile

Fig: SNMP Community Settings

The *Community* link opens the **SNMP Community Settings** Page.

This page allows the user to add new community configuration to the table and delete existing community configuration from the same

The table below lists the fields present in this page.

Community Index - Enter the Index to the community table. The communities NETMAN and PUBLIC are created, once the switch is started to provide SNMP access to the switch.

Community Name - Enter the community name. The communities NETMAN and PUBLIC are created, once the switch is started to provide SNMP access to the switch.

Security Name - Enter the security name. Default security name is None.

Context Name - Enter the context name. Default context name is Null.

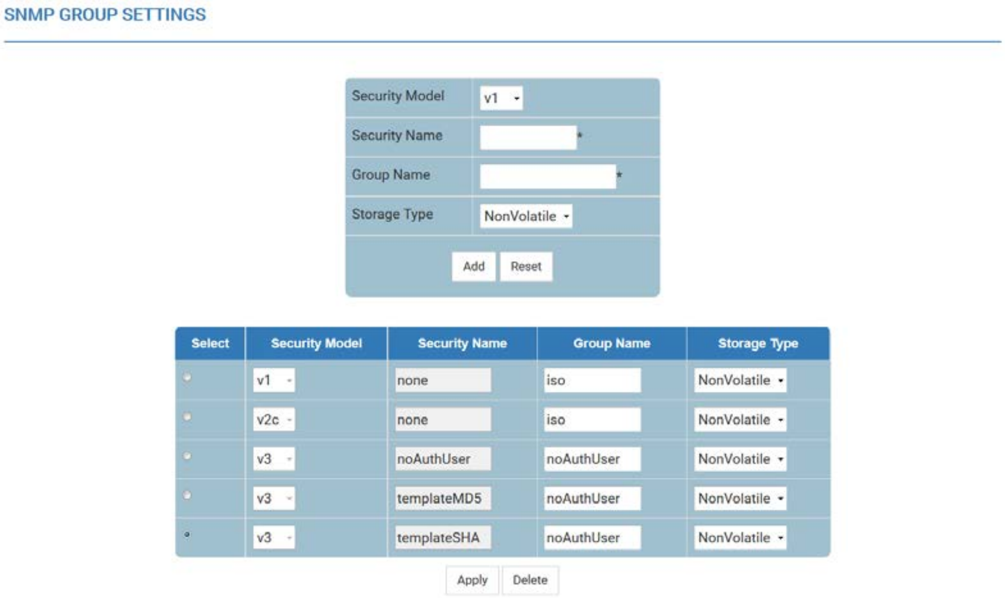
Transport Tag - Enter the transport tag. Default transport tag is Null.

Storage Type - Select the required Storage type for the community. Default storage type is Volatile. The list contains:

* Volatile - Sets the storage type as temporary and erases the configuration setting on restarting the system.

* Non Volatile - Sets the storage type as permanent and saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.2 Group


SNMP GROUP SETTINGS

Security Model	v1
Security Name	*
Group Name	*
Storage Type	NonVolatile

Select	Security Model	Security Name	Group Name	Storage Type
○	v1	none	iso	NonVolatile
○	v2c	none	iso	NonVolatile
○	v3	noAuthUser	noAuthUser	NonVolatile
○	v3	templateMD5	noAuthUser	NonVolatile
●	v3	templateSHA	noAuthUser	NonVolatile

Fig: SNMP GROUP Settings

The *Group* link opens the **SNMP GROUP Settings** Page.

This page allows the user to configure the SNMP Group Settings

The table below lists the fields present in this page.

Security Model - Select the version of the SNMP. The list contains:

* v1 - Sets the SNMP version as Version 1.

* v2c - Sets the SNMP version as Version 2.

* v3 - Sets the SNMP version as Version 3.

Security Name - Enter the security name of the group.

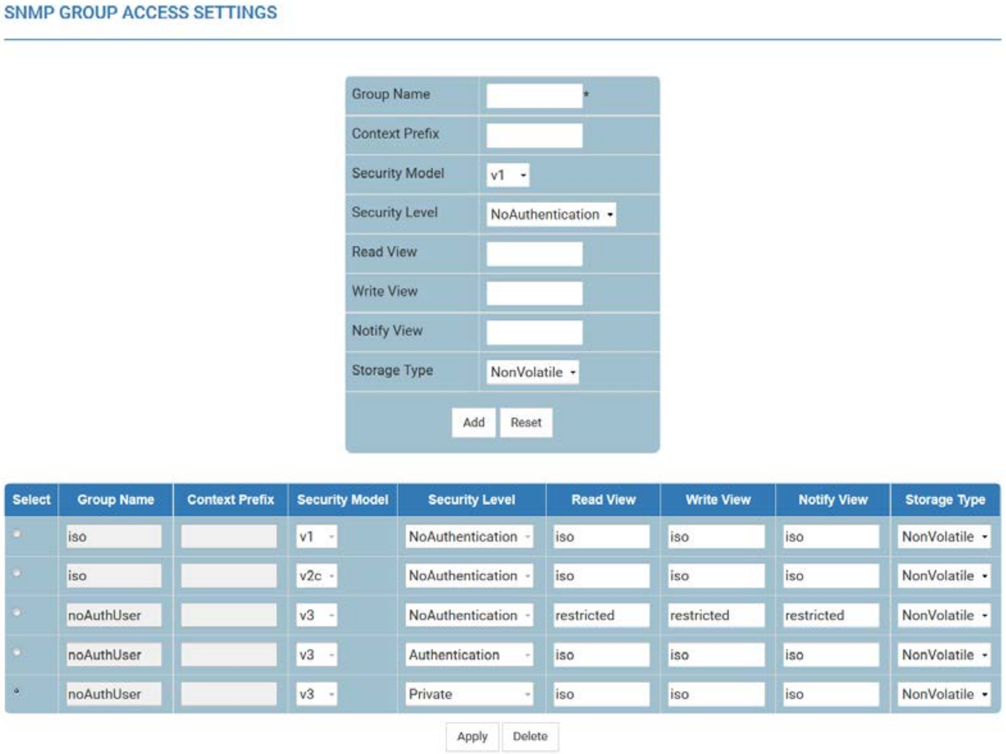
Group Name - Enter the name of the SNMP group. The SNMP groups iso and initial are created, once the switch is started.

Storage Type - Select the required Storage type for the group entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Stes the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.3 Group Access



SNMP GROUP ACCESS SETTINGS

Group Name	*
Context Prefix	
Security Model	v1
Security Level	NoAuthentication
Read View	
Write View	
Notify View	
Storage Type	NonVolatile

Select	Group Name	Context Prefix	Security Model	Security Level	Read View	Write View	Notify View	Storage Type
○	iso		v1	NoAuthentication	iso	iso	iso	NonVolatile
○	iso		v2c	NoAuthentication	iso	iso	iso	NonVolatile
○	noAuthUser		v3	NoAuthentication	restricted	restricted	restricted	NonVolatile
○	noAuthUser		v3	Authentication	iso	iso	iso	NonVolatile
●	noAuthUser		v3	Private	iso	iso	iso	NonVolatile

Fig: SNMP GROUP Access Settings

The *Group Access* link opens the **SNMP GROUP Access Settings** Page.

This page allows the user to configure SNMP Group Access Settings.

> A SNMP Group has to be created prior to the Group Access configuration. The groups that are created in the SNMP Group Settings section will be displayed in the bottom form of this panel.

The table below lists the fields present in this page.

Group Name - Enter the name of the group. The maximum size is 32.

Context Prefix - Enter the name of the context. It is defined in VACM table of RFC 3415. The maximum size is 32.

Security Model - Select the version of the SNMP. The list options are:

* v1 - Sets the SNMP version as Version 1.

* v2c - Sets the SNMP version as Version 2.

* v3 - Sets the SNMP version as Version 3.

Security Level - Select the version of the SNMP. The list contains:

* NoAuthentication - Sets no authentication

* Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.

* Private - Sets both authentication and privacy.

Read View - Enter the read view identifier from which the user can read the data The maximum size is 32.

Write View - Enter the write view identifier from which the user has both the read and write access. The maximum size is 32.

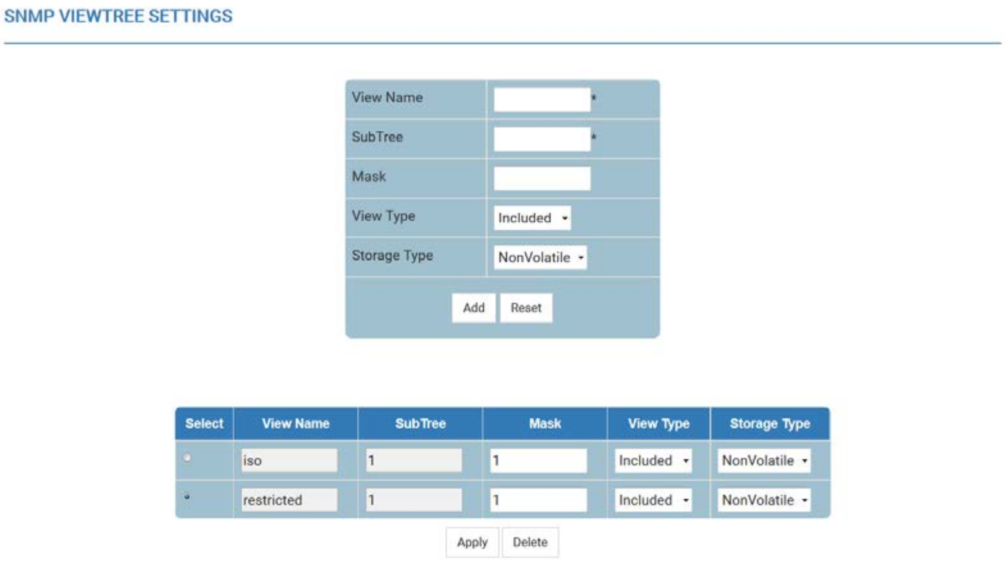
Notify View - Enter the notify view identifier. From this identifier number the changes made will be noted and sent to a destination through a tag. The maximum size is 32.

Storage Type - Select the required Storage type for the group access entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.4 View



SNMP VIEWTREE SETTINGS

View Name	*
SubTree	*
Mask	
View Type	Included
Storage Type	NonVolatile

Select	View Name	SubTree	Mask	View Type	Storage Type
○	iso	1	1	Included	NonVolatile
●	restricted	1	1	Included	NonVolatile

Fig: SNMP ViewTree Settings

The *View* link opens the **SNMP ViewTree Settings** Page.

This page allows the user to configure the SNMP ViewTree Settings.

> A SNMP Group and SNMP Access settings have to be created prior to the Group View configuration.

The table below lists the fields present in this page.

View Name - Enter the View Name for which the view details are to be configured.

SubTree - Enter the Sub Tree value for the particular view.

Mask - Enter the Mask value for the particular view.

View Type - Select the View Type. The list contains:

* Included - Allows access to the subtree.

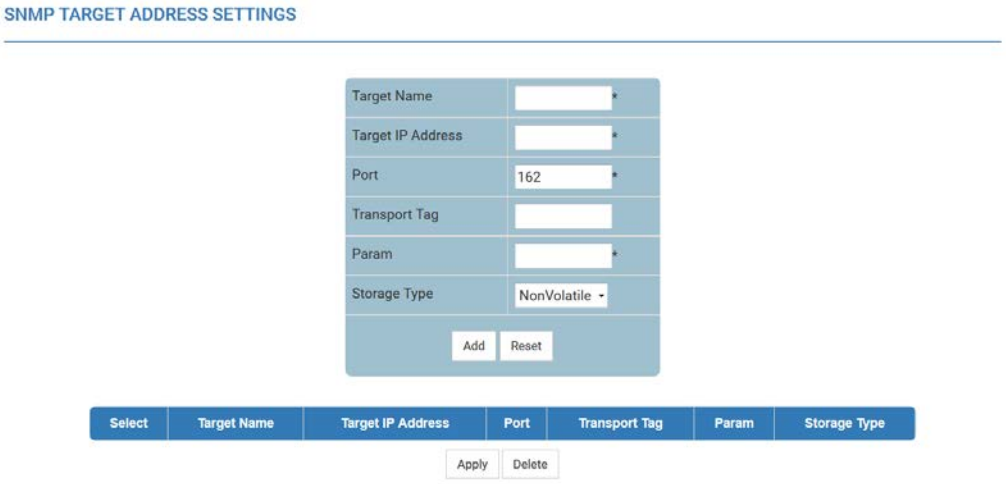
* Excluded - Denies access to the subtree.

Storage Type Select the required Storage type for the view tree entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.5 Target Address



SNMP TARGET ADDRESS SETTINGS

Target Name	*
Target IP Address	*
Port	162 *
Transport Tag	
Param	*
Storage Type	NonVolatile

Select	Target Name	Target IP Address	Port	Transport Tag	Param	Storage Type

Fig: SNMP Target Address Settings

The *Target Address* link opens the **SNMP Target Address Settings** Page.
This page allows the user to configure the SNMP Target Address Settings information

The table below lists the fields present in this page.

Target Name - Enter a unique identifier of the Target. The maximum size is 32.

Target IP Address - Enter a target address to which the generated SNMP notifications are sent.

Port - Enter the port number through which the generated SNMP notifications are sent to the target address.

Transport tag - Enter the tag identifier that is used to select the target address for the SNMP notifications.

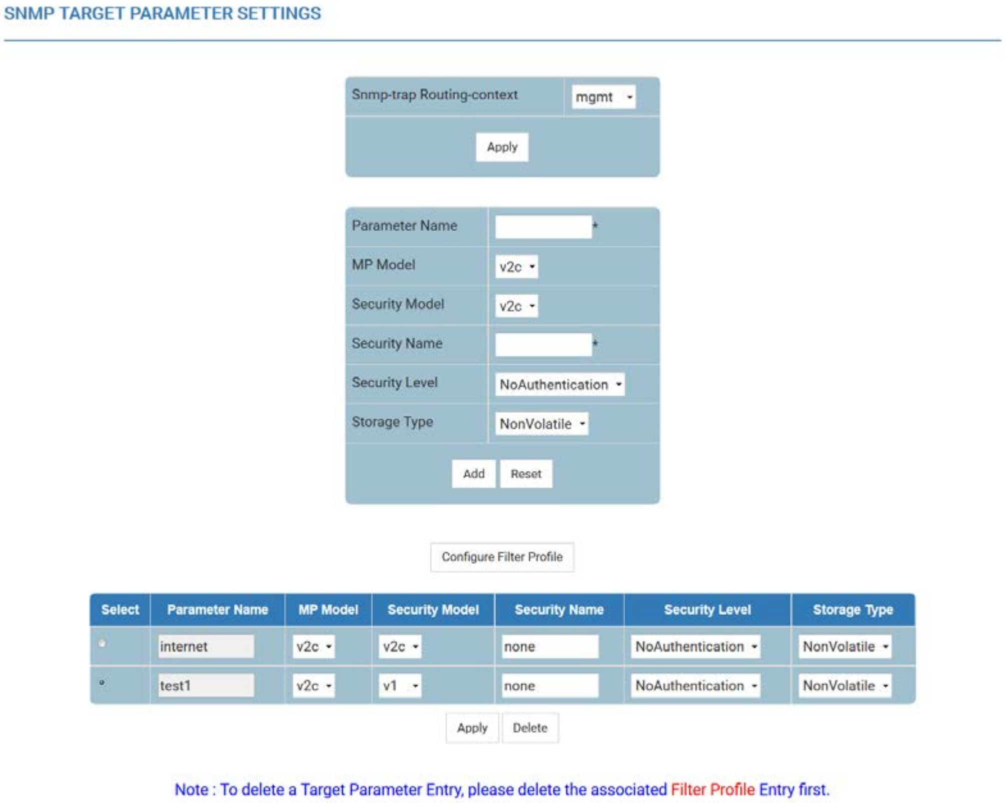
Param - Enter SNMP parameters to be used when generating messages to be sent to transport address. The maximum size is 32.

Storage Type - Select the required Storage type for the target address entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.6 TargetParameter



SNMP TARGET PARAMETER SETTINGS

Snmp-trap Routing-context	mgmt

Apply

Parameter Name	*
MP Model	v2c
Security Model	v2c
Security Name	*
Security Level	NoAuthentication
Storage Type	NonVolatile

Add Reset

Configure Filter Profile

Select	Parameter Name	MP Model	Security Model	Security Name	Security Level	Storage Type
○	internet	v2c	v2c	none	NoAuthentication	NonVolatile
●	test1	v2c	v1	none	NoAuthentication	NonVolatile

Apply Delete

Note : To delete a Target Parameter Entry, please delete the associated Filter Profile Entry first.

Fig: SNMP Target Parameter Settings

The *TargetParameter* link opens the **SNMP Target Parameter Settings** Page.

This page allows the user to configure the SNMP target information to be used in the generation of SNMP messages.

The table below lists the fields present in this page.

Snmp-trap Routing-context - Select routing context for Snmp-trap.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Parameter Name - Enter a unique identifier of the parameter. The maximum size is 32.

MP Model - Select the MP model of the SNMP. Options are:

* v1 - Sets the MP model as Version 1.

* v2c - Sets MP model as Version 2.

* v3 - Sets the MP model as Version 3.

Security Model - Select the version of the SNMP. Options are:

* v1 - Sets the security model as Version 1.

* v2c - Sets the security model as Version 2.

* v3 - Sets the security model as Version 3.

Security Name - Enter the security name, on whose behalf SNMP messages will be generated. The maximum size is 32.

Security Level - Select the level of security to be used when generating SNMP messages. The list contains:

* NoAuthentication - Sets no authentication.

* Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.

* Private - Both authentication and privacy.

Storage Type - Select the required Storage type for the target parameter entry. Options are:

* Volatile - Storage type is temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Storage type is permanent. Saves the configuration to the system.

You can view the Saved configuration on restarting the system.

3.22.7 Filter Profile

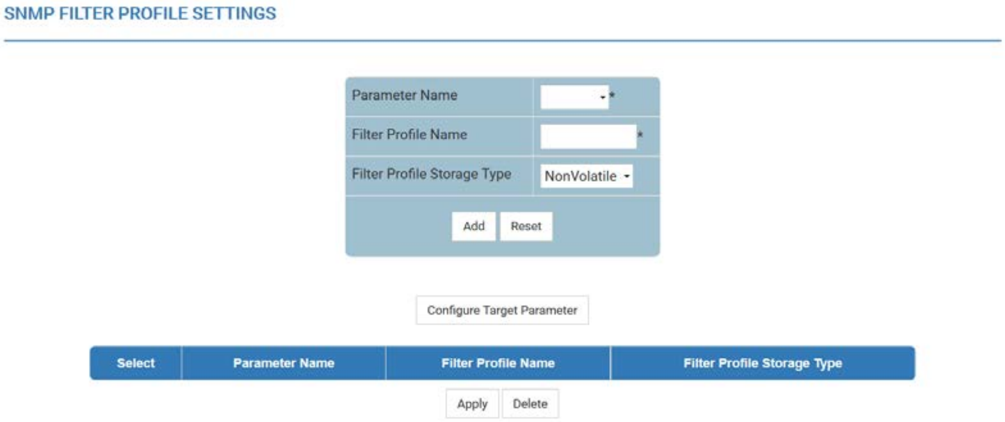

SNMP FILTER PROFILE SETTINGS
Parameter Name
Filter Profile Name
Filter Profile Storage Type
NonVolatile
Add
Reset
Configure Target Parameter
Select
Parameter Name
Filter Profile Name
Filter Profile Storage Type
Apply
Delete

Fig: SNMP Filter Profile Settings

The *Filter Profile* link opens the **SNMP Filter Profile Settings** Page.
This page allows the user to configure the filter profile that is to be used when generating notifications using the corresponding entry in the target parameters table.

The table below lists the fields present in this page.

Parameter Name - Select the existing parameter name to which the filter profile setting should be assigned.

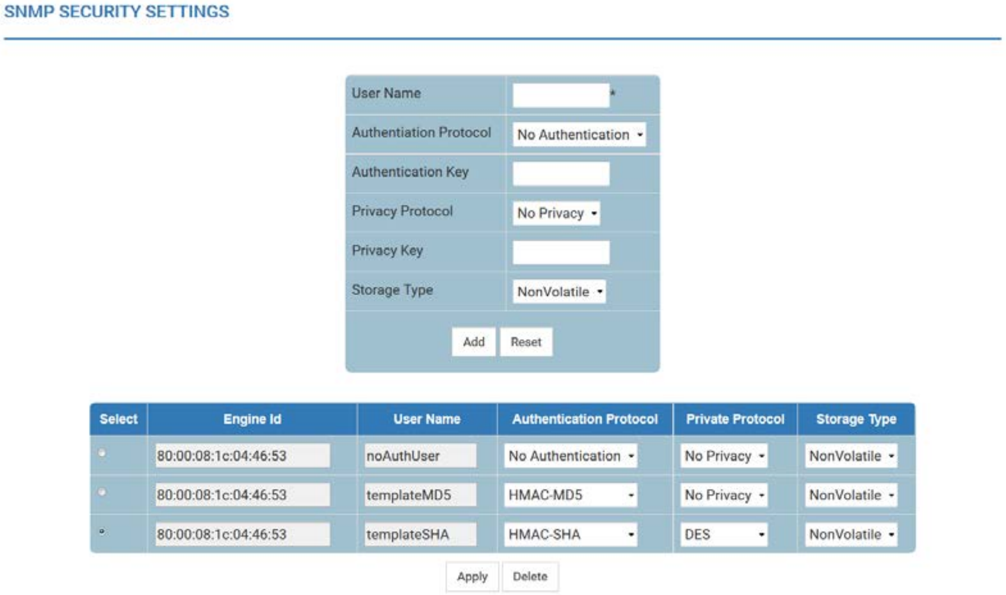
Filter Profile Name - Enter the name for the filter profile. This name is used when generating notifications using the corresponding entry in the target address table. This value is a string of maximum size of 32.

Filter Profile Storage Type - Select the storage type for the filter profile entry.
By default storage type is set as NonVolatile. The list contains:

* Volatile **-** Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* NonVolatile **-** Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.8 User



SNMP SECURITY SETTINGS

User Name	*
Authentiation Protocol	No Authentication
Authentication Key	
Privacy Protocol	No Privacy
Privacy Key	
Storage Type	NonVolatile

Select	Engine Id	User Name	Authentication Protocol	Private Protocol	Storage Type
○	80:00:08:1c:04:46:53	noAuthUser	No Authentication	No Privacy	NonVolatile
○	80:00:08:1c:04:46:53	templateMD5	HMAC-MD5	No Privacy	NonVolatile
●	80:00:08:1c:04:46:53	templateSHA	HMAC-SHA	DES	NonVolatile

Fig: SNMP Security Settings

The *User* link opens the **SNMP Security Settings** Page.

This page allows the user to configure a user and security parameters for that user.

The table below lists the fields present in this page.

User Name - Enter the user name which is the User-based Security Model dependent security ID. The maximum size is 32.

Engine Id - Displays the administratively unique identifier of an SNMP engine. This value is used only for identification and not for addressing. This is a read only field.

Authentication Protocol - Select the type of authentication protocol used for authentication. The list contains:

* No Authentication - Sets no authentication.

* HMAC-MD5 - Sets the Message Digest 5 based authentication.

* HMAC-SHA - Sets the Security Hash Algorithm based authentication.

Authentication Key - Enter the secret authentication key used for messages sent on behalf of this user to/from the SNMP. The maximum size is 40.

Privacy Protocol - Select the type of protocol to be is used in this case. The list contains:

* No Privacy - Sets no privacy

* DES - Data Encryption Standard protocol provides an algorithm to encrypt PPP encapsulated packets.

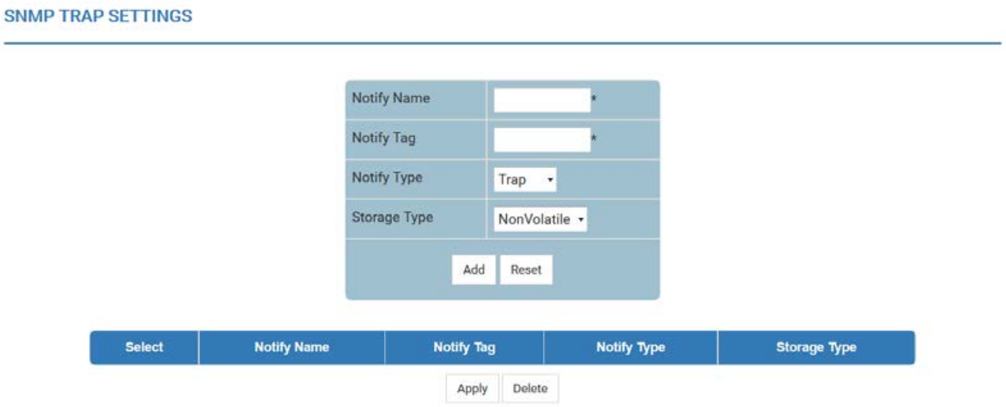
Privacy Key - Enter the key. The messages sent on behalf of a user to/from the SNMP, can be protected from disclosure. The maximum size is 32.

Storage Type - Select the required Storage type for the security settings entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile **-** Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.9 Trap Manager



SNMP TRAP SETTINGS

Notify Name	*
Notify Tag	*
Notify Type	Trap
Storage Type	NonVolatile

Select	Notify Name	Notify Tag	Notify Type	Storage Type

Fig: SNMP TRAP Settings

The *Trap Manager* link opens the **SNMP TRAP Settings** Page.

This page allows the user to configure set of management targets to receive notifications.

The table below lists the fields present in this page.

Notify Name - Enter a unique identifier associated with the entry. The maximum size is 32.

Notify Tag - Enter the notification tag, which is used to select entries in the Target Address Table. The maximum size is 32.

Notify Type - Select the notification type. The list contains:

* Trap - Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system.

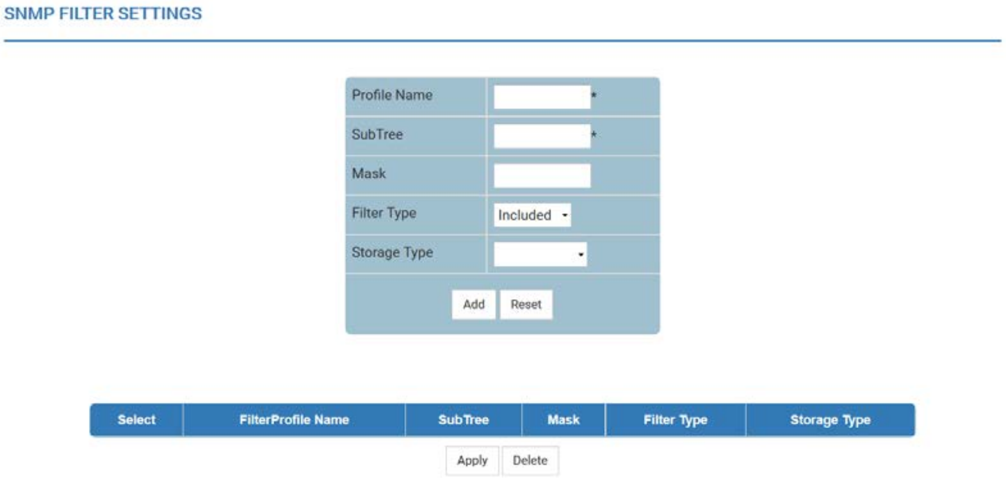
* Inform - Allows routers / switches to send inform requests to SNMP managers

Storage Type Select the required Storage type for the trap settings entry. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

* Non Volatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.22.10 Filter Conf


SNMP FILTER SETTINGS

Profile Name	*
SubTree	*
Mask	
Filter Type	Included
Storage Type	

Select	FilterProfile Name	SubTree	Mask	Filter Type	Storage Type

Fig: SNMP Filter Settings

The *Filter Conf* link opens the **SNMP Filter Settings** Page.

This page allows the user to configure notification filters that are used to determine the particular management target that should receive particular notification. The generated notification is compared with filters associated with each management target to determine the target to which the notification is to be sent.

The table below lists the fields present in this page.

Profile Name - Enter the filter profile name that should be used during generating notifications. This value is a string of maximum size of 32.

> The profile name should have been already created through SNMP Filter Profile Settings page.

SubTree - Enter the MIB subtree that is combined with corresponding instance of mask to define a family of subtrees which are included in or excluded from the filter profile.

Mask - Enter the bit mask that is combined with MIB subtree to define a family of subtrees. This is an octet string of maximum size of 16.

Filter Type - Select the type of filter to be applied for the filter entry.

By default filter type is set as included. The list contains:

* Included - The family of filter subtrees defined using MIB subtree and bit mask is included in a filter.

* Excluded - The family of filter subtrees defined using MIB subtree and bit mask is excluded from a filter.

Storage Type - Select the storage type for the filter entry.

By default storage type is set as NonVolatile. The list contains:

* Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

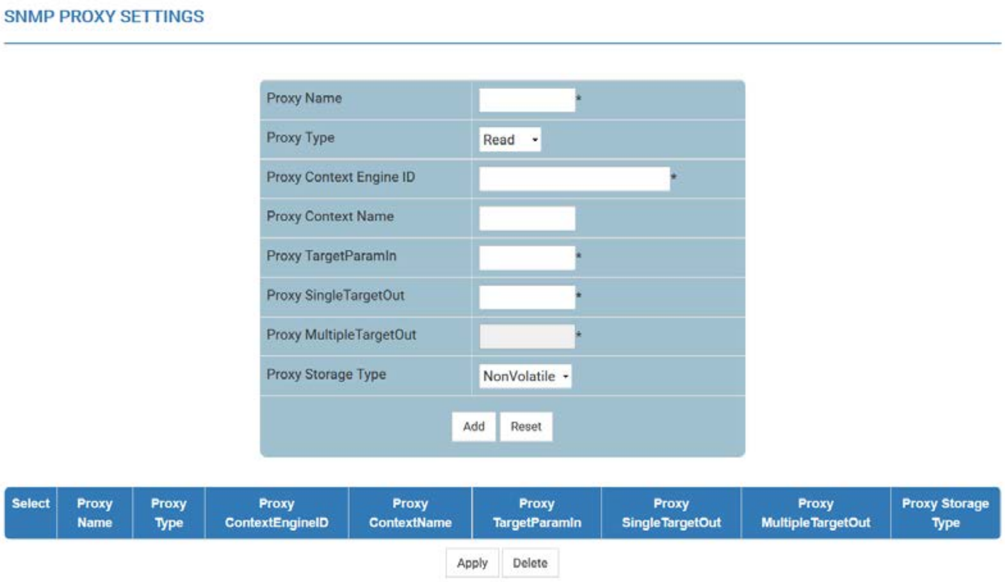
* NonVolatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3.23SNMP PROXY

The *SNMP PROXY* link allows you to configure the SNMP PROXY settings for switch. User can configure SNMP PROXY on the following two pages.

- SNMP PROXY
- SNMP MIB PROXY

3.23.1 SNMP PROXY



SNMP PROXY SETTINGS

Proxy Name	*
Proxy Type	Read
Proxy Context Engine ID	*
Proxy Context Name	
Proxy TargetParamIn	*
Proxy SingleTargetOut	*
Proxy MultipleTargetOut	*
Proxy Storage Type	NonVolatile

Select	Proxy Name	Proxy Type	Proxy ContextEngineID	Proxy ContextName	Proxy TargetParamIn	Proxy SingleTargetOut	Proxy MultipleTargetOut	Proxy Storage Type

Fig: SNMP PROXY Settings

The *SNMP PROXY* link opens the **SNMP PROXY Settings** Page.

This page allows the user to configure translation parameters for forwarding SNMP messages.

The table below lists the fields present in this page.

Proxy Name - Enter the unique proxy name that identifies an entry in the proxy table.

This value is a string of maximum size of 32.

Proxy Type - Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains:

* Read - Read messages are forwarded to get the request from the manager.

* Write - Write messages are forwarded to set configurations.

* Inform - Notification messages are forwarded to the agent.

* Trap - SNMP trap messages are forwarded to the agent.

Proxy Context Engine ID - Enter the context engine ID of the agent with whom the manager communicates through the proxy.

Proxy Context Name - Enter a unique context name for an SNMP sub agent. This name is used to identify the corresponding sub agent when more than one sub agent exists.

Proxy TargetParamIn -Enter the SNMP version that the manager sends as request to the proxy.

Proxy Single TargetOut - Enter the SNMP version that the proxy uses to communicate with the agent.

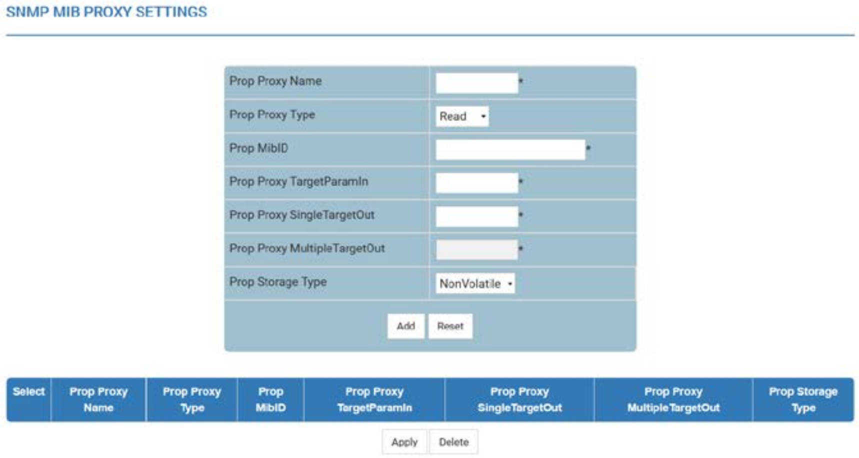
Proxy Multiple TargetOut - Enter the SNMP version that the proxy uses to communicate with multiple agents.

Proxy Storage Type - Select the type of storage for the proxy. The list contains:

* Volatile - The configuration is lost after the switch is reboot, even if the entry is saved.

* Non-Volatile **-** The configuration is available even after the switch is reboot, if the entry is saved.

3.23.2 SNMP MIB PROXY



SNMP MIB PROXY SETTINGS

Prop Proxy Name	*
Prop Proxy Type	Read
Prop MibID	*
Prop Proxy TargetParamIn	*
Prop Proxy SingleTargetOut	*
Prop Proxy MultipleTargetOut	*
Prop Storage Type	NonVolatile

Select	Prop Proxy Name	Prop Proxy Type	Prop MibID	Prop Proxy TargetParamIn	Prop Proxy SingleTargetOut	Prop Proxy MultipleTargetOut	Prop Storage Type

Fig: SNMP MIB PROXY Settings

The *SNMP MIB PROXY* link opens the **SNMP MIB PROXY Settings** Page.

The form at the top is used to configure an SNMP MIB proxy settings entry in the system and the one at the bottom is used to delete or modify the entry.

The table below lists the fields present in this page.

Prop Proxy Name - Enter the unique proxy name that identifies an entry in the proxy table.

This value is a string of maximum size of 32.

Prop Proxy Type - Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains:

* Read **-** Read messages are forwarded to get the request from the manager.

* Write **-** Write messages are forwarded to set configurations.

* Inform **-** Notification messages are forwarded to the agent.

* Trap - SNMP trap messages are forwarded to the agent.

Prop MibID - Enter the proprietary MIB ID which is used as the root object ID.

Prop ProxyTargetParamIn - Enter the SNMP version that the manager sends as request to the proxy.

Prop ProxySingleTargetOut - Enter the SNMP version that the proxy uses to communicate with the agent.

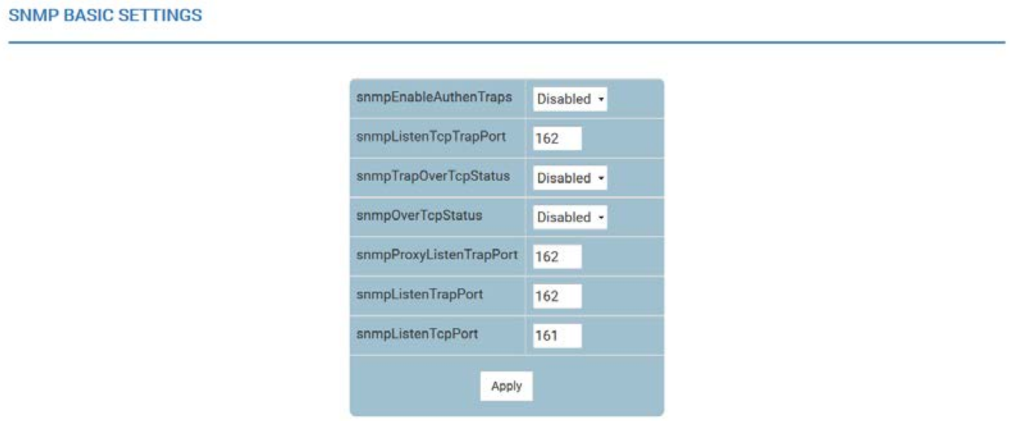
Prop ProxyMultipleTargetOut - Enter the SNMP version that the proxy uses to communicate with multiple agents.

Prop Proxy Storage Type - Select the type of storage for the proxy. The list contains:

* Volatile - The configuration is lost after the switch is reboot, even if the entry is saved.

* Non-Volatile **-** The configuration is available even after the switch is reboot, if the entry is saved.

3.24SNMP SCALARS



SNMP BASIC SETTINGS

snmpEnableAuthenTraps	Disabled
snmpListenTcpTrapPort	162
snmpTrapOverTcpStatus	Disabled
snmpOverTcpStatus	Disabled
snmpProxyListenTrapPort	162
snmpListenTrapPort	162
snmpListenTcpPort	161

Fig: SNMP Basic Settings

The *SNMP Basic Settings* link opens the **SNMP Basic Settings** Page.
This page is used to configure SNMP scalar parameters which are independent of each other.

The table below lists the fields present in this page.

snmpEnableAuthenTraps - Select the status of the authentication failure traps. The list contains:

* Enabled **-** Enables the generation of authentication failure traps.

* Disabled **-** Disables the generation of authentication failure traps.

snmpListenTcpTrapPort - Enter the port number on which SNMP trap message are sent to the manager over TCP.

The default value is 162.

snmpTrapOverTcpStatus - Select the status of sending SNMP trap messages over TCP. The list contains:

* Enables - Allows sending of SNMP trap messages over TCP.

* Disables - Blocks sending of SNMP trap messages over TCP.

snmpOverTcpStatus - Select the status of sending SNMP messages over TCP. The list contains:

* Enables - Allows sending of SNMP messages over TCP. All SNMP messages are send over TCP instead of UDP.

* Disables - Blocks sending of SNMP messages over TCP.

snmpProxyListenTrapPort - Enter the port number on which proxy listens for trap and inform messages from the agent.

The default value is 162.

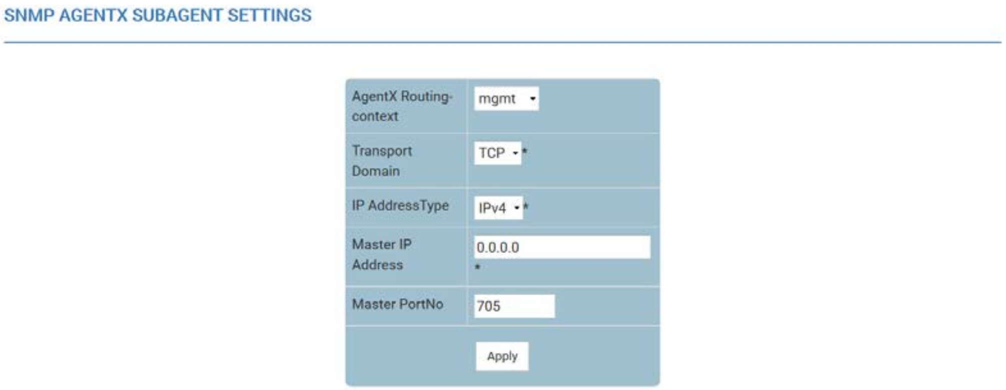
snmpListenTrapPort - Enter the port number on which SNMP trap messages are sent to the manager.

The default value is 162.

snmpListenTcpPort - Enter the port number on which SNMP messages are sent to the manager over TCP.

The default value is 161.

3.25SNMP AGENTX



SNMP AGENTX SUBAGENT SETTINGS

AgentX Routing-context	mgmt
Transport Domain	TCP *
IP AddressType	IPv4 *
Master IP Address	0.0.0.0 *
Master PortNo	705
	Apply

Fig: SNMP Agentx Subagent Settings

The *Subagent Settings* link opens the **SNMP Agentx Subagent Settings** Page.

SNMP agentx is a standardized framework for extensible SNMP agents. It defines

* Processing entities called master agents and subagents.

* A protocol (AgentX) that is used to communicate between master agents and sub agents.

* The elements of procedure by which the extensible agent processes SNMP protocol messages.

The table below lists the fields present in this page.

AgentX Routing-context - Select routing context for SNMP AgentX.

By default it as set as mgmt. The list contains:

* default - use the "default" VRF table for switch front ports.

* mgmt - use the "mgmt VRF table for switch OOB port.

Transport Domain - Select the transport domain to be used as TCP

IP AddressType - Specifies the IP address type. The list contains:

* IPv4 - Sets the IP Address type as version 4.

* IPv6 - Sets the IP Address type as version 6.

Master IP Address - Enter the master agent IP address.

Master PortNo - Enter the master agent port number.

4 Layer 2 Management

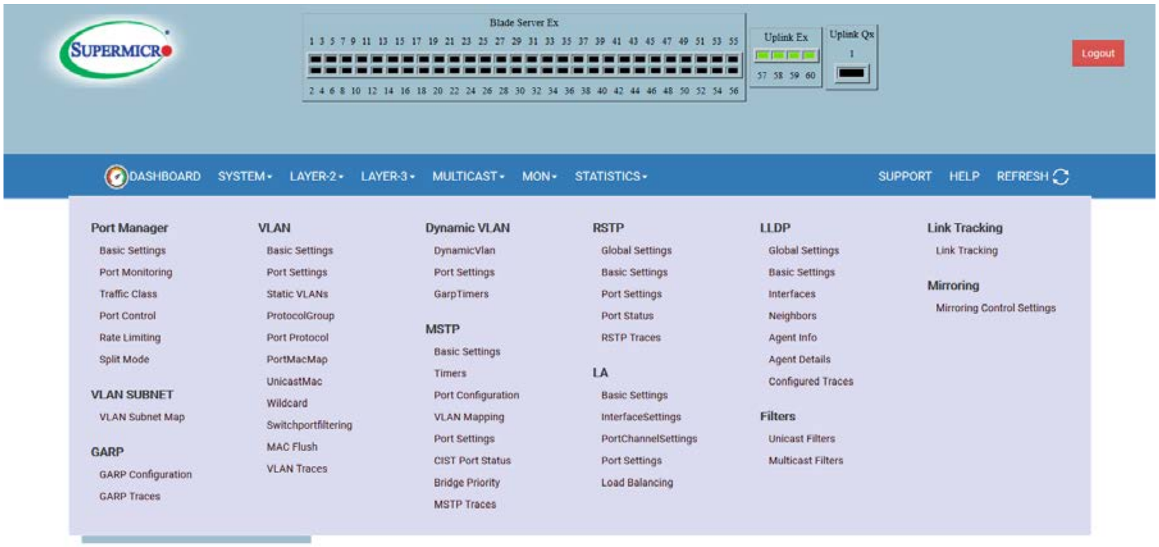


Fig: Layer 2 Management

This page has links to all features present in the layer2 group.

- Port Manager
- VLAN SUBNET
- GARP
- VLAN
- Dynamic VLAN
- MSTP
- RSTP
- LA
- LLDP
- Filters
- Link Tracking
- Mirroring

4.1 Port Manager

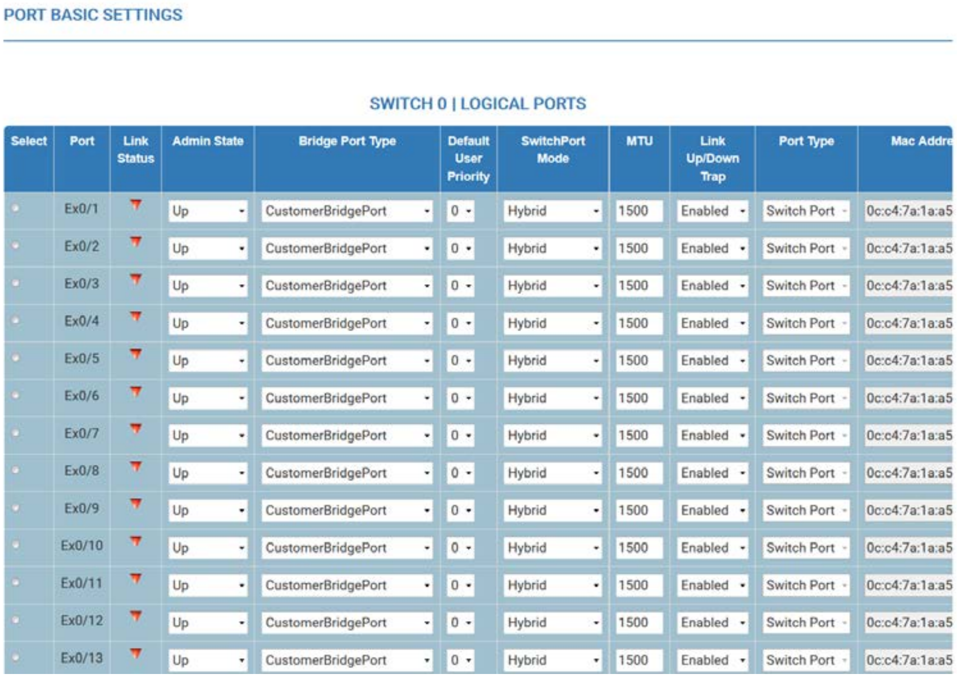
The *Port Manager* link allows you to configure the Port Manager for switch. User can configure Port Manager on the following six pages.

- Basic Settings
- Port Monitoring
- Traffic Class
- Port Control
- Rate Limiting
- Split Mode

Note

In all port based configuration pages, the port number group links are provided in top. For e.g. as Gi1/1 – Ex 1/2. In normal standalone operation of the switch, there shall be only one link and the corresponding port configuration was displayed below.

4.1.1Basic Settings



PORT BASIC SETTINGS

SWITCH 0 | LOGICAL PORTS

Select	Port	Link Status	Admin State	Bridge Port Type	Default User Priority	SwitchPort Mode	MTU	Link Up/Down Trap	Port Type	Mac Addre
○	Ex0/1	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/2	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/3	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/4	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/5	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/6	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/7	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/8	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/9	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/10	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/11	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/12	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5
○	Ex0/13	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	0c:c4:7a:1a:a5

Fig: Port Basic Settings

The *Basic Settings* link opens the **Port Basic Settings** Page.

This page allows the user to configure general information applicable for all physical ports in a switch on per port basis. You can customize all physical ports of the switch at any time.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Link Status - Displays the status of the link using graphics. The link represents a physical connection established between the switches or switch and device in a network. The graphical representations are:

* Green up arrow - Denotes that the link is working. That is, a physical connection established for the port is active and is ready for exchange of traffic.

Red down arrow - Denotes that the link is not working. That is, no physical connection is established for the port or the established physical connection is not active and is a faulty one.

Admin State - Select the desired state of the port. By default, the state is set as Up. The state changes to Up or Down state, as a result of either explicit management action or per configuration information retained by the managed system. The list contains:

* Up - Allows the port to transmit/receive the traffic. The port cannot transmit/receive the traffic, if the Link is not working.

* Down - Blocks the port from transmitting/receiving the traffic. The port will not transmit/receive the traffic, even if the Link is working.

* LoopBack - Sets the desired admin state as loopback

> The connection to the switch will be lost and the web page will not be displayed, if the admin state of the port to which the PC is connected is set as Down.

Bridge Port Type - Displays the bridge port type for the particular port. The configuration associated with the port is flushed, once the bridge port type is changed.

The port type can be configured, only if the bridge mode is selected as Customer Bridge or Provider Bridge (Provider Bridge is not available so far) Mode.

By default, the bridge port type is set as CustomerBridgePort for customer bridges and as ProviderNwPort for provider core and edge bridges. The list contains:

* ProviderNwPort - Denotes that the port is connected to a single provider.

* CustomerNwPort - Denotes that the port is in the S-VLAN component and can transmit or receive frames for single customer. All packets received on this port are mapped to single service instance identifier by PVID of the port. The Acceptable Frame Type is always set as UnTagged and Priority Tagged. This bridge port type is supported only in provider bridging.

* CustomerNwPortStagged - Denotes that the port is in the S-VLAN component and can transmit or receive frames for single customer. VLAN classification is based on S-tag received on the interface or PVID of the port. The Ingress Filtering is always set as Enabled on the port.

* CustomerEdgePort - Denotes that the port is in a PEB that is connected to a single customer. The packets received on this port are initially classified to a CVLAN. CVLAN classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service instance selection is done for a frame based on the entry present in the C-VID registration table for the pair (C-VID, reception port).

* PropCustomerEdgePort - Denotes that the port is connected to a single customer, where multiple services can be provided based on only proprietary SVLAN classification tables. S-VLAN classification is not done based on C-VID registration table on the port.

* PropCustomerNwPort - Denotes that the port is connected to a single customer, where multiple services can be provided based on CVLANs by assigning one of the proprietary SVLAN classification tables to the port. The services can also be assigned using other proprietary SVLAN classification tables, where CVLAN is not the index of the table.

* PropProviderNwPort - Denotes that the port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its ethertype. The packets received with standard Q tag is considered as S-Tagged packets.

* CustomerBridgePort - Denotes the port to be used in customer bridges and in

1 This page is not available in Workgroup and Enterprise package.

provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs.

* None - Denotes that the bridge port type is not set for the port. This is currently not supported.

Example:

1. The following details are flushed, when port types CustomerNwPortStagged and ProviderNwPort are changed to any other type:

* Unicast entries learnt on the port

* VID translation table entries associated with the port

2. The following details are flushed, when port type CustomerBridgePort is changed to any other type.

* Unicast entries learnt on the port

* C-VID registration table entries associated with the port

* PEP configuration table entries

* Service priority regeneration table entries

>

* Bridge port type can be set only for switch ports and not for router ports, IVR interfaces and I-LAN interfaces.

* The port type can be set only as CustomerBridgePort in customer bridges.

* The port type can be set only as ProviderNwPort in provider core and edge bridges.

* The port type can be set only as CustomerNwPort or ProviderNwPort, in provider backbone bridge.

* The port types CustomerEdgePort and PropCustomerEdgePort, are allowed only in PEBs.

* The port type cannot be set for a port-channel port, if physical ports are aggregated in the port-channel.

The port type cannot be set for a port that is part of a port-channel.

Default User Priority - Select the default ingress user priority for the port.

By default, the user priority is set as 0. The list contains values from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority.

>

* This priority is useful only on media, such as Ethernet, that does not support native user priority.

* The default user priority is grayed out and cannot be configured, if the Port Type is set as Router Port.

Switch Port Mode - Select the mode of operation for the switch port. The mode defines the way of handling of traffic for VLANs.

By default, the mode is set as Hybrid. The list contains:

* Access - Configures the port as access port that accepts and sends only untagged frames, is added as a member to specific VLAN only, and carries traffic only for the VLAN to which the port is assigned.

* Trunk - Configures the port as trunk port that accepts and sends only tagged frames, is added as member of all existing VLANs and for any new VLAN created, and carries traffic for all VLANs. The trunk port accepts untagged frames too, if the Acceptable
Frame Type is set as All.

* Hybrid - Configures the port as hybrid port that accepts and sends both tagged and untagged frames.

* Host - Enables Ingress Filtering and configures the port as host port that operates based on the secondary VLAN to which it is configured as member port.

* If a host port is a member port of an isolated VLAN, traffic from the host port is sent only to the promiscuous port of the private VLAN and the trunk port.

* If a host port is a member port of the community VLAN, traffic from the host port can be sent only to other ports of the community VLAN, trunk port and promiscuous port of the private VLAN.

* Promiscuous - Enables Ingress Filtering and configures the port as promiscuous port that is used to move traffic between ports in community or isolated VLANs. This port communicates with all interfaces, including the isolated and community ports within a PVLAN.

>

* The switch port mode can be set as Access for a port, only if the Dynamic Vlan
Status is set as Disabled for that port and Acceptable Frame Type is set as
UnTagged and Priority Tagged for that port.

* The switch port mode can be set as Trunk for a port, only if the port is not a member of Untagged Ports for a VLAN.

* The switch port mode is grayed out and cannot be configured, if the Port Type is set as Router Port.

* A host port can be associated only with one secondary VLAN and with the associated primary VLAN.

* Promiscuous ports should be configured as member port of primary VLAN and member port of all secondary VLANs associated with that primary VLAN.

* Host and promiscuous ports should be configured as untagged members of primary / secondary VLANs.

* An access / hybrid port automatically changes as a host port, when configured as a member port of a primary / secondary VLAN.

* Ingress Filtering cannot be disabled on host and promiscuous ports.

* The port is removed from the associated PVLAN domain, when the mode is changed from promiscuous / host to access / hybrid.

MTU - Enter the MTU for the interface. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.

Default value is assigned for MTU based on the type/protocol of the interface, if the MTU value is not configured during creation of interface. This value ranges between 46 and 9216 bytes.

Ethernet v2, PPP default 1500

Ethernet 802.3 1492

Ethernet Jumbo Frames 1500-9000

PPPoE 1480

L2TP 1460

FDDI 4500

>

* The MTU value can be changed for the interface, only if the Admin State of the interface is set as Down.

* The MTU value should be set as lowest of the MTU values of the member ports, while configuring for logical VLAN interfaces.

Link Up/Down Trap - Select whether the linkUp / linkDown trap should be generated for the interface. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow. By default, the trap is set as Enabled for interfaces that do not operate on top of any other interface. Otherwise, the trap is set as Disabled. The list contains:

* Enabled - Enables the generation of linkUp/linkDown traps for the interface.

* Disabled - Disables the generation of linkUp/linkDown traps for the interface.

Port Type - Select the port type to operate the port as an L2 port or as an L3 port.

By default, the type is set as Switch Port for the newly enabled physical port. The list contains:

* Switch Port - Sets the port as an L2 port. The port forwards traffic based on the MAC address and operates in layer 2.

* Router Port - Sets the port as an L3 port. The port forwards traffic based on the IP address and operates in layer 3. The port is not associated with a particular VLAN, does not support VLAN sub interfaces and behaves like a normal L3 interface.

The port type can be configured, only if the Admin State of the interface is set as Down.

Mac Address - Enter the unicast MAC address of the interface. This value is set as an octet string of zero length for interface (example, serial line) that does not have address at its protocol sub-layer.

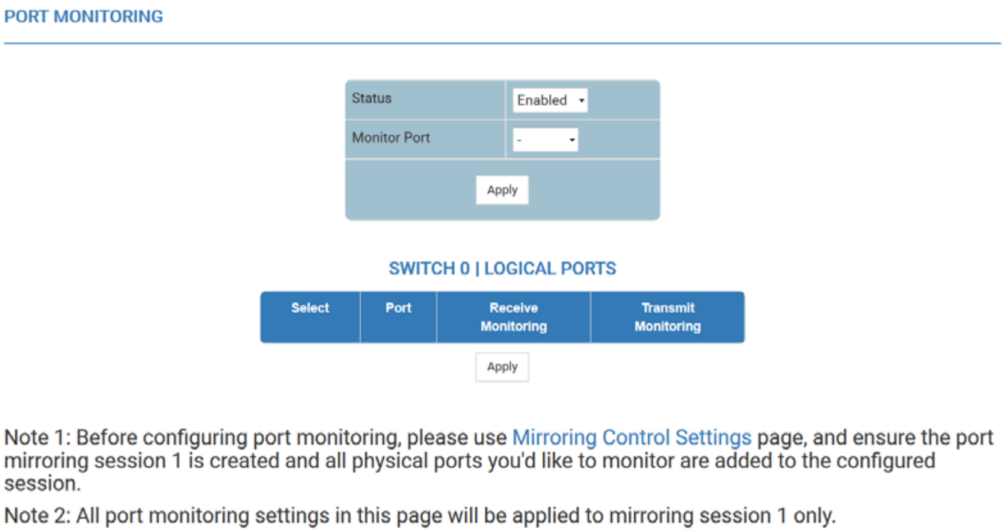
By default, the MAC address is obtained from the switch.

>

* The MAC address can be configured, only if the Admin State of the interface is set as Down.

* This field is valid only if the type/protocol of interface is ethernetCsmacd (Ethernet/802.3) or ieee8023ad (LA MIB).

4.1.2 Port Monitoring



PORT MONITORING

Status	Enabled
Monitor Port	-

SWITCH 0 | LOGICAL PORTS

Select	Port	Receive Monitoring	Transmit Monitoring

Note 1: Before configuring port monitoring, please use Mirroring Control Settings page, and ensure the port mirroring session 1 is created and all physical ports you'd like to monitor are added to the configured session.

Note 2: All port monitoring settings in this page will be applied to mirroring session 1 only.

Fig: Port Monitoring

The *Port Monitoring* link opens the **Port Monitoring** Page.

This page allows the user to configure the mirroring feature related parameters to monitor the traffic that meets network operator specified criteria. It also allows the user to configure port mirroring globally and per port basis.

The table below lists the fields present in this page.

Status - Select whether the port mirroring feature should be enabled globally for all ports of the switch.

Mirroring feature provides management control to monitor the traffic that meets the criteria specified by network operator.

By default, the status is set as Disabled. The list contains:

* Enabled - Enables globally the mirroring feature in the switch.

* Disabled - Disables globally the mirroring feature in the switch.

> The Monitor Port must be set, once the status is set as Enabled.

Monitor Port - Select the port to which the mirrored traffic is to be copied. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number.

The format is interface type slot number/port number. There is no space between these two entries.

All ports available in the switch at that time are populated in the list.

Example: Gi0/1

(Here Gi is interface type Gigabit Ethernet interface

0 is slot number and

1 is port number.)

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Receive Monitoring - Select whether the ingress traffic should be mirrored.

By default, the receive monitoring status is set as Disabled. The list contains:

* Enabled - Enables mirroring of ingress traffic over this interface to port that is configured in the field Monitor Port. The mirroring of ingress traffic is not performed, if the mirroring feature Status is globally disabled.

* Disabled - Disables mirroring of ingress traffic over this interface.

> The receive monitoring feature cannot be set as Enabled for the port configured as Monitor Port.

Transmit Monitoring - Select whether the egress traffic should be mirrored.

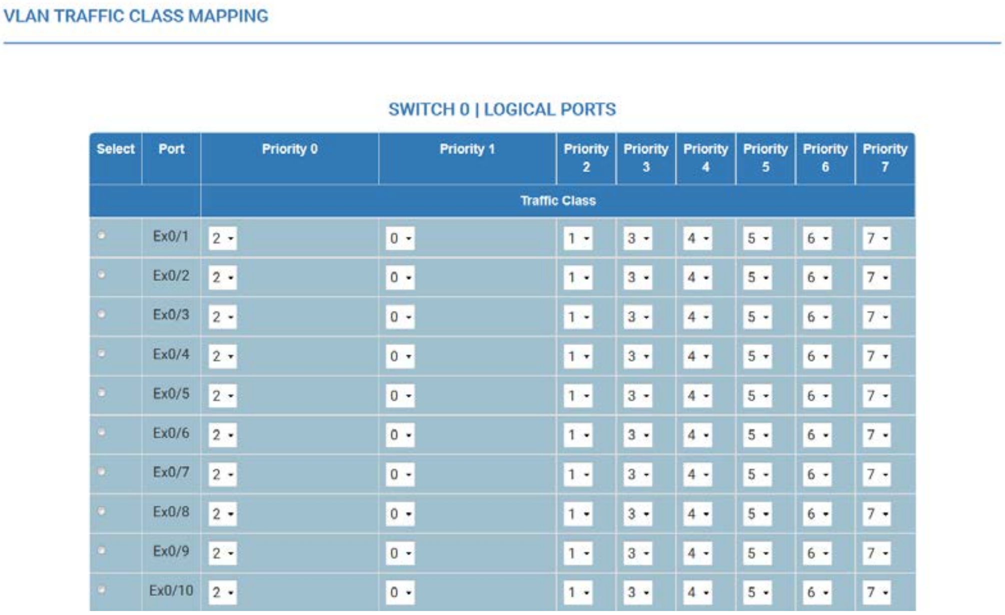
By default, the transmit monitoring status is set as Disabled. The list contains:

* Enabled - Enables mirroring of egress traffic over this interface to port that is configured in the field Monitor Port. The mirroring of egress traffic is not performed, if the mirroring feature Status is globally disabled.

* Disabled - Disables mirroring of egress traffic over this interface.

> The transmit monitoring cannot be set as Enabled for the port configured as Monitor Port.

4.1.3 Traffic Class



VLAN TRAFFIC CLASS MAPPING

SWITCH 0 | LOGICAL PORTS

Select	Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7
		Traffic Class							
○	Ex0/1	2	0	1	3	4	5	6	7
○	Ex0/2	2	0	1	3	4	5	6	7
○	Ex0/3	2	0	1	3	4	5	6	7
○	Ex0/4	2	0	1	3	4	5	6	7
○	Ex0/5	2	0	1	3	4	5	6	7
○	Ex0/6	2	0	1	3	4	5	6	7
○	Ex0/7	2	0	1	3	4	5	6	7
○	Ex0/8	2	0	1	3	4	5	6	7
○	Ex0/9	2	0	1	3	4	5	6	7
○	Ex0/10	2	0	1	3	4	5	6	7

Fig: VLAN Traffic Class Mapping

The *Traffic Class* link opens the **VLAN Traffic Class Mapping** Page.

This page allows the user to map evaluated user priority to traffic class, for forwarding by the bridge. It supports eight traffic classes to handle priority traffic. Each traffic is assigned a traffic type based on the time sensitiveness of the traffic.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

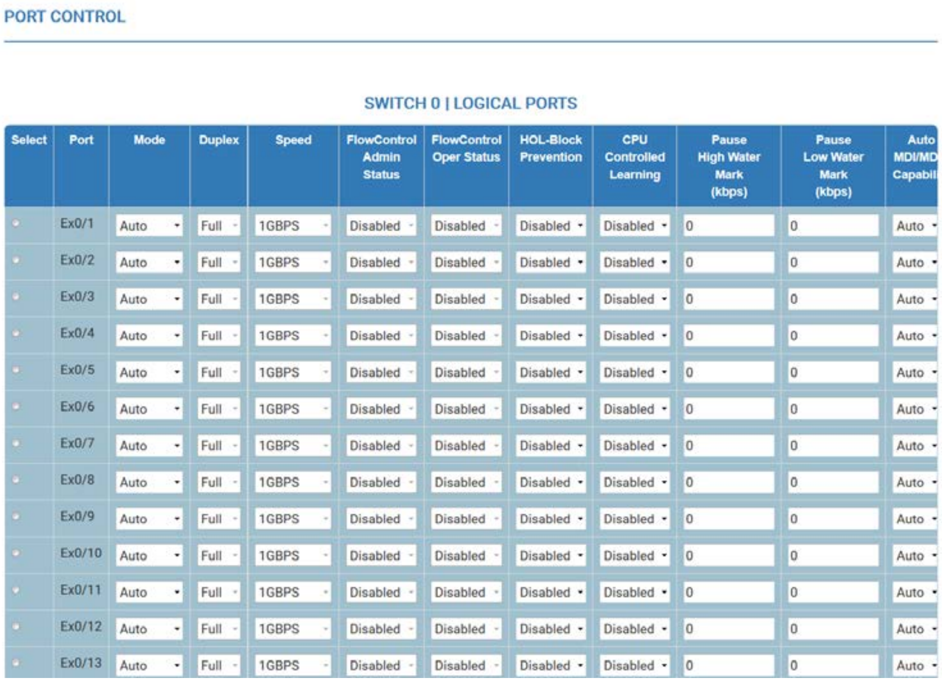
Traffic Class - Select the traffic class value to which the received frame of specified priority is to be mapped.

The priority value ranges from 0 to 7. The priority determined for the received frame is equivalent to the priority indicated in the received tagged frame or one of the evaluated priorities determined based on the media-type.

The priority determined is equal to the Default User Priority value for the ingress port, if the untagged frames are received from Ethernet media.

The priority determined is equal to the Regen user priority2 value for the ingress port and media-specific user priority, if the untagged frames are received from non-Ethernet media.

4.1.4 Port Control



PORT CONTROL

SWITCH 0 | LOGICAL PORTS

Select	Port	Mode	Duplex	Speed	FlowControl Admin Status	FlowControl Oper Status	HOL-Block Prevention	CPU Controlled Learning	Pause High Water Mark (kbps)	Pause Low Water Mark (kbps)	Auto MDI/MD Capabil
○	Ex0/1	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/2	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/3	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/4	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/5	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/6	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/7	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/8	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/9	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/10	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/11	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/12	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto
○	Ex0/13	Auto	Full	1GBPS	Disabled	Disabled	Disabled	Disabled	0	0	Auto

Fig: Port control

The *Port control* link opens the **Port control** Page.

This screen allows the user to configure the port specific parameters such as negotiation mode, of the switch.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Mode - Select the mode of negotiation for the port. The negotiation avoids the risk of network disruption that arises from interference of dissimilar technologies with each other.

By default, the mode is set as Auto. The list contains:

* Auto - Advertises and negotiates the parameters such as speed, duplex mode and flow control, of one port on an end of a link with other port on the another end of the link to find an optimal connectivity between them.

* NoNego - Uses the configured values for the parameters such as speed, duplex mode and flow control. This mode is used when the other switch does not have the capability to configure negotiation mode as auto and no-negotiation.

Duplex - Select the duplex mode that represents the flow of data through the port.

The duplex mode can be configured, only if the negotiation Mode is set as NoNego.

The duplex mode is automatically configured based on the hardware after negotiating with the peer, if the negotiation Mode is set as Auto.

The list contains:

* Full - Ports can send and receive data at same time.

* Half - Ports can either send or receive data at that specified time.

Speed - Select the speed of the interface.

The speed can be configured, only if the negotiation Mode is set as NoNego.

The speed is automatically configured based on the hardware after negotiating with the peer, if the negotiation Mode is set as Auto.

The list contains:

* 10 MBPS - Port can transfer data at the rate of 10 Mega bits per second.

* 100 MBPS - Port can transfer data at the rate of 100 Mega bits per second.

* 1 GB - Port can transfer data at the rate of 1Giga bits per second.

FlowControl Admin Status - Select the default administrative PAUSE mode for the interface. PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands. This command is used to pause the flow of data for a time that is measured in units of quanta, where each unit is equal to 512 bit times.

The PAUSE mode can be configured, only if the negotiation Mode is set as NoNego for the MAU attached to the interface.

The PAUSE mode is automatically configured to the mode to which the interface will automatically revert once auto-negotiation is disabled, if the negotiation Mode is set as Auto for the MAU attached to the interface.

The list contains:

* Disabled - Disables the flow control mechanism (that is, PAUSE).

* Transmit - Enables the transmission of MAC control frames used for PAUSE, to a remote device.

* Receive - Enables the reception of MAC control frames used for PAUSE from, a remote device.

* Both - Enables both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device.

>

* This mode is applied only for the interface operating in full Duplex mode. Otherwise, the value set in this mode is ignored.

* The PAUSE mode cannot be set as Transmit and Receive on interfaces that operates at 100 Mega bits per second or less.

FlowControl Oper Status - Displays the PAUSE mode currently used in the interface.

The value is set based on the auto-negotiation function, if the negotiation Mode is set as Auto for the MAU attached to the interface.

The list contains:

* Invalid

* Disabled - Denotes that the flow control mechanism (that is, PAUSE) is disabled.

This value is returned by

* Interfaces operating in half Duplex mode and

* Interfaces on which auto negotiation process is not yet completed.

* Transmit - Denotes that the transmission of MAC control frames used for PAUSE, to a remote device is enabled. This value is never returned by interfaces operating at 100 Mega bits per second or less.

* Receive - Denotes that the reception of MAC control frames used for PAUSE, to a remote device is enabled. This value is never returned by interfaces operating at 100 Mega bits per second or less.

* Both - Denotes that both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device is enabled.

HOL-Block Prevention - Select whether the HOL blocking should be prevented on a port. HOL blocking happens when HOL packet of a buffer cannot be switched to an output port.

By default, the HOL block prevention is set as Enabled. The list contains:

* Enabled - Prevents HOL blocking from occurring on the port. The high priority packets are placed in a separate queue and the low priority packets are discarded.

The applications or TCP protocol keeps track of necessity to retransmit discarded packets.

* Disabled - Does not prevent HOL blocking on the port.

CPU Controlled Learning - Select CPU controlled learning of the interface.

By default, the CPU controlled learning is set as Disabled. The list contains:

* Enabled - Software learning of MAC Address from the packets arriving on the interface instead of hardware learning of MAC address.

* Disabled - Disables CPU controlled learning of MAC Address on the interface.

Pause High Water Mark - Configures the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges between 1 and 80000000 kbps.

Pause Low Water Mark - Configures the ingress rate below which transmission of PAUSE frames are stopped. This value ranges between 1 and 80000000 kbps.

Auto MDI/MDIX Capability - Select MDI/MDIX mode of the interface.

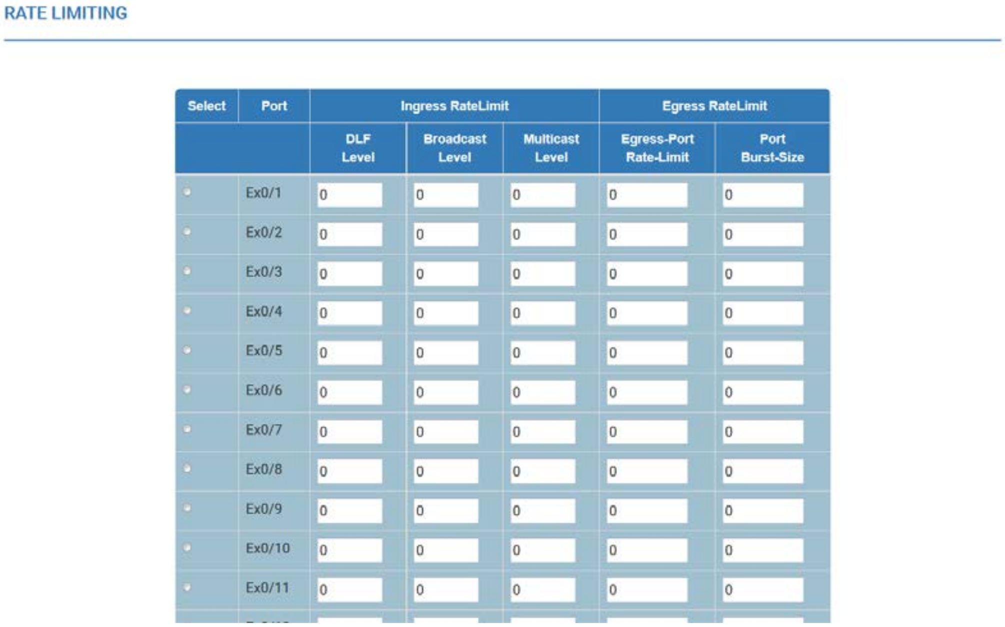
By default, the MDI/MDIX mode is set as Auto. The list contains:

* Auto - Enables the MDI/MDIX Auto Cross over of the interface.

* Mdi - Sets the interface to mdi mode.

* Mdix - Sets the interface to mdix mode.

4.1.5 Rate Limiting



RATE LIMITING

Select	Port	Ingress RateLimit			Egress RateLimit	
		DLF Level	Broadcast Level	Multicast Level	Egress-Port Rate-Limit	Port Burst-Size
○	Ex0/1	0	0	0	0	0
○	Ex0/2	0	0	0	0	0
○	Ex0/3	0	0	0	0	0
○	Ex0/4	0	0	0	0	0
○	Ex0/5	0	0	0	0	0
○	Ex0/6	0	0	0	0	0
○	Ex0/7	0	0	0	0	0
○	Ex0/8	0	0	0	0	0
○	Ex0/9	0	0	0	0	0
○	Ex0/10	0	0	0	0	0
○	Ex0/11	0	0	0	0	0

Fig: Rate Limiting

The *Port control* link opens the **Port control** Page.

This page allows you to control the rate limiting parameters for all interfaces in the switch. The rate control feature protects the switch from packet flooding from malicious users. This feature allows you to set threshold traffic rate so that the traffic exceeding the threshold rate is dropped. Rate control can be applied on unknown unicast, multicast and broadcast traffic.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

DLF Level - Enter the limiting value for the maximum number of DLF (Destination Lookup Failure) packets that can be transmitted per second over the interface.

The value range is limited by the underlying hardware. The value 0 disables rate limiting for destination look up failure packets on the interface.

This value ranges between 0 and 262143. Default value is 0.

Broadcast Level - Enter the limiting value for the maximum number of broadcast packets that can be transmitted per second over the interface.

The value range is limited by the underlying hardware. The value 0 disables rate limiting for broadcast packets on the interface.

This value ranges between 0 and 262143. Default value is 0.

Multicast Level - Enter the limiting value for the maximum number of multicast packets that can be transmitted per second over the interface.

The value range is limited by the underlying hardware. The value 0 disables rate limiting for multicast packets on the interface.

This value ranges between 0 and 262143. Default value is 0.

Egress-Port Rate-Limit - Enter the rate limit value that represents the maximum number of packets to be transferred per second on a port.

The rate limit is applied based on the operating speed of the port. It affects the interface speed and is affected by the metering feature.

The value 0 disables rate limiting, that is, sets the port to the configured speed.

This value ranges between 0 and 80000000.

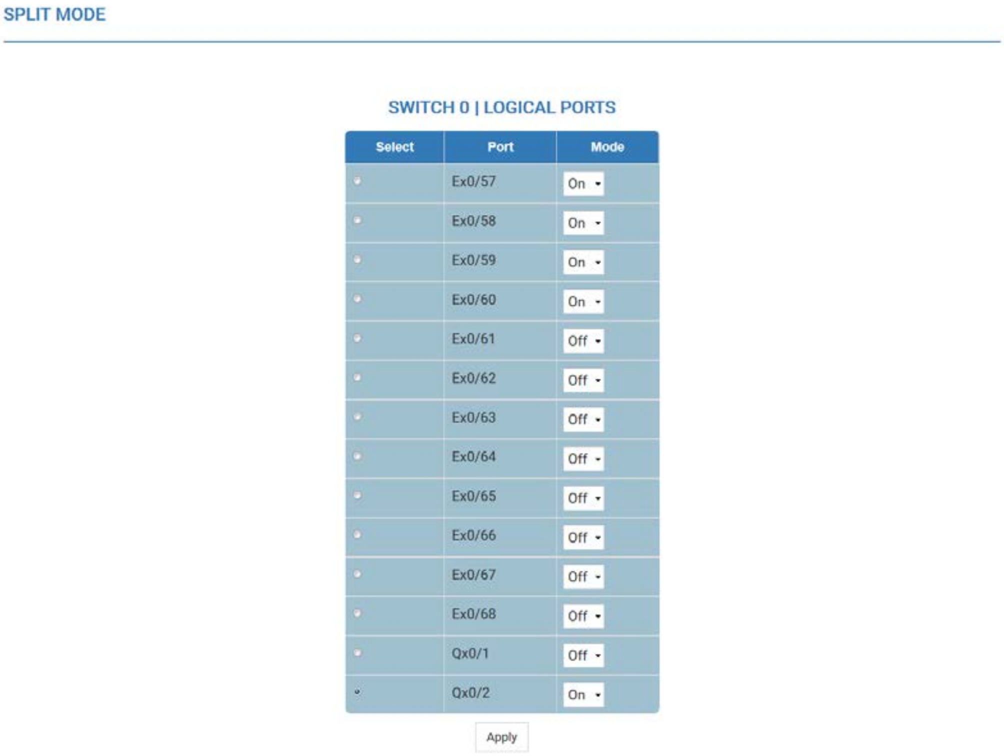
Port Burst-Size - Enter the burst size that represents the maximum number of packet burst to be transferred per second on a port.

The burst size is applied based on the operating speed of the port. It affects the interface speed and is affected by the metering feature.

The value 0 disables burst rate limiting, that is, sets the port burst rate limit to the configured speed.

This value ranges between 0 and 80000000.

4.1.6 Split Mode



SPLIT MODE

SWITCH 0 | LOGICAL PORTS

Select	Port	Mode
○	Ex0/57	On
○	Ex0/58	On
○	Ex0/59	On
○	Ex0/60	On
○	Ex0/61	Off
○	Ex0/62	Off
○	Ex0/63	Off
○	Ex0/64	Off
○	Ex0/65	Off
○	Ex0/66	Off
○	Ex0/67	Off
○	Ex0/68	Off
○	Qx0/1	Off
●	Qx0/2	On

Fig: Split Mode

The *Split Mode* link opens the **Split Mode** Page.

This page allows user to configure the split mode for those interfaces supported this feature in the switch.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port supported split mode, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

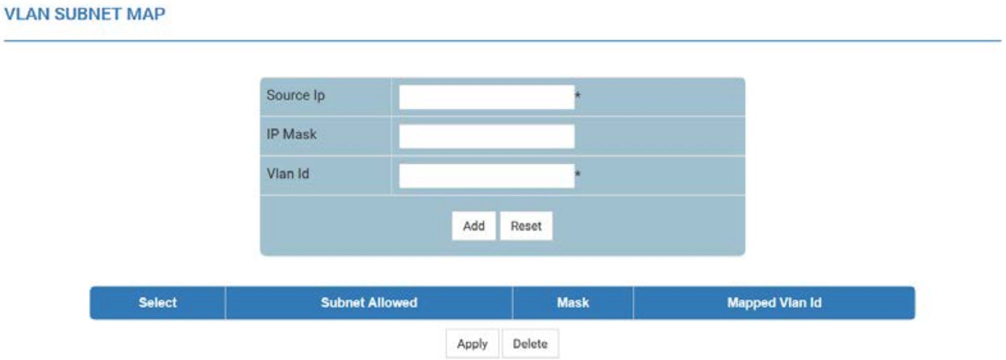
Mode - Specifies the actions to turn on / off split mode on the port. The options are:

* Off **-** Turn off split mode on the port

* On **-** Turn on split mode on the port

Qx-Ethernet ports only support "Off" action to turn off split mode.

4.2 VLAN SUBNET



Select	Subnet Allowed	Mask	Mapped Vlan Id

Fig: VLAN Subnet Map

The *VLAN Subnet Map* link opens the **VLAN Subnet Map** Page.

This page allows the user to map IP subnet address to the VLAN ID for subnet-based VLAN membership classification. The source IP-subnet address in the incoming packets is used to classify VLAN membership.

The table below lists the fields present in the page.

Select - Click to select the entry for which VLAN subnet map needs to be configured.

Subnet Allowed - Enter the source IP subnet address to be used for deciding on discarding/allowing of ARP frames.

All devices in the specified subnet are considered as the member of the mapped VLAN.

For example, if the source IP subnet address is configured as 12.0.0.0 and the subnet mask is set as 255.255.0, then the devices with IP in the range 12.0.0.1 to 12.0.0.255, are considered as a member of the VLAN.

Mask - Enter the subnet mask for the source IP subnet address.

Mapped Vlan Id - Enter the VLAN ID that uniquely identifies a specific VLAN to which the source IP subnet address should be mapped.

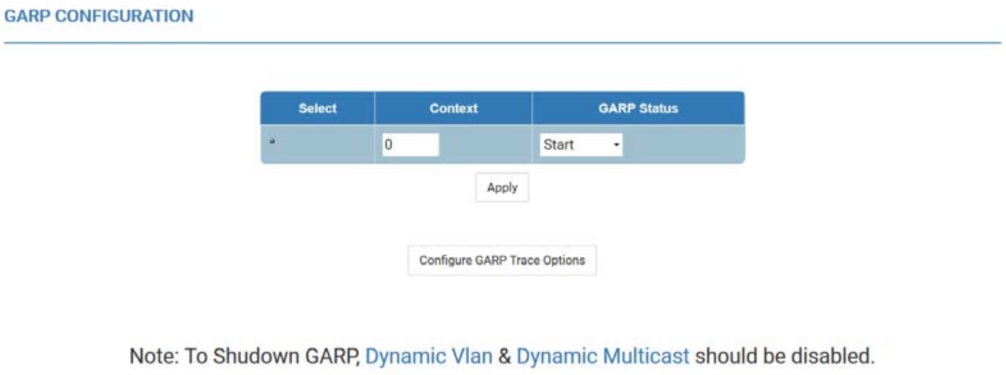
This value ranges between 1 and 4069.

4.3 GARP

The *GARP* link allows you to configure the *GARP* settings for switch. User can configure *GARP* on the following two pages.

- GARP Configuration
- GARP Traces

4.3.1 GARP Configuration



GARP CONFIGURATION

Select	Context	GARP Status
●	0	Start

Note: To Shudown GARP, Dynamic Vlan & Dynamic Multicast should be disabled.

Fig: GARP Configuration

The *GARP Configuration* link opens the **GARP Configuration** Page.

This page allows the user to enable GARP status in the Virtual contexts created in the system.

The table below lists the fields present in the page.

Select - Click to select the context to start or shutdown GARP module.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Garp Status - Select the administrative status requested by management for GARP.

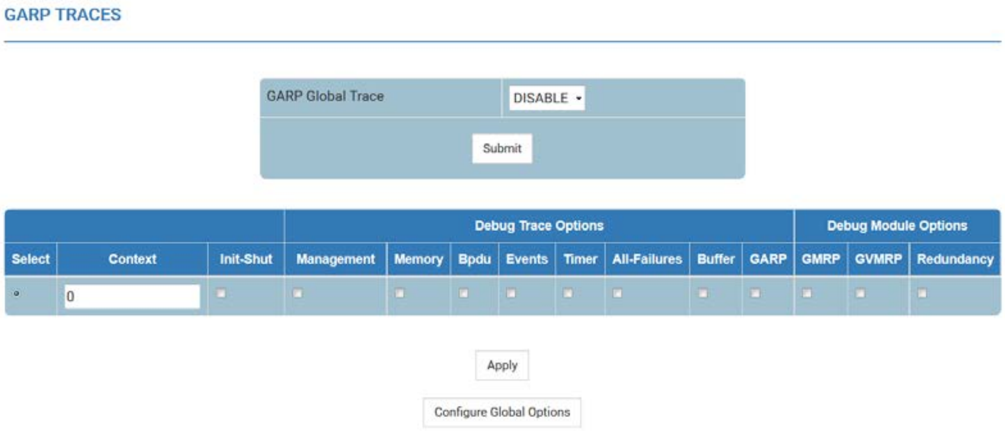
By default, the status is set as Start for the default context ID (that is, 0) and is set as Shutdown for other context IDs. The list contains:

* Start - Enables GARP in the switch on all ports. GMRP and GVRP are enabled explicitly, once the disabled GARP is enabled.

* Shutdown - Disables GARP in the switch on all ports and releases all memories.

> To shutdown GARP functionality, Dynamic VLAN and Dynamic Multicast should be disabled in the Dynamic Vlan Global Configuration and GMRP Global Configuration pages.

4.3.2 GARP Traces



GARP TRACES

GARP Global Trace	DISABLE ▾

			Debug Trace Options								Debug Module Options		
Select	Context	Init-Shut	Management	Memory	Bpdu	Events	Timer	All-Failures	Buffer	GARP	GMRP	GVMRP	Redundancy
●	0	□	□	□	□	□	□	□	□	□	□	□	□

Fig: GARP Traces

The *GARP Traces* link opens the **GARP Traces** Page.

This page allows the user to enable the required debug statements required during debug operation.

Any one of the options from the Debug Module Options and at least one of the options from Debug Trace Options should be selected for the configuration to be effective.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in the page.

GARP Global Trace - Select the global status of the GARP trace in the switch. This sets the VLAN trace status for all virtual switches created in the switch.

The list contains:

* ENABLE - Enables the GARP traces in the switch for all virtual switches. The debug statement is generated for the selected traces.

* DISABLE - Disables the GARP traces in the switch for all virtual switches. The debug statement is not generated for any of the traces, even if the specific trace is selected.

Select - Click to select the context for which the trace levels need to be set.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Debug Trace Options - Select the traces for which debug statements is to be generated. The options are:

* Init-Shut - Generates debug statements for init and shutdown traces. This trace is generated on failed initilization and shutting down of GARP related entries.

* Management - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the GARP features.

* Memory - Generates debug statements for data path traces. This trace is generated during failure in packet processing.

* Bpdu - Generates debug statements for BPDU traces. This trace is generated during failure in modification or retrieving of GARP entries.

* Events - Generates debug statements for packet dump traces. This trace is currently not used in GARP module.

* Timer - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.

* All-Failures - Generates debug statements for all failure traces of the above mentioned traces.

* Buffer - Generates debug statements for GARP buffer related traces. This trace is currently not used in GARP module.

Debug Module Options - Select the module for which the debug statements should be generated. The options are:

* GARP - Generates the debug statements for the GARP module.

* GMRP - Generates the debug statements for the GMRP module.

* GVMRP - Generates the debug statements for the GVRP module.

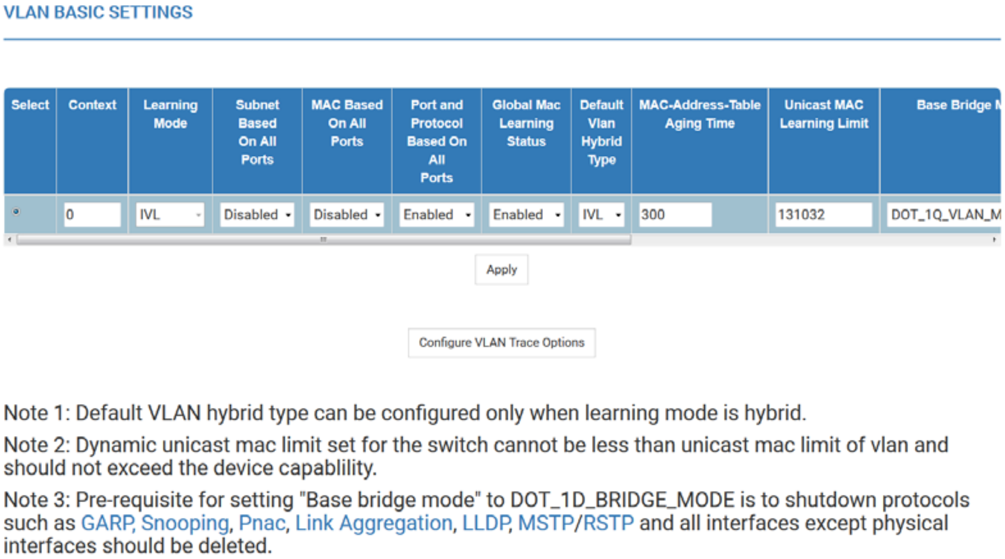
* Redundancy - Generates the debug statements for the GARP redundancy module

4.4 VLAN

The *VLAN* link allows you to configure the *VLAN* settings for switch. User can configure *VLAN* on the following eleven pages.

- Basic Settings
- Port Settings
- Static VLANs
- ProtocolGroup
- Port Protocol
- PortMacMap
- UnicastMac
- WildCard
- Switchportfiltering
- MAC Flush
- VLAN Traces

4.4.1 Basic Settings



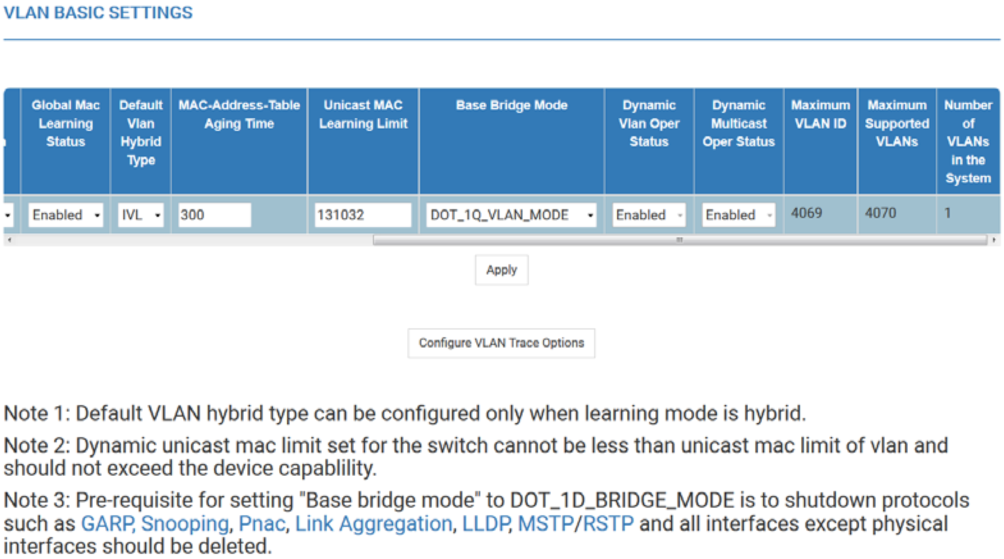
VLAN BASIC SETTINGS

Select	Context	Learning Mode	Subnet Based On All Ports	MAC Based On All Ports	Port and Protocol Based On All Ports	Global Mac Learning Status	Default Vlan Hybrid Type	MAC-Address-Table Aging Time	Unicast MAC Learning Limit	Base Bridge M
○	0	IVL	Disabled	Disabled	Enabled	Enabled	IVL	300	131032	DOT_1Q_VLAN_M

Note 1: Default VLAN hybrid type can be configured only when learning mode is hybrid.

Note 2: Dynamic unicast mac limit set for the switch cannot be less than unicast mac limit of vlan and should not exceed the device capablility.

Note 3: Pre-requisite for setting "Base bridge mode" to DOT_1D_BRIDGE_MODE is to shutdown protocols such as GARP, Snooping, Pnac, Link Aggregation, LLDP, MSTP/RSTP and all interfaces except physical interfaces should be deleted.



VLAN BASIC SETTINGS

Global Mac Learning Status	Default Vlan Hybrid Type	MAC-Address-Table Aging Time	Unicast MAC Learning Limit	Base Bridge Mode	Dynamic Vlan Oper Status	Dynamic Multicast Oper Status	Maximum VLAN ID	Maximum Supported VLANs	Number of VLANs in the System
Enabled	IVL	300	131032	DOT_1Q_VLAN_MODE	Enabled	Enabled	4069	4070	1

Note 1: Default VLAN hybrid type can be configured only when learning mode is hybrid.

Note 2: Dynamic unicast mac limit set for the switch cannot be less than unicast mac limit of vlan and should not exceed the device capablility.

Note 3: Pre-requisite for setting "Base bridge mode" to DOT_1D_BRIDGE_MODE is to shutdown protocols such as GARP, Snooping, Pnac, Link Aggregation, LLDP, MSTP/RSTP and all interfaces except physical interfaces should be deleted.

Fig: VLAN Basic settings

The *Basic settings* link opens the **VLAN Basic settings** Page.

This page allows the user to configure, for each available virtual context, the VLAN details that are used globally in the switch for all ports available in the switch. It allows the user to set the parameters such as VLAN type, which are fundamental for the VLAN configuration in the switch. When all the VLAN type related fields Subnet Based On All Ports, MAC Based on All Ports, and Port and Protocol Based on All Ports are set as Enabled, the VLAN membership classification is done in the following order:

1. MAC-based VLAN classification

2. Subnet-based VLAN classification

3. Port and protocol based VLAN classification

Click Configure VLAN Trace Options, to access the VLAN Traces page.

The table below lists the fields present in the page.

Select - Click to select the context ID to configure the VLAN Basic settings for the virtual context.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Learning Mode - Select the type of VLAN learning mode to be applied for all ports.

This mode defines the forwarding database modes of operation to be implemented by the switch. By default, learning mode is set as IVL. The list contains:

* IVL - Separate forwarding database is created for each VLAN. The information learnt from a VLAN is not shared among other relative VLANs during forwarding decisions. This mode is suitable in situations where the database size is not a constraint and end stations operate over multiple VLANs with the same MAC address.

* SVL - Single forwarding database is created for all VLANs. The information learnt from a VLAN is shared among all other relative VLANs during forwarding decision. This mode is suitable in situations where the learning database size is a constraint.

* HYBRID - Same forwarding database is created for some VLANs and separate forwarding database is used for some VLANs. The usage of same or separate forwarding database for the VLAN is decided based on the configuration done in the L2 Unicast Filter Configuration page.

> The following actions are taken, when the learning mode is changed,

* The static FID-VLAN mapping and static unicast entries should be reconfigured respectively in the pages Port VLAN Protocol Settings and Static VLAN Configuration.

* Static unicast configurations associated with old FID will be deleted.

Subnet Based On All Ports - Select whether the classification of VLAN membership should be done based on subnet on all available ports.

VLAN membership classification is done by matching the source IP address in the packet to a VLAN-ID using an administrator configured table, if the subnet based VLAN classification is enabled.

By default, the subnet based VLAN classification is set as Enabled. The list contains:

* Enabled - Enables the subnet based VLAN membership classification on all ports of the switch.

* Disabled - Disables the subnet based VLAN membership classification on all ports of the switch.

MAC Based on All Ports - Select whether the classification of VLAN membership should be done based on MAC on all available ports.

VLAN membership classification is done based on the source MAC address of the received frame if the MAC based VLAN classification is enabled. For this type, the VLAN membership should be assigned initially.

By default, the MAC based VLAN classification is set as Enabled. The list contains:

* Enabled - Enables MAC based VLAN membership classification on all ports of the switch.

* Disabled - Disables MAC based VLAN membership classification on all ports of the switch.

Port and Protocol Based on All Ports - Select whether the classification of VLAN membership should be done based on port and protocol on all available ports.

VLAN membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port, if the port and protocol based VLAN classification is enabled.

By default, the port and protocol based VLAN classification is set as Enabled. The list contains:

* Enabled - Enables port and protocol based VLAN membership classification on all ports of the switch.

* Disabled - Disables port and protocol based VLAN membership classification on all ports of the switch.

Default Vlan Hybrid Type - Select the default Vlan Hybrid Type to be applied for all ports of the switch, if Learning Mode is set as HYBRID.

By default, Default VLAN Hybrid Type is set as IVL. The list contains:

* IVL - Separate forwarding database is created for each VLAN. The information learnt from a VLAN is not shared among other relative VLANs during forwarding decisions. This mode is suitable in situations where the database size is not a constraint and end stations operate over multiple VLANs with the same MAC address.

* SVL - Single forwarding database is created for all VLANs. The information learnt from a VLAN is shared among all other relative VLANs during forwarding decision. This mode is suitable in situations where the learning database size is a constraint.

> Once the learning mode is changed,

* The static FID-VLAN mapping and static unicast entries should be reconfigured respectively in the pages Port VLAN Protocol Settings and Static VLAN Configuration.

* Static unicast configurations associated with old FID will be deleted.

MAC-Address-Table Aging Time - Enter the timeout period (in seconds) to age out the dynamically learned forwarding database entries. This timer is started once the switch identifies the MAC address.

This value ranges between 10 and 1000000 seconds. Default value is 300 seconds.

Unicast MAC Learning Limit - Enter the maximum number of unicast MAC addresses that can be learned in the virtual context.

This value ranges between 0 and 4294967295. The maximum number of unicast
MAC addresses that can be learnt for the different kind of boards are:

* 950 for BCM and Marvell boards
* 16128 for xCAT board.

>

* The upper limit value depends upon the underlying hardware.
* The unicast MAC learning limit cannot be configured greater than the default value.
* This value should be greater than the value set in the field Mac Limit for the VLAN and should not exceed the switch capability.

Base Bridge Mode - Select the base bridge-mode in which the switch should operate. The list contains:

* DOT_1D_BRIDGE_MODE - Makes the switch to behave according to IEEE 802.1d implementation.
* DOT_1Q_VLAN_MODE - Makes the switch to behave according to IEEE 802.1q implementation.

>

* The base bridge mode can be set as DOT_1D_BRIDGE_MODE, only if the GARP, IGS, MLDS, PNAC LA, LLDP, RSTP and MSTP modules are shutdown and logical interfaces are deleted. These configurations should be done in the following order:

1. Shutdown GARP. The Dynamic VLAN and Dynamic Multicast should be disabled in the Dynamic Vlan Global Configuration and Dynamic Multicast Global Configuration pages, before shutting down GARP.
2. Shutdown IGMP snooping module using the field System Control in the IGMP Snooping Configuration page under the path Multicast > IGMP Snooping > Basic Settings.
3. Shutdown MSTP module using the field System Control in the Global Configuration page under the path Layer2 Management > MSTP > Basic Settings.
4. Shutdown RSTP module using the field System Control in the Global Configuration page under the path Layer2 Management > RSTP > Global Settings.
5. Shutdown PNAC module using the field System Control in the 802.1x Basic Settings page under the path Layer2 Management > 802.1x > Basic Settings.
6. Shutdown LA module using the field System Control in the LA Basic Settings page under the path Layer2 Management > LA > Basic Settings.
7. Shutdown LLDP module using the field Global Status in the LLDP Global Configurations page under the path Layer2 Management > LLDP > Global Setting.

8. Shutdown MLDS module using the field System Control in the MLD Snooping Configuration page under path Multicast > MLD Snooping > Basic Settings.

9. The DOT_1D_BRIDGE_MODE operates over the physical interface alone, so all other VLAN / tunnel interfaces should be deleted.

> If the WEB interface is connected through the Layer3 IP interface, then you should first create a router port and assign IP address for that router port to re-establish the WEB connectivity through the newly created router port. The existing Layer 3 IP interfaces can then be deleted and base bridge mode can be set as DOT_1D_BRIDGE_MODE.

Dynamic Vlan Oper Status - Displays the operational status of the Dynamic VLAN GVRP module).

GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in the LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in the topology. The GVRP module registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP.

By default the operational status is set as Enabled. The list contains:

* Enabled - Denotes that the GVRP module is enabled in the switch.

* Disabled - Denotes that the GVRP module is disabled in the switch.

Dynamic Multicast Oper Status - Displays the operational status of the GMRP module.

GMRP uses the services of GARP to propagate multicast registration information to the bridges in the LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP.

By default the operational status is set as Enabled. The list contains:

* Enabled - Denotes that the GMRP module is enabled in the switch.

* Disabled - Denotes that the GMRP module is disabled in the switch.

Maximum VLAN ID - Displays the largest valid VLAN / VFI ID accepted in the system. This value ranges between 1 and 65535..

* vlan-id - This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094

* vfi-id - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

* * The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

* * VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

* * The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

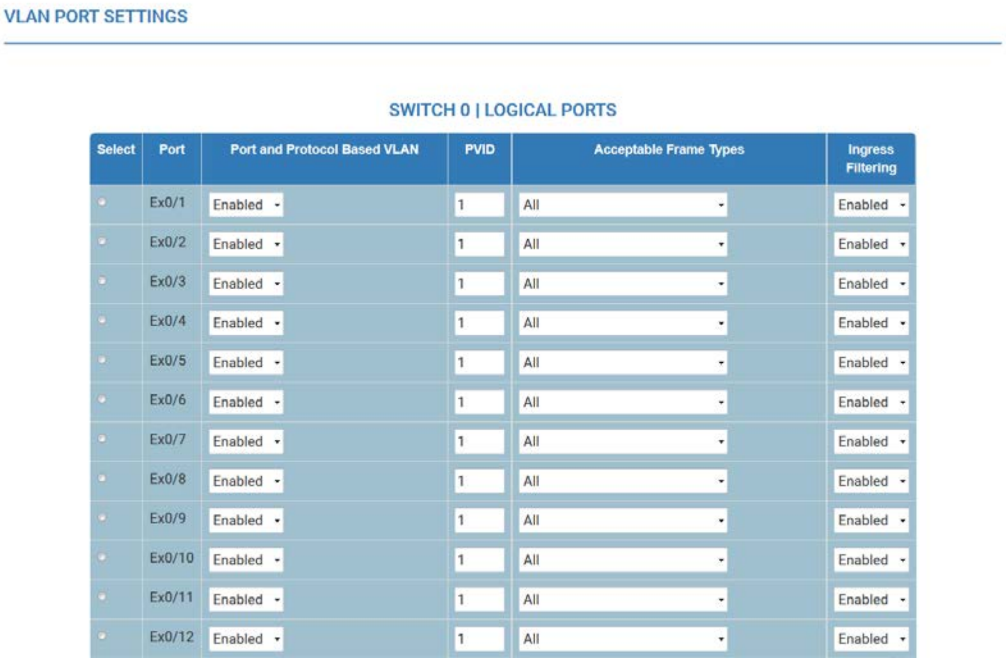
> The VLAN ID cannot be configured greater than the value displayed in the field.

Maximum Supported VLANs - Displays the maximum number of VLANs the switch can support.

Number of VLANs in the System - Displays the total number of VLANs currently active in the device. By default, Vlan 1 is active in the system and hence this value is set as 1.

To configure VLAN basic settings for each virtual switch context, configure the parameters described above and click Apply to apply the configuration in the switch.

4.4.2 Port Settings


VLAN PORT SETTINGS

SWITCH 0 | LOGICAL PORTS

Select	Port	Port and Protocol Based VLAN	PVID	Acceptable Frame Types	Ingress Filtering
○	Ex0/1	Enabled	1	All	Enabled
○	Ex0/2	Enabled	1	All	Enabled
○	Ex0/3	Enabled	1	All	Enabled
○	Ex0/4	Enabled	1	All	Enabled
○	Ex0/5	Enabled	1	All	Enabled
○	Ex0/6	Enabled	1	All	Enabled
○	Ex0/7	Enabled	1	All	Enabled
○	Ex0/8	Enabled	1	All	Enabled
○	Ex0/9	Enabled	1	All	Enabled
○	Ex0/10	Enabled	1	All	Enabled
○	Ex0/11	Enabled	1	All	Enabled
○	Ex0/12	Enabled	1	All	Enabled

Fig: VLAN Port Settings

The *Port Settings* link opens the **VLAN Port Settings** Page.

This page allows the user to configure VLAN details such as VLAN membership classification type, for the physical ports available in the device.

The table below lists the fields present in the page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Port and Protocol Based VLAN - Select whether the port and protocol based VLAN membership classification is supported in the port.

VLAN membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port, if the port and protocol based VLAN classification is supported.

By default, the port and protocol based VLAN classification is set similar as that of the Port and Protocol Based VLAN. The list contains:

* Enabled - Enables port and protocol based VLAN classification in the port.

* Disabled - Disables port and protocol based VLAN classification in the port.

This field can be configured independently without depending on the VLAN type configuration done globally in the device. That is, this field does not depend upon the value set in the field Port and Protocol Based on All Ports.

PVID - Displays the PVID, which represents the VLAN ID assigned to untagged frames or priority-tagged frames received on the port.

The PVID is used for port based VLAN type membership classification.

By default, default VLAN ID (that is, 1) is set as the PVID. This value ranges between 1 and 4094.

Acceptable Frame Types - Select the type of VLAN dependent BPDU frames to be accepted by the port during the VLAN membership configuration.

By default, the frame type is set as All. The list contains:

* All - Accepts tagged, untagged and priority tagged frames received on the port and subjects the frames to Ingress Filtering setting.

* Tagged - Accepts only the tagged frames received on the port. Rejects untagged or priority tagged frames received on the port.

* UnTagged and Priority Tagged - Accepts only the untagged or priority tagged frames received on the port. Rejects tagged frames received on the port.

* This field does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames such as GMRP BPDU.

* The frame type is always set as UnTagged and Priority Tagged, if the Bridge Port Type is set as CustomerNwPort.

Ingress Filtering - Select whether the filtering should be applied for the incoming frames received on the port.

By default, the ingress filtering is set as Disabled. The list contains:

* Enabled - Accepts only the incoming frames of the VLANs that have this port in its member list.

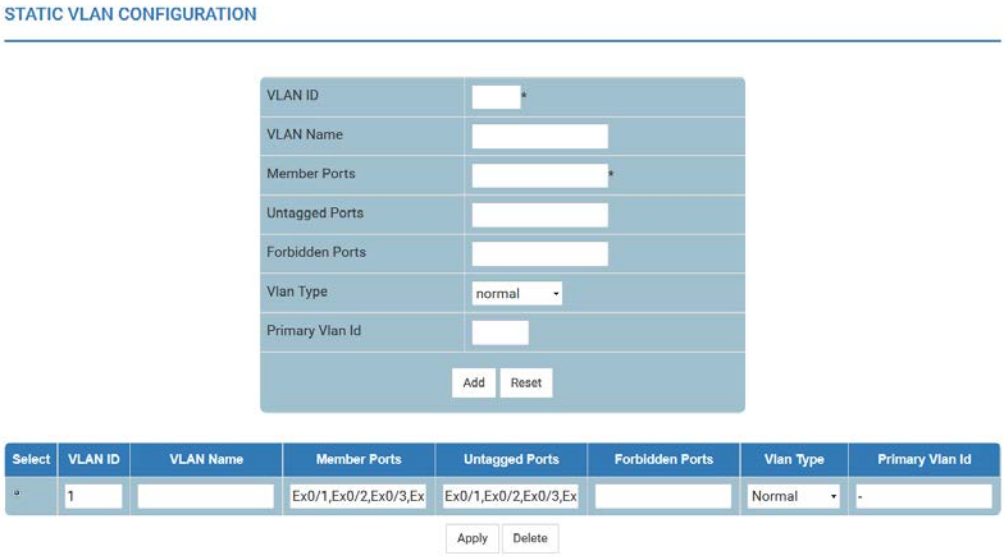
* Disabled - Accepts all incoming frames received on the port.

* This field does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames such as GMRP BPDU.

* The filtering is always set as Enabled, if the Bridge Port Type is set as CustomerNwPortStagged.

* The ingress filtering cannot be disabled for port whose Switch Port Mode is set as host or promiscuous.

4.4.3 Static VLANs



STATIC VLAN CONFIGURATION

VLAN ID	*
VLAN Name	
Member Ports	*
Untagged Ports	
Forbidden Ports	
Vlan Type	normal
Primary Vlan Id	

Select	VLAN ID	VLAN Name	Member Ports	Untagged Ports	Forbidden Ports	Vlan Type	Primary Vlan Id
○	1		Ex0/1,Ex0/2,Ex0/3,Ex	Ex0/1,Ex0/2,Ex0/3,Ex		Normal	-

Fig: Static VLAN Configuration

The *Static VLANs* link opens the **Static VLAN Configuration** Page.

This page allows the user to create / delete VLANs in the switch and statically configure details such as member port, for the VLANs in the switch. These static configuration details are permanent and can be restored after the switch is reset.

* The default VLAN entry, VLAN ID 1, cannot be deleted.

The table below lists the fields present in the page.

VLAN ID - Enter the VLAN ID that uniquely identifies a specific VLAN.

This value ranges between 1 and 4069.

VLAN Name - Enter an administratively assigned string, which is used to identify the VLAN.

The maximum length of this name should be 32 characters.

Member Ports - Enter a port or a set of ports, which need to be part of the VLAN identified by the VLAN ID. Use comma as a separator between the ports while configuring a list of ports. This list includes both tagged and untagged members of the VLAN.

The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and

1 is port number)

Untagged Ports - Enter port or set of ports, which should transmit egress packets for the VLAN as untagged packets. Use comma as a separator between the ports while configuring a list of ports.

Ports which are attached to VLAN-unaware devices should be configured as untagged-ports for a given VLAN.

The untagged ports list should be a sub-set of the VLAN Member Ports.

The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and

1 is port number)

* The port can be configured as a untagged port, only if the Switch Port Mode of the port is not set as trunk.

* The ports configured as untagged ports should be a subset of Member Ports.

Forbidden ports - Enter port or set of ports which should never receive packets from the VLAN mentioned in the VLAN ID. Use comma as a separator between the ports while configuring a list of ports.

The ports configured in the Forbidden Ports list should be mutually exclusive to the Member Ports list field.

The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and

1 is port number)

Vlan Type - Select the private VLAN type to be applied for the specified VLAN ID.

This value can be configured only when VLAN is not activated.

By default, private VLAN type is set as Normal The list contains:

* Normal - The configured VLAN is not assigned to any private VLAN domain.

* Primary - The configured VLAN is set as primary VLAN in a private VLAN domain.

* Isolated - The configured VLAN is set as isolated VLAN in a private VLAN domain. The devices connected to host port of this VLAN can not communicate with each other. One primary VLAN ID should be configured for every isolated VLAN.

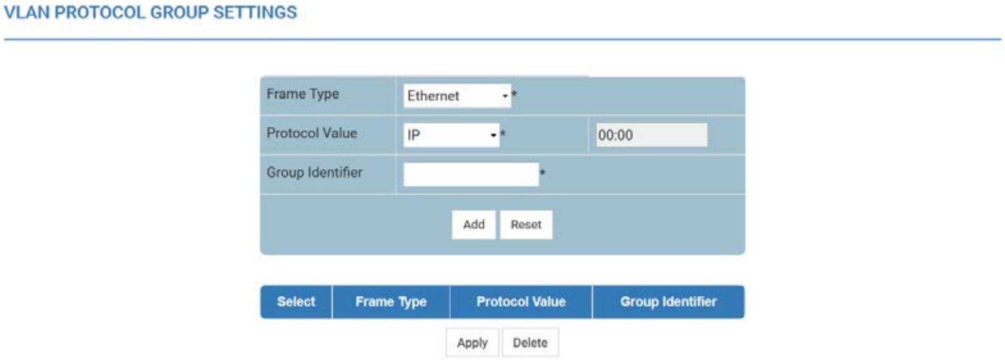
* Community - The configured VLAN is set as community VLAN in a private VLAN domain. The community VLAN behaves in same manner as a normal VLAN in Layer 2. One primary VLAN ID should be configured for every isolated VLAN.

Primary Vlan Id - Enter the primary VLAN ID that uniquely identifies a primary VLAN associated with the specified VLAN ID.

This value cannot be configured for the VLAN types as Normal and Primary.

This value ranges between 1 and 4069.

4.4.4 ProtocolGroup


VLAN PROTOCOL GROUP SETTINGS

Frame Type	Ethernet *	
Protocol Value	IP *	00:00
Group Identifier	*	

Select	Frame Type	Protocol Value	Group Identifier

Fig: VLAN Protocol Group Settings

The *ProtocolGroup* link opens the **VLAN Protocol Group Settings** Page.

This page allows the user to create a protocol group with a specific protocol and encapsulation frame type combination. The created protocol group is used for protocol-VLAN based membership classification. The specified protocol is applied above the data-link layer in a protocol template, and the frame type is applied in the template.

The table below lists the fields present in the page.

Select - Click to select the Frame Type for which the Group Identifier needs to be modified or deleted.

Frame Type - Select the data-link encapsulation format to be applied in a protocol template. By default the Frame Type is set as Ethernet. The list contains:

* Ethernet - Applies the standard IEEE 802.3 frame format. This format contains the following:

1. Preamble - 7 byte value that allows the Ethernet card to synchronize with the beginning of a frame.
2. SFD - 1 byte value that indicates the start of a frame.
3. Destination - 6 byte MAC address of the destination.
4. Source - 6 byte MAC address of the source or a broadcast.
5. Length - 2 byte value representing the number of bytes in the data fields.
6. Data - 46 to 1500 bytes higher layer information containing protocol information or user data.
7. FCS - 4 byte value representing the cyclic redundancy check used by source and destination to verify a successful transmission.

* SNAP - Applies the sub-network access protocol format. This format contains the same structure as LLC Format except the following additional fields added before the data field.

1. OUI - 3 byte value representing organizational unique ID assigned to vendors for differentiating protocols from different manufacturers.

2. Type - 2-byte value representing protocol type that defines a specific protocol in the SNAP. This maintains compatibility with Ethernet v2.

* SNAP802.1H - Applies the sub-network access protocol format. This format contains the same structure as LLC Format except the following additional fields added before the data field.

1. 3 octet field having value 00:00:F8 signifying that next 2 octet field is the encoding of 802.3 type field in an IEEE 802.2/SNAP header.

2. 2 octet type field - encoding of 802.3 type field in an IEEE 802.2/SNAP header.

* SNAP_OTHER - Applies the sub-network access protocol format. This format contains the same structure as LLC Format except for an additional 5 octet.

SNAP protocol identifier (PID) added before the data field. The value of the PID is not in either of the ranges used for RFC_1042 (SNAP) or SNAP 802.1H.

* LLC_OTHER - Applies the LLC format. This format contains the same structure as IEEE 802.3 frame except the following additional fields added before the data field.

1. DSAP - 1 byte value representing destination service access point to determine the protocol used for the upper layer.

2. SSAP - 1 byte value representing source service access point to determine the protocol used for the upper layer.

3. Control - 1 byte value that is used by certain protocols for administration.

> The option SNAP_OTHER can be used, only if the Protocol Value is set as OTHER.

Protocol Value - Select the protocol to be applied above the data-link layer in a protocol template. By default, the protocol value is set as IP The protocol identification is internally handled using octet string. The list contains:

* IP - Sets the protocol as IP, which is used for communicating data across network using TCP/IP. The corresponding octet string is 08:00.

* NOVELL - Sets the protocol as Novell Netware protocol suite, which is developed by Novell Inc. The corresponding octet string is ff:ff.

* NETBIOS - Sets the protocol as NetBIOS over TCP/IP, which allows legacy application relying on the NetBIOS API to be used on modern TCP/IP networks.

The corresponding octet string is f0:f0.

This option can be set only for the Frame Type set as LLC_OTHER.

* APPLETALK - Sets the protocol as AppleTalk, which is a proprietary suite of protocols developed by Apple Inc. The corresponding octet string is 80:9b.

* OTHER - Sets the protocol as some other protocol other than IP, NOVELL, NETBIOS and APPLETALK.

The octet string for the respective protocol can be entered in the text box placed next to this field. This text box is grayed out and cannot be configured, if the option other than OTHER is selected.

This value is set as 16-bit (2 octet) IEEE 802.3 type field, if the field Frame Type is set as Ethernet, SNAP, and SNAP802.1H.

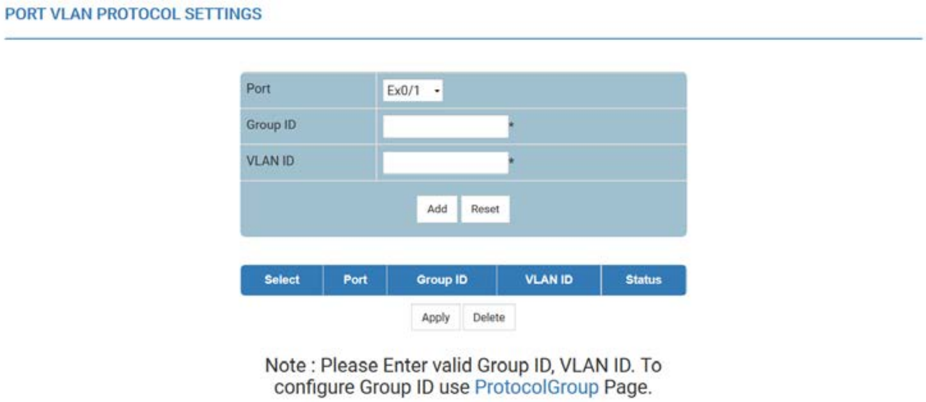
This value is set as 40-bit (5 octet) PID, if the field Frame Type is set as SNAP_OTHER.

This value is set as 2 octet IEEE 802.2 LSAP pair, if the field Frame Type is set as LLC_OTHER. The first octet is used for DSAP and the second octet is used for SSAP.

Group Identifier - Enter the group ID that represents a specific group of protocols that are associated together when assigning a VID to a frame.

This value ranges between 0 and 2147483647.

4.4.5 Port Protocol



Port: Ex0/1
Group ID: *
VLAN ID: *

Select	Port	Group ID	VLAN ID	Status

Note : Please Enter valid Group ID, VLAN ID. To configure Group ID use ProtocolGroup Page.

Fig: Port VLAN Protocol Settings

The *Port Protocol* link opens the **Port VLAN Protocol Settings** Page.

This page allows the user to configure the VID set for a particular port for port and protocol based VLAN classification. Only existing group ID can be assigned for the port. An un-configured VLAN ID can be assigned for a port. When the VLAN is configured, forwarding will take place according to the VID set for the particular port.

The table below lists the fields present in the page.

Select - Click to select the Port for which the Group ID and VLAN ID mapping needs to be modified or deleted.

Port - Select the port to which the VLAN ID and group ID should be mapped. This is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Group ID - Enter the group ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port.

This value ranges between 0 and 2147483647.

> The Group Id entered should have already been created using the Layer2 Management > VLAN > VLAN Protocol Group Setting Page.

VLAN ID - Enter the VLAN ID that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port.

This value ranges between 1 and 4094.

Status - Displays the status of the respective row / entry. This list contains:

* Up - Denotes the entry is created and operationally up.

* Down - Denotes the entry is created but operationally down.

* Under Creation - Denotes the entry is being created and not available for operation / usage.

4.4.6 PortMacMap

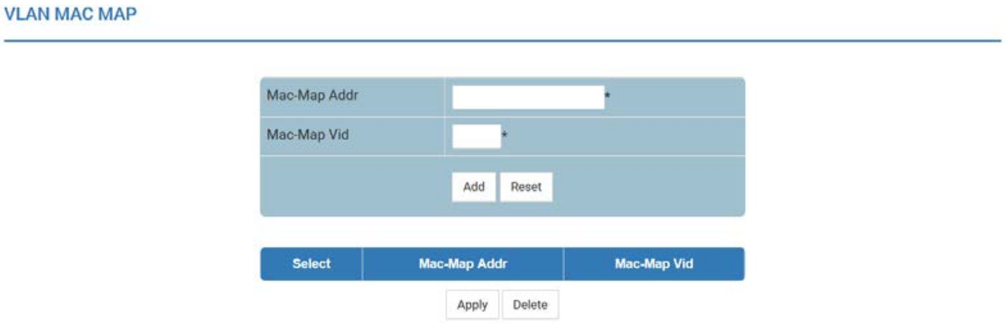


Fig: VLAN Mac Map

The *PortMacMap* link opens the **VLAN Mac Map** Page.

This page allows the user to map the VLAN and MAC address for MAC based VLAN classification.

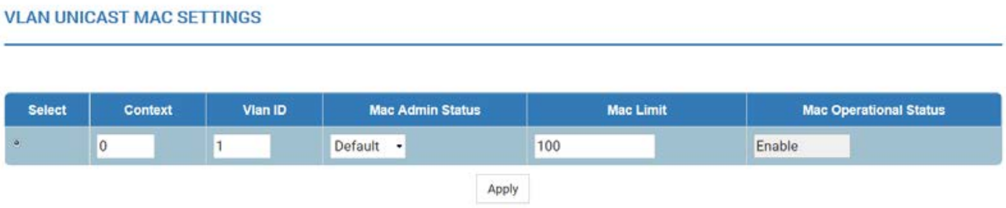
The table below lists the fields present in the page.

Mac-Map Addr - Enter a unique unicast MAC address, which should be mapped to the VLAN and used for MAC based VLAN membership classification.

Mac-Map Vid - Enter the VLAN ID that uniquely identifies a specific VLAN to which the MAC address should be mapped. This VLAN ID is associated with a specific group of protocols for the specific port.

This value ranges between 1 and 4094.

4.4.7 UnicastMac



VLAN UNICAST MAC SETTINGS

Select	Context	Vlan ID	Mac Admin Status	Mac Limit	Mac Operational Status
○	0	1	Default	100	Enable

Fig: VLAN Unicast Mac Settings

The *UnicastMac* link opens the **VLAN Unicast Mac Settings** Page.

This page allows the user to configure the unicast MAC address control information of each created VLAN. It displays the unicast MAC setting details for the VLAN created in the page Static VLAN Configuration and for the default VLAN, once this page is accessed. It displays the unicast MAC settings details for the default VLAN alone, if no new VLAN is created in the page Static VLAN Configuration.

The table below lists the fields present in the page.

Select - Click to select the VLAN entry for which the unicast MAC settings should be configured.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Vlan ID - Displays the VLAN ID that uniquely identifies a specific VLAN.

This value ranges between 1 and 4094.

Mac Admin Status - Select the MAC administration status to learn unicast MAC address for the VLAN.

By default, the status is set as Default. The list contains:

* Enabled - Learns the unicast MAC address for the VLAN.

* Disabled - Does not learn the unicast MAC address for the VLAN.

* Default - Sets the default MAC administration status.

Mac Limit - Enter the maximum number of distinct unicast MAC addresses that can be learnt in the VLAN.

This value ranges between 0 and 131032. The maximum number of unicast MAC addresses that can be learnt for the different kind of boards are:

* The lower and upper limit values depend upon the underlying hardware.

* The MAC limit cannot be configured greater than the default value.

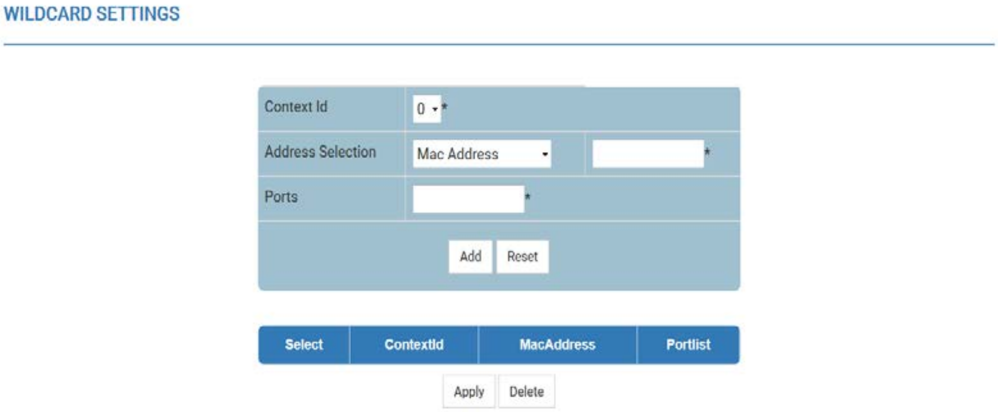
Mac Operational Status - Displays the operational status of the MAC learning for the VLAN. The list contains:

* Enable - Denotes that the MAC learning for the VLAN is enabled.

* Disable - Denotes that the MAC learning for the VLAN is disabled.

If the VLAN does not have any Member Ports, then the Mac operational status for that VLAN is always set as Disable. Otherwise, the Mac operational status is set as same as that of the field Mac Admin Status.

4.4.8 Wildcard


WILDCARD SETTINGS

Context Id: 0 *

Address Selection: Mac Address *

Ports: *

Select	ContextId	MacAddress	Portlist

Fig: Wildcard Settings

The *Wildcard* link opens the **Wildcard Settings** Page.

This page allows the user to configure wild card VLAN, which has ID as 0xFFF. The wild card VLAN static filtering information is used for all VLANs for which no specific static filtering is configured in L2 Unicast Filter Configuration or L2 Multicast Filter Configuration page.

The table below lists the fields present in the page.

Context Id - Select the virtual context ID that uniquely represents a virtual switch created in the physical switch.

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Address Selection - Select the type of destination MAC address to which the filtering information of the wild card entry should be applied. The list contains:

* Broadcast Address - Forwards the received frames that contain any MAC address, through the Ports, if no specific static filtering is configured. The destination MAC address is automatically set as ff:ff:ff:ff:ff:ff and the text box next to this field is grayed out and cannnot be configured.

* Mac Address - Forwards the received frames that contains the MAC address configured in the text box next to this field, through the Ports, if no specific static filtering is configured.

Ports - Enter port or set of ports, to which frames received from any other port and for any VLAN containing destination MAC address similar to that set in the field Address Selection should be forwarded, if there is no specific static filtering entry exists for the MAC specified in the packet.

Use comma as a separator between the ports while configuring a list of ports.

The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

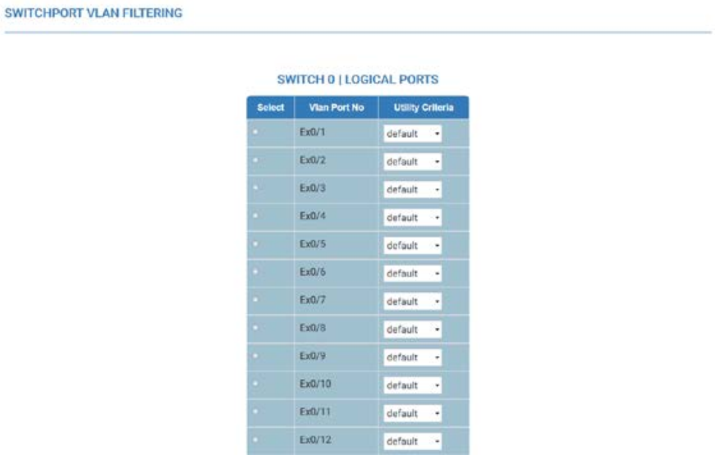
Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and

1 is port number)

4.4.9 Switchportfiltering



SWITCHPORT VLAN FILTERING

SWITCH 0 | LOGICAL PORTS

Select	Vlan Port No	Utility Criteria
○	Ex0/1	default
○	Ex0/2	default
○	Ex0/3	default
○	Ex0/4	default
○	Ex0/5	default
○	Ex0/6	default
○	Ex0/7	default
○	Ex0/8	default
○	Ex0/9	default
○	Ex0/10	default
○	Ex0/11	default
○	Ex0/12	default

Fig: SwitchPort VLAN Filtering

The *Switchportfiltering* link opens the **SwitchPort VLAN Filtering** Page.

This page allows the user to create filtering utility criteria for the ports available in the switch. This utility criteria is used to reduce the capacity requirement of the filtering database and to reduce the time for which service is affected, by retaining the filtering information learnt prior to a change in the physical topology of the network.

The table below lists the fields present in the page.

Select - Click to select the port for which filtering utility criteria needs to be configured.

Vlan Port No - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Utility Criteria - Select the filtering utility criteria to be applied for the port. The learning on a port is decided based on the selected filtering utility criteria.

By default, the criteria are set as default. The list contains:

* default - Learning of source MAC from a packet received on the port is done, only if there is atleast one member port for a VLAN mentioned in the packet.

* enhanced - Learning of source MAC from a packet received on the port is done, only if the following conditions are satisfied.

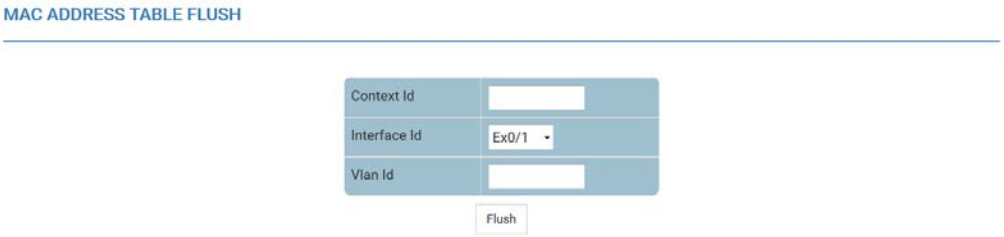
1. At least one VLAN that uses the FID includes the reception port and at least one other Port with a port state of Learning or Forwarding in its member set.

2. The operPointToPointMAC parameter is false for the reception port.

Or

Ingress to the VLAN is permitted through a port other than source and reception. This port can be or not be in the member set for the VLAN.

4.4.10 MAC Flush



MAC ADDRESS TABLE FLUSH

Context Id	
Interface Id	Ex0/1
Vlan Id	

Fig: MAC Address Table Flush

The *MAC Flush* link opens the **MAC Address Table Flush** Page.

This page allows user to flush the MAC address table in the switch.

The table below lists the fields present in this page.

Context Id - Enter the virtual context ID that uniquely represents a virtual switch created in the physical switch.

This value ranges between 0 and 65535.

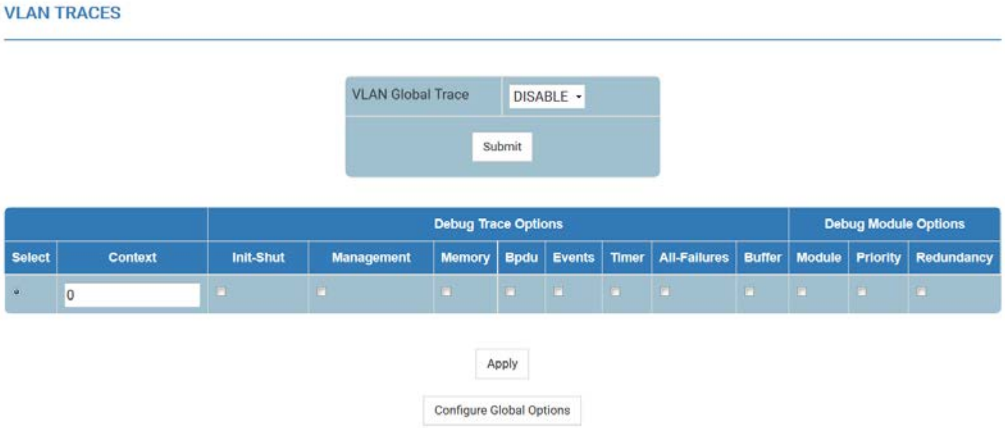
Interface Id - Enter the port, which is a combination of interface type and interface ID.

The interface ID is a combination of slot number and the port number (slot number/port number).

Vlan Id - Enter the VLAN ID that uniquely identifies a specific VLAN.

This value ranges between 1 and 4094.

4.4.11 VLAN Traces



VLAN TRACES

VLAN Global Trace: DISABLE

		Debug Trace Options							Debug Module Options		
Select	Context	Init-Shut	Management	Memory	Bpdu	Events	Timer	All-Failures	Buffer	Module	Priority	Redundancy
○	0	□	□	□	□	□	□	□	□	□	□	□

Fig: VLAN Traces

The *MAC Flush* link opens the **MAC Address Table Flush** Page.

This page allows the user to choose the debug level for VLAN module in the switch. One or more debug levels can be chosen based on requirements.

Any one of the options from the Debug Module Options and at least one of the options from Debug Trace Options should be selected for the configuration to be effective.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in the page.

VLAN Global Trace - Select the global status of the VLAN trace in the switch. This sets the VLAN trace status for all virtual switches created in the switch.

The list contains:

* ENABLE - Enables the VLAN traces in the switch for all virtual switches. The debug statement is generated for the selected traces.

* DISABLE - Disables the VLAN traces in the switch for all virtual switches. The debug statement is not generated for any of the traces, even if the specific trace is selected.

Select - Click to select the context for which the configuration needs to be done.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Debug Trace Options -Select the traces for which debug statements is to be generated. The options are:

* Init-Shut - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of VLAN related entries.

* Management - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the VLAN features.

* Memory - Generates debug statements for data path traces. This trace is generated during failure in packet processing.

* Bpdu - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of VLAN entries.

* Events - Generates debug statements for packet dump traces. This trace is currently not used in VLAN module.

* Timer - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.

* All-Failures - Generates debug statements for all failure traces of the above mentioned traces.

* Buffer - Generates debug statements for VLAN buffer related traces. This trace is currently not used in VLAN module.

Debug Module Options - Select the module for which the debug statements should be generated. The list contains:

* Module - Generates the debug statements for the VLAN module.

* Priority - Generates the debug statements for the VLAN priority module.

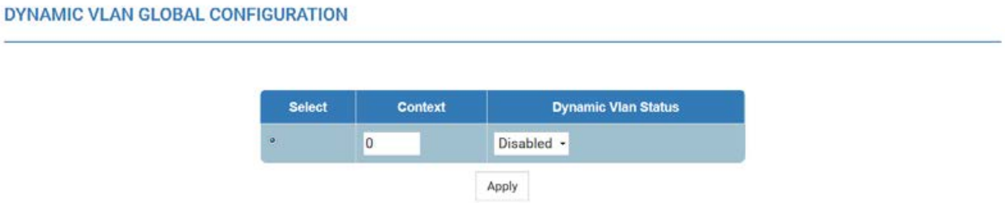
* Redundancy - Generates the debug statements for the VLAN redundancy module.

4.5 Dynamic Vlan

The Dynamic Vlan link allows you to configure the Dynamic Vlan settings for switch. User can configure Dynamic Vlan on the following three pages.

- Dynamic Vlan
- Port Settings
- GarpTimers

4.5.1 DynamicVlan



DYNAMIC VLAN GLOBAL CONFIGURATION

Select	Context	Dynamic Vlan Status
○	0	Disabled

Fig: Dynamic Vlan Global Configuration

The *DynamicVlan* link opens the **Dynamic Vlan Global Configuration** Page.

The page allows the user to globally enable/disable dynamic VLAN feature (GVRP) for the virtual contexts available in the switch.

Dynamic VLAN feature should be disabled, to shut down GARP for the specific context switch.

The table below lists the fields present in the page.

Select - Click to select the context for which the configuration needs to be done.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

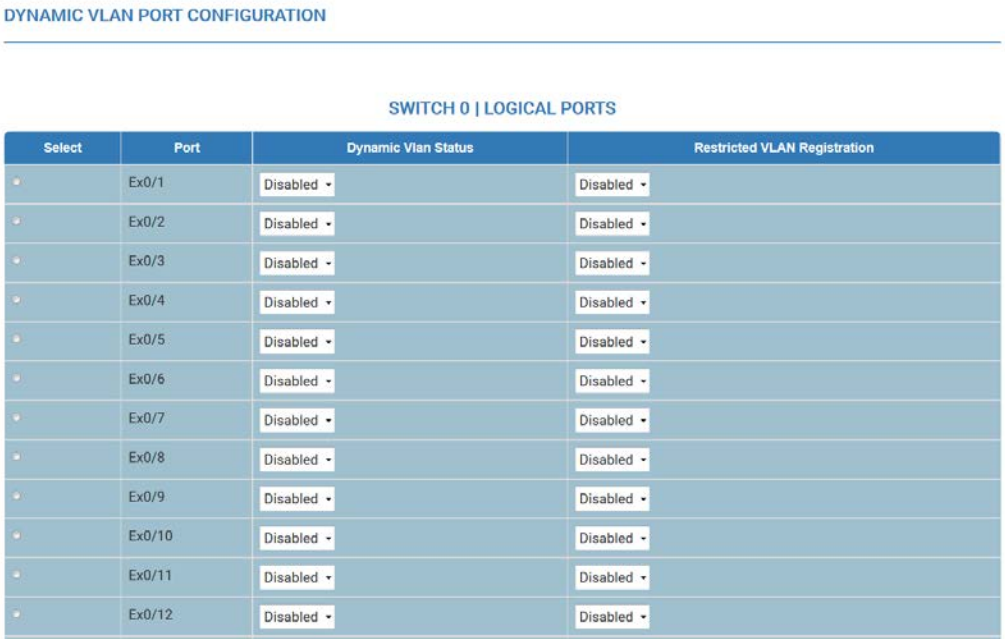
Dynamic Vlan Status - Select the administrative status requested by management for GVRP. By default, the status is set as Enabled for the default context ID (that is, 0) and is set as Disabled for other context IDs. The list contains:

* Enabled **-** Enables GVRP on the switch, on all ports for which GVRP is not specifically disabled in the Dynamic Vlan Port Configuration page..

* Disabled - Disables GVRP on all ports of the switch and transparently forwards all GVRP packets.

The administrative status affects all GVRP applicant and registrar state machine. All GVRP state machines on all ports are idle when status is changed from Disabled to Enabled.

4.5.2 Port Settings



DYNAMIC VLAN PORT CONFIGURATION

SWITCH 0 | LOGICAL PORTS

Select	Port	Dynamic Vlan Status	Restricted VLAN Registration
○	Ex0/1	Disabled	Disabled
○	Ex0/2	Disabled	Disabled
○	Ex0/3	Disabled	Disabled
○	Ex0/4	Disabled	Disabled
○	Ex0/5	Disabled	Disabled
○	Ex0/6	Disabled	Disabled
○	Ex0/7	Disabled	Disabled
○	Ex0/8	Disabled	Disabled
○	Ex0/9	Disabled	Disabled
○	Ex0/10	Disabled	Disabled
○	Ex0/11	Disabled	Disabled
○	Ex0/12	Disabled	Disabled

Fig: Dynamic Vlan Port Configuration

The *Port Settings* link opens the **Dynamic Vlan Port Configuration** Page.
This page allows the user to configure the dynamic VLAN feature related parameters for each physical port available in the switch.

The table below lists the fields present in this page.
Select - Click to select the port for which the configuration needs to be done.
Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
Dynamic Vlan Status   Select the state of GVRP operation in the port. This state affects all GVRP applicant and registrar state machines in the port. All GVRP state machines in the port are reset once the state is changed from Disabled to Enabled.
By default, the state is set as Enabled on all physical ports. The list contains:
* Enabled - Enables GVRP in the port, only if the dynamic VLAN feature (Dynamic Vlan Status) is globally enabled. Otherwise GVRP is not enabled in the port. Once the dynamic VLAN feature (Dynamic Vlan Status) is globally disabled, GVRP enabled in the port is also disabled.
* Disabled - Disables GVRP in the port, even if the dynamic VLAN feature (Dynamic Vlan Status) is globally enabled. Silently discards any received GVRP packets and does not propagate GVRP registrations from other ports.

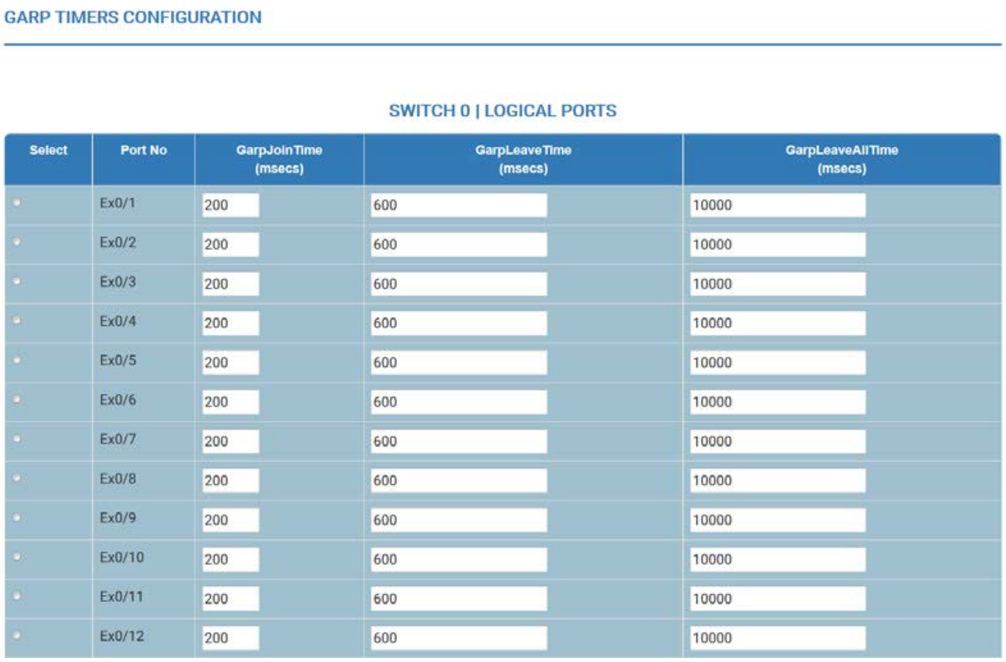
Restricted VLAN Registration Select whether to restrict GVRP from dynamically registering the VLAN.

By default, the registration is set as Disabled. The list contains:

* Enabled - Enables restricted VLAN registration. That is, the creation or modification of a dynamic VLAN entry is permitted only for VLANs for which static VLAN registration entries exist.

* Disabled - Disables restricted VLAN registration. That is, the creation or modification of a dynamic VLAN entry is permitted for all VLANs.

4.5.3 GarpTimers



GARP TIMERS CONFIGURATION

SWITCH 0 | LOGICAL PORTS

Select	Port No	GarpJoinTime (msecs)	GarpLeaveTime (msecs)	GarpLeaveAllTime (msecs)
○	Ex0/1	200	600	10000
○	Ex0/2	200	600	10000
○	Ex0/3	200	600	10000
○	Ex0/4	200	600	10000
○	Ex0/5	200	600	10000
○	Ex0/6	200	600	10000
○	Ex0/7	200	600	10000
○	Ex0/8	200	600	10000
○	Ex0/9	200	600	10000
○	Ex0/10	200	600	10000
○	Ex0/11	200	600	10000
○	Ex0/12	200	600	10000

Fig: Garp Timers Configuration

The *GarpTimers* link opens the **Garp Timers Configuration** Page.

This page allows the user to configure the timer used in GARP on physical ports available in the switch. GARP uses these timer values to control the transmission of GARP PDUs used in synchronizing the attribute information between the switches, and in registering and de-registering of attribute values.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port No - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

GarpJoinTime (msecs) - Enter the time duration till which a GARP participant must wait for its join message to be acknowledged before re-sending the join message. The join message is retransmitted only once, if the initial message is not acknowledged. This timer is started when the initial join message is sent.

The join message is sent by a GARP participant to another GARP participant for registering:

* Its attributes with other participant

* Its manually configured attributes

* Attributes received from a third GARP participant

This value is represented in milliseconds. Default value is 200 milliseconds. You can set the value as multiple of tens only (that is, as 210, 220, 230 and so on).

This value should satisfy the condition:

GarpJoinTime > 0 and (2*GarpJoinTime) < GarpLeaveTime.

GarpLeaveTime (msecs) - Enter the time duration till which a GARP participant must wait for any join message before removing attribute details (that is, waiting time for a registrar to move from empty state (MT) to leave state (LV)). This timer is started when a leave message is sent to de-register the attribute details.

The leave messages are sent from a GARP participant to another participant in the following scenario:

* Its attributes should be de-registered

* Its attributes are manually de-registered

* It receives leave messages from a third GARP participant

This value is represented in milliseconds. Default value is 600 milliseconds. You can set the value as multiple of tens only (that is, as 610, 620, 630 and so on).

The leave time should be greater than or two times as that of the GarpJoinTime.

That is, the maximum value of the leave time cannot be more than two times of the join time.

For example, if you configure join time as 500 milliseconds, then the leave time value can be from 510 milliseconds to 1000 milliseconds only.

GarpLeaveAllTime (msecs) - Enter the time period during which the details of the registered attributes are maintained. The attribute details should be re-registered after this time interval. A leaveall message is sent from a GARP participant to other GARP participants, after this time interval. This timer is started once a GARP participant started or reregistration is done.

The leaveall messages are sent from a GARP participant to other participants for:

* De-registering all registered attributes

* Re-registering all attributes with each of the participants

This value is represented in milliseconds. Default value is 10000 milliseconds. You can set the value as multiple of tens (that is, as 10010, 10020 and so on).

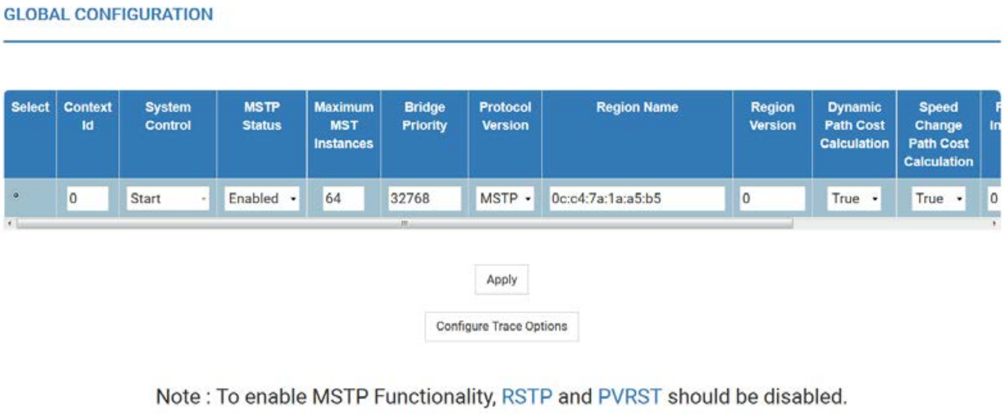
The leaveall time should be greater than 0 and greater than GarpLeaveTime.

4.6 MSTP

The MSTP link allows you to configure the MSTP settings for switch. User can configure MSTP on the following eight pages.

- Basic Settings
- Timers
- Port configuration
- VLAN Mapping
- Port Settings
- CIST Port Status
- Bridge Priority
- MSTP Traces

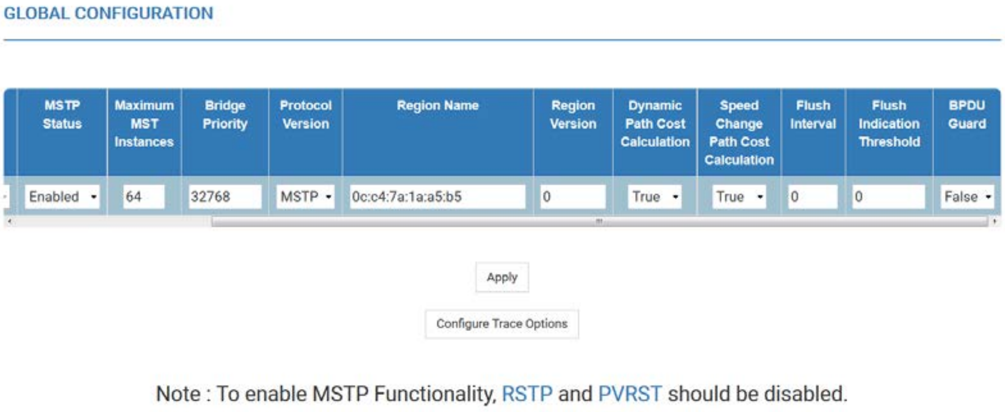
4.6.1 Basic Settings



GLOBAL CONFIGURATION

Select	Context Id	System Control	MSTP Status	Maximum MST Instances	Bridge Priority	Protocol Version	Region Name	Region Version	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	F In
○	0	Start	Enabled	64	32768	MSTP	0c:c4:7a:1a:a5:b5	0	True	True	0

Note : To enable MSTP Functionality, RSTP and PVRST should be disabled.



GLOBAL CONFIGURATION

MSTP Status	Maximum MST Instances	Bridge Priority	Protocol Version	Region Name	Region Version	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
Enabled	64	32768	MSTP	0c:c4:7a:1a:a5:b5	0	True	True	0	0	False

Note : To enable MSTP Functionality, RSTP and PVRST should be disabled.

Fig: Global Configuration

The *Basic Settings* link opens the **Global Configuration** page.

This page allows the user to configure, for each available virtual contexts, the MST module parameters that are used globally in the switch for all ports.

The table below lists the fields present in this page.

Select - Click to select the context for which the configuration needs to be done.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

System Control - Select the administrative shutdown status requested by management for the MST feature.

This status allows the user to set the availability of the MST feature on all ports in the switch.

By default, the system control is set as Start. The list contains:

* Start - Activates the MST feature in the switch on all ports. The required memory is allocated for the feature.

* Shutdown - Stops the MST feature in the switch on all ports. The allocated memory is released and made available for other activities.

>

* The administrative status is grayed out and cannot be configured, if the MSTP
Status is set as Enabled.

* The administrative status can be set as Shutdown, only if the MSTP Status is set as Disabled.

* The administrative status can be set as Start, only if the RSTP System Control and PVRST System Control are set as Shutdown.

MSTP Status - Select the administrative status requested by management for the MST feature. MSTP is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It provides multiple forwarding paths for data traffic and enables load balancing.

By default, the MSTP Status is set as Enabled. The list contains:

* Enabled - Enables the MST feature in the switch on all ports.

* Disabled - Disables the MST feature in the switch on all ports.

>

* To enable MSTP globally in the switch, the MSTP System Control status should be set as Start.

* All the fields in this page (except the System Control) are grayed out and cannot be configured, once the MSTP status is set as Disabled.

Maximum MST Instances - Enter the maximum number of spanning trees to be allowed in the switch. This value represents the maximum number of active MSTIs that can be created. This allows the user to limit the number of spanning tree instances to be allowed in the switch.

This does not count the special MSTID such as PTETID (Provider Backbone Bridging - Traffic Engineering Multiple Spanning Tree ID), used to identify VIDs used by ESPs.

This value ranges between 1 and 64. Default value is 64.

Bridge Priority - Enter the priority value that is assigned to the switch. This value is used during the election of CIST root, CIST regional root and IST root.

This value ranges between 0 and 61440. Default value is 32768.

The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

Protocol Version - Select the version of STP in which the switch is currently running. This allows the user to set the type of STP to be used by the switch to form loop-free topology.

By default the version is set as MSTP. The list contains:

* STP - Removes the loop using the STP specified in IEEE 802.1D.

* RSTP - Removes the loop using the RSTP specified in IEEE 802.1w.

* MSTP - Removes the loop using the MSTP specified in IEEE 802.1s.

> The fields Region Name and Region Version are grayed out and cannot be configured, once the protocol version is set as STP or RSTP.

Region Name - Enter the unique name for the region- s configuration to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances.

By default, the region name is same as that of the Switch Base MAC Address configured in the Factory Default Settings page.

This value is an octet string of maximum size 32.

Region Version - Enter the unique identifier that represents the specific MST region.

This value ranges between 0 and 65535.

Dynamic Path Cost Calculation - Select whether the dynamic path cost calculation is allowed. The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. According to the specification, path cost is calculated by dividing the speed with bandwidth of the segment connected to the port.

By default, the dynamic calculation is set as False. The list contains:

* True - Dynamically calculates path cost based on the speed of the ports whose

Admin State is set as Up at that time. The path cost is not changed based on the operational status of the ports, once calculated.

* False - Dynamically calculates path cost based on the link speed at the time of port creation.

The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation, if you have manually assigned Path Cost for the port.

Speed Change Path Cost Calculation - Select whether the dynamic path cost is to be calculated for ports whose speed changes dynamically. This feature is mainly used for LA ports whose speed changes due to the addition and deletion of ports from the port channel.

By default, the speed change path cost calculation is set as False. The list contains:

* True - Dynamically calculates path cost for ports based on their speed at that time. The path cost is calculated, if the speed of the port changes.

* False - Does not dynamically calculate the path cost for ports based their speed at that time.

The manually assigned path cost is used irrespective of the status (True or False) of the path cost calculation, if you have manually assigned Path Cost for the port.

Flush Interval - Enter the the flush interval timer value (in centi-seconds), which controls the number of flush indications invoked from spanning-tree module per instance basis.

This value ranges between 0 and 500. Default value is 0.

> The flush interval is grayed out and cannot be configured, if the RSTP Status is set as Disabled.

Flush Interval Threshold - Enter the flush indication threshold value for a specific instance. This indicates the number of flush indications to go before the flush-interval timer method triggers. This value ranges between 0 and 65535. Default value is 0.

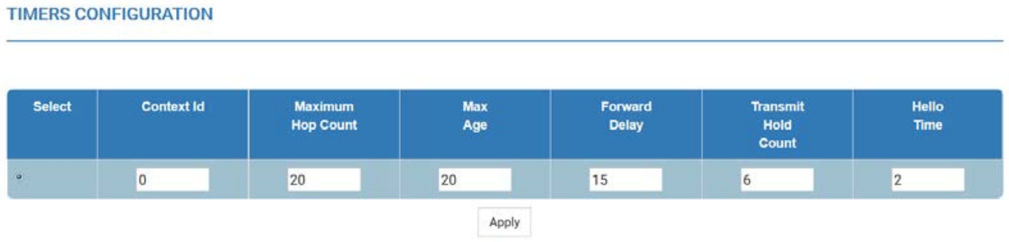
> The flush interval threshold is grayed out and cannot be configured, if the RSTP Status is set as **Disabled. BPDU Guard** - Select whether an interface in the error-disabled state when it receives a BPDU packet.

By default, the BPDU guard is set as False. The list contains:

* True - Enables bpduguard feature on all edge ports.

* False - Disables bpduguard feature on all edge ports.

4.6.2 Timers



TIMERS CONFIGURATION

Select	Context Id	Maximum Hop Count	Max Age	Forward Delay	Transmit Hold Count	Hello Time
●	0	20	20	15	6	2

Fig: Timers Configuration

The *Timers* link opens the **Timers Configuration** page.
This page allows the user to configure the timers used in MSTP protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports.

The table below lists the fields present in this page.
Select - Click to select the context for which the configuration needs to be done.
Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.
>
* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).
This value ranges between 0 and 65535. The default value is 0.
Maximum Hop Count - Enter the maximum hop count value that represents the maximum number of switches that a packet can cross before it is dropped. This value is used by the switch to avoid infinite looping of the packets, if it is elected as the root switch in the topology.
The root switch always transmits a BPDU with the maximum hop count value. The receiving switch decrements the value by one and propagates the BPDU with modified hop count value. The BPDU is discarded and the information held is aged out, when the count reaches 0.
This value ranges between 6 and 40. Default value is 20.
Max Age - Enter the maximum expected arrival time (in seconds) of hello BPDUs. This value represents the time interval until which the information received in the MSTP BDPU is valid.
This value is used by MSTP while interacting with switches using STP, RSTP or PVRST as its spanning tree protocol.
This value ranges between 6 and 40 seconds. Default value is 20 seconds.
Forward Delay - Enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state.
This value ranges between 4 and 30 seconds. Default value is 15 seconds.

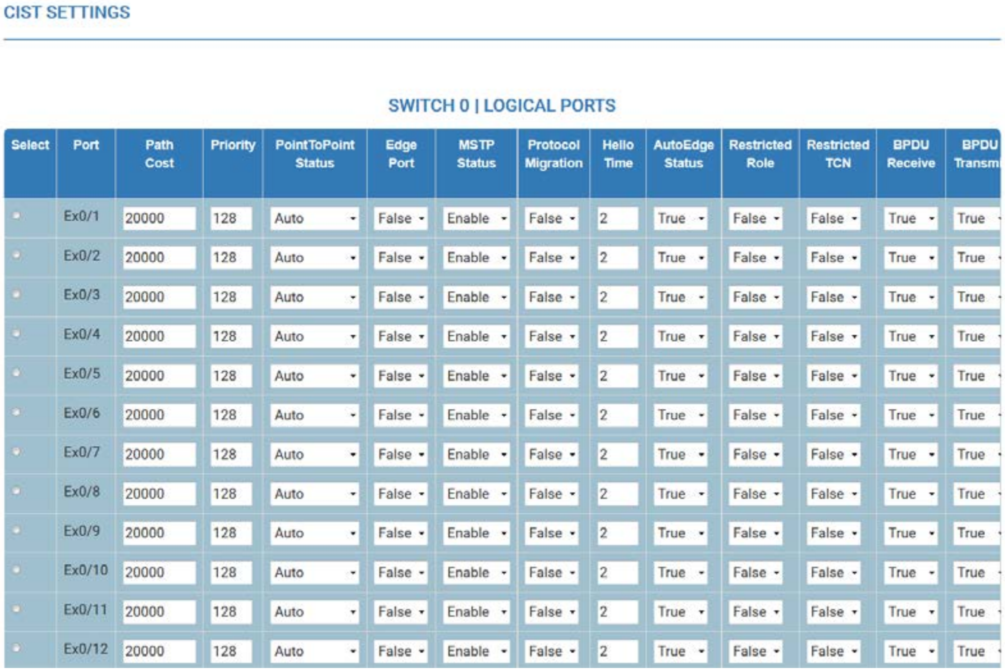
Transmit Hold Count - Enter the maximum number of packets that can be sent in a given interval. This value is configured to avoid flooding. Port transmit state machine uses this value to limit the maximum transmission rate.

This value ranges between 1 and 10. Default value is 6.

Hello Time - Displays the time interval (in seconds) between two successive configuration BPDUs generated by the root switch.

This value can be either 1 or 2 seconds. Default value is 2.

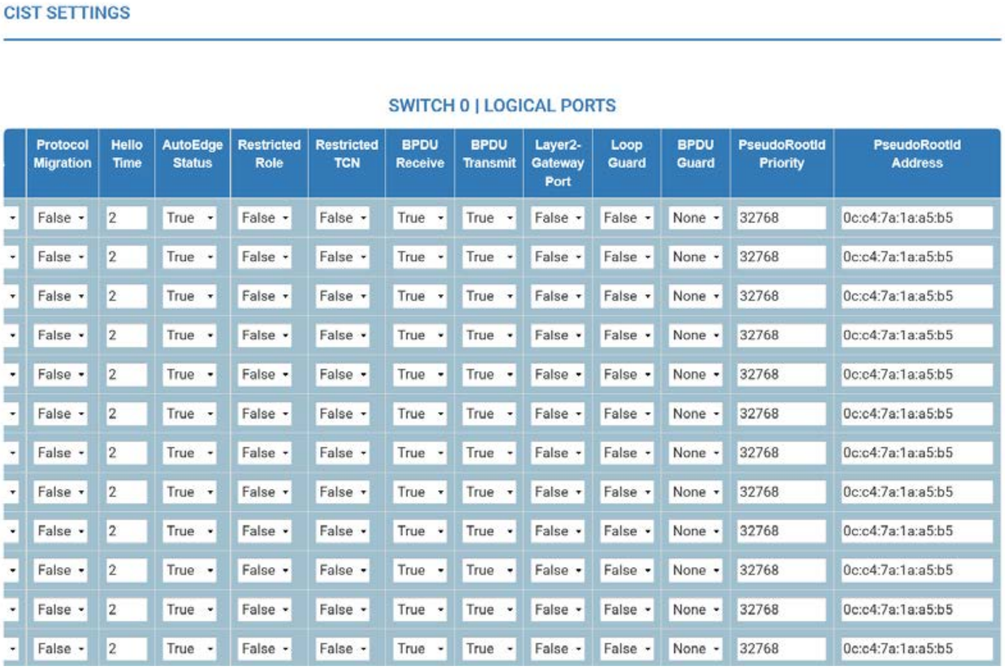
4.6.3 Port Configuration



CIST SETTINGS

SWITCH 0 | LOGICAL PORTS

Select	Port	Path Cost	Priority	PointToPoint Status	Edge Port	MSTP Status	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN	BPDU Receive	BPDU Transm
○	Ex0/1	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/2	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/3	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/4	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/5	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/6	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/7	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/8	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/9	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/10	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/11	20000	128	Auto	False	Enable	False	2	True	False	False	True	True
○	Ex0/12	20000	128	Auto	False	Enable	False	2	True	False	False	True	True



CIST SETTINGS

SWITCH 0 | LOGICAL PORTS

	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN	BPDU Receive	BPDU Transmit	Layer2-Gateway Port	Loop Guard	BPDU Guard	PseudoRootId Priority	PseudoRootId Address
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5
	False	2	True	False	False	True	True	False	False	None	32768	0c:c4:7a:1a:a5:b5

Fig: CIST Settings

The *Port Configuration* link opens the **CIST Settings** page.

This page allows the user to configure the port information for CIST, which spans across the entire topology irrespective of MST and SST regions. CIST is a single common/active topology consisting of all switches in the topology.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Path Cost - Enter the path cost that contributes to the path cost of paths containing the port. The paths- path cost is used during calculation of shortest path to reach the CIST root. The path cost represents the distance between the root port and designated port.

This value ranges between 1 and 200000000. Default value is 200000 for all physical ports and 199999 for port channels.

>

* The default value is used as the path cost, if you have not configured it, and the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if you have not manually configured the path cost and one of these fields is set as True.

* The configured value is used as the path cost irrespective of the status (True or False) of the fields Dynamic Path Cost Calculation and Speed Change Path Cost Calculation, if you have configured it.

Priority - Enter the priority value that is assigned to the port. This value is used during the role selection process. The Role is computed for the port for instances to which the port is assigned as member.

This value ranges between 0 and 240. Default value is 128.

This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on.

Point-to-Point Status - Select the administrative point-to-point status of the LAN segment attached to the port.

By default, the point-to-point status is set as Auto. The list contains:

* ForceTrue - Always treats the port as if it is connected to a point-to-point link.

* ForceFalse - Always treats the port as if it is having a shared media connection.

* Auto - Treats the ports as having a shared media connection or a point-point link based on the prevailing conditions.

Port is considered to have a point-to-point link if,

* It is an aggregator and all of its members can be aggregated.

* The MAC entity is configured for full Duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as Auto).

Otherwise port is considered to have a shared media connection

Edge Port - Select the administrative value of the Edge Port parameter.

By default, the edge port administrative value is set as False. The list contains:

* True - Sets the port as an edge port (that is, the Port State is immediately set as forwarding). It is connected directly to a single end station. It allows MSTP to converge faster and does not wait to receive BPDUs.

* False - Sets the port as a non-Edge port (that is, the spanning tree process is performed using the MSTP). It is connected to a routing device such as switch.

The value of the Edge Port parameter depends on the option selected in the field Auto Edge Status. The value of the Edge Port parameter is automatically updated, if the Auto Edge Status is set as True.

MSTP Status - Select the MSTP status of the port for all spanning tree instances. This value will override the port- s status in the MSTI contexts.

By default, the status is set as Enable. The list contains:

* Enable - Enables MST in the port. MAC frames are forwarded and their source addresses are learnt.

* Disable - Disables MST in the ports. MAC frames are not forwarded and their source addresses are not learnt.

Protocol Migration - Select the protocol migration state of the port. This is used to control the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches.

By default, protocol migration is set as False. The list contains:

* True - Allows the port to transmit BPDUs based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit MSTP BPDUs without instance information.

* False - Does not perform protocol migration mechanism. The port always transmits the standard MSTP BPDUs.

> The protocol migration is grayed out and cannot be configured, if the MSTP
Status is set as Disable.

Hello Time - Enter the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port.

This value can be either 1 or 2 seconds. Default value is 2 seconds.

Auto Edge Status - Select whether the Edge Port parameter of the port is detected automatically or configured manually.

By default, the auto edge status is set as True. The list contains:

* True - Automatically detects and sets value for Edge Port parameter. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received by that port. This overrides the value set in the field Edge Port, based on the reception of BPDU.

* False - Uses the manually configured value for the Edge Port parameter. The value set in the field Edge Port is used for the Edge Port parameter.

Restricted Role - Select whether the selection of port Role as root can be blocked during the role selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology.

By default, the restricted role is set as False. The list contains:

* True - Blocks the port from being selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected. You can apply this option for ports that are not fully under your control.

> The blocking of port from being selected as a root port may cause lack of spanning tree connectivity.

* False - Includes all available ports of the topology, in the root selection process to select the root for CIST or any MSTI.

Restricted TCN - Select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core region of the network from causing address flushing in the region.

By default, the restricted TCN is set as False. The list contains:

* True - Blocks the port from propagating the received topology change notifications and topology changes to other ports.

> The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.

* False - Allows the port to propagate the received topology change notifications and topology changes to other ports.

BPDU Receive - Select the processing status of the received MSTP BPDUs.

By default, this field is set as True. The list contains:

* True - Normally processes the MSTP BPDUs received on the port.

* False - Discards the MSTP BPDUs received on the port.

BPDU Transmit - Select the BPDU transmission status of the port.

By default, this field is set as True. The list contains:

* True - Transmits the MSTP BPDUs from the port.

* False - Blocks the transmission of MSTP BPDUs from the port.

> This field should be set as False, for ports to be configured as Layer2-Gateway Port.

Layer2-Gateway Port - Select whether the port acts as a normal port or as a L2GP. L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when Admin State is set as Up.

By default, this field is set as false. The list contains:

* True - Allows the port to operate as a L2GP.

* False - Allows the port to operate as a normal port.

>

* BPDU Transmit should be set as False, before configuring the port as a Layer 2 gateway port.

* L2GP should not be enabled on ports whose Bridge Port Type is set as PIPs or
CBPs, as the effect is unknown.

* Restricted Role and Restricted TCN configuration are disabled for the port configured as L2GP.

* L2GP cannot be enabled on ports with SISP enabled interfaces.

* The Port State of the L2GP is always set as discarding.

Loop Guard - Select whether the loop guard feature is enabled or disabled. This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic.

By default, this field is set as False. The list contains:

* True - Enables the loop guard feature in the port.

* False - Disables the loop guard feature in the port.

BPDU Guard - Select whether the BPDU guard feature is enabled or disabled. This feature disables the port and puts the port in error-disabled state on receiving BPDU, if the portfast feature is enabled on the port. This feature prevents the devices connected to the port from participating in STP operation. Once disabled, the port can be enabled only manually.

By default, this field is set as None. The list contains:

* None - Removes the BPDU guard feature.

* True - Enables the BPDU guard feature in the port.

* False - Disables the BPDU guard feature in the port.

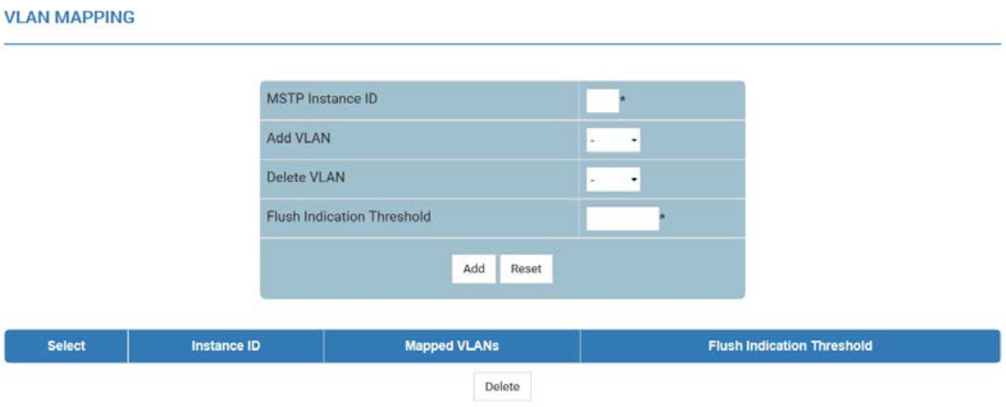
PseudoRootId Priority - Enter the priority of the pseudo root. This value is used by port configured as L2GP (that is, the field Layer2-Gateway Port is set as True).

This value ranges between 0 and 61440. Default value is the priority value assigned to the switch. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

PsuedoRootId Address - Enter the unicast MAC address of the pseudo root. This value is used by port configured as L2GP (that is, the field Layer2-Gateway Port is set as True).

Default value is the base MAC address assigned to the switch.

4.6.4 VLAN Mapping



Select	Instance ID	Mapped VLANs	Flush Indication Threshold

Fig: VLAN Mapping

The *VLAN Mapping* link opens the **VLAN Mapping** page.

This page allows the user to map / unmap VLANs for each instance of MSTP and create/delete instance specific information for the member ports of the VLAN. The instance specific information for the port in one instance is independent of its information in other instance.

The table below lists the fields present in this page.

MSTP Instance ID - Enter an integer value that is used to uniquely identify an instance of the MSTP. This value ranges between 1 and 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID, which can be used by ESPs.

>

* Any external agent can separately provide ESPs. The ESPs do not use spanning tree.

Add VLAN - Select the VLAN that should be mapped to the MSTP instance. The list contains VLAN Name for the VLANs available in the switch at that time.

The mapping of VLAN to the MSTP instance is not done again, if the VLAN is already mapped to that instance.

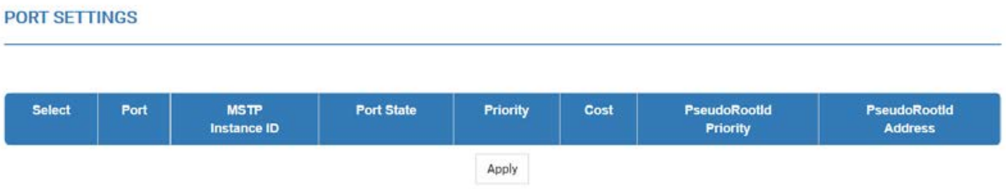
Delete VLAN - Select the VLAN that should be unmapped from the MSTP instance. The list contains VLAN Name for the VLANs available in the switch at that time.

The unmapping of VLAN from the MSTP instance is not done, if the VLAN is already unmapped from that instance.

Mapped VLANs - Displays the VLAN mapped to the MSTP instance.

Flush Indication Threshold - Enter the flush indication threshold value for a specific instance. This indicates the number of flush indications to go before the flush-interval timer method triggers. This value ranges between 0 and 65535. The default value is 0.

4.6.5 Port Settings


PORT SETTINGS

Select	Port	MSTP Instance ID	Port State	Priority	Cost	PseudoRootId Priority	PseudoRootId Address

Fig: Port Settings

The *Port Settings* link opens the **Port Settings** page.

This page allows the user to configure port specific information for all ports available in the switch on per port basis. It also allows the user to assign ports to specific MSTP instances so that the instances can make use of the port information.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

MSTP Instance ID - Displays an integer value that is used to uniquely identify an instance of the MSTP.

This value ranges between 1 and 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID, which can be used by ESPs.

>

* Any external agent can separately provide ESPs. The ESPs do not use spanning tree.

Port State - Select the status of the MSTP in the port. The list contains:

* Enabled - Enables MSTP in the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data.

* Disabled - Disables MSTP in the port. The port does not participate in the STP process and is not ready to transmit/receive BPDUs and data.

Priority - Enter the priority value that is assigned to the port. This value is used during the role selection process. The Role is computed for the port for instances in which the port is assigned as member.

This value ranges between 0 and 240. Default value is 128.

This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on.

Cost - Enter the cost that contributes to the path cost of paths containing the port.

The paths - path cost is used during calculation of shortest path to reach the MSTI root.

The path cost represents the distance between the root port and designated port.

This value ranges between 1 and 200000000. Default value is 200000 for all physical ports and 199999 for port channels.

>

* The default value is used as the path cost, if you have not configured it, and the Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if you have not manually configured the path cost and one of these fields is set as True.

* The configured value is used as the path cost irrespective of the status (True or False) of the fields Dynamic Path Cost Calculation and Speed Change Path Cost Calculation.

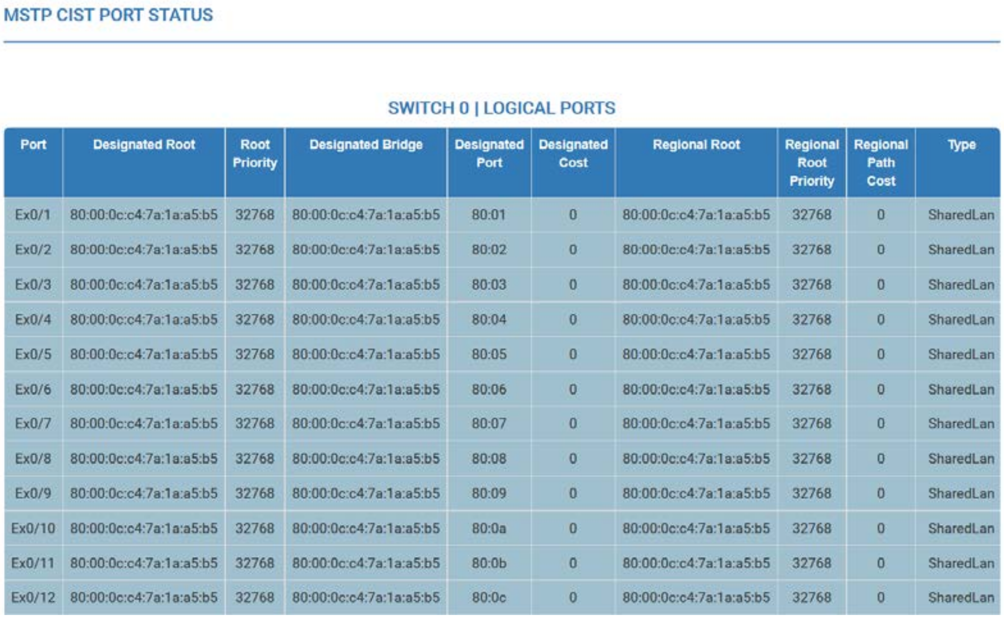
PseudoRootId Priority - Enter the priority of the pseudo root. This value is used by port configured as L2GP (that is, the field Layer2-Gateway Port is set as True).

This value ranges between 0 and 61440. Default value is the priority value assigned to the switch. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

PsuedoRootId Address - Enter the unicast MAC address of the pseudo root. This value is used by port configured as L2GP (that is, the field Layer2-Gateway Port is set as True).

Default value is the base MAC address assigned to the switch.

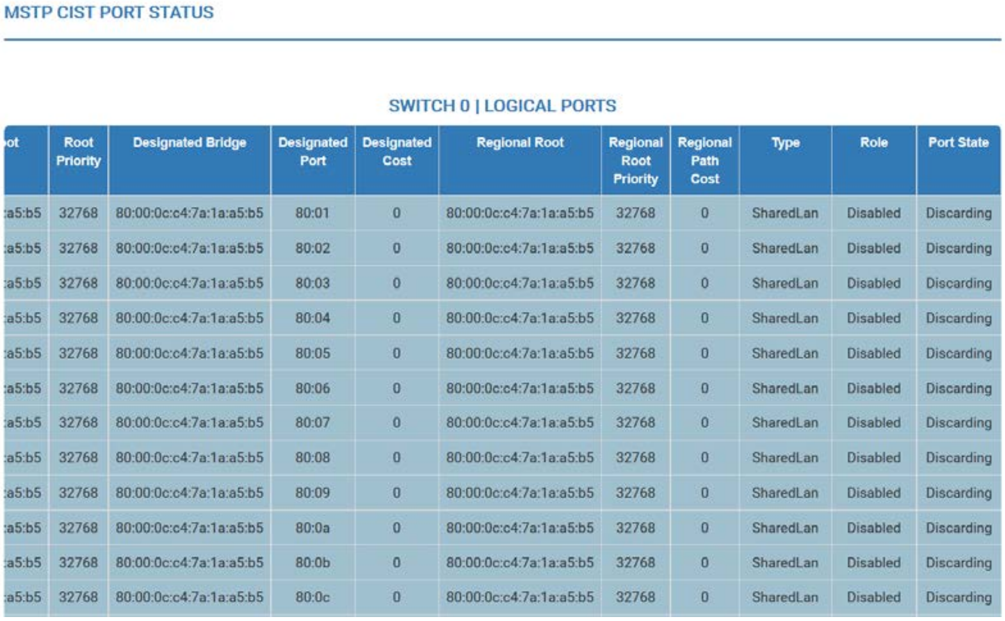
4.6.6 CIST Port Status



MSTP CIST PORT STATUS

SWITCH 0 | LOGICAL PORTS

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type
Ex0/1	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:01	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/2	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:02	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/3	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:03	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/4	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:04	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/5	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:05	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/6	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:06	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/7	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:07	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/8	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:08	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/9	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:09	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/10	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0a	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/11	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0b	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan
Ex0/12	80:00:0c:c4:7a:1a:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0c	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan



MSTP CIST PORT STATUS

SWITCH 0 | LOGICAL PORTS

ot	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:01	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:02	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:03	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:04	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:05	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:06	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:07	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:08	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:09	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0a	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0b	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding
:a5:b5	32768	80:00:0c:c4:7a:1a:a5:b5	80:0c	0	80:00:0c:c4:7a:1a:a5:b5	32768	0	SharedLan	Disabled	Discarding

Fig: MSTP CIST Port Status

The *CIST Port Status* link opens the **MSTP CIST Port Status** page.

This page allows the user to view information maintained by every port of the switch for CIST.

The table below lists the fields present in this page.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Designated Root - Displays the unique identifier of the bridge recorded as the CIST root in the transmitted configuration BPDUs.

This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Root priority - Displays the Bridge Priority that represents the priority of the bridge recorded as the CIST root in the configuration BPDUs transmitted.

This value ranges between 0 and 61440. Default value is 32768.

Designated Bridge - Displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment.

This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Designated Port - Displays the identifier of the port on the Designated Bridge for the port's segment.

This represents the port through which the Designated Bridge forwards frames to and from the segment.

This value is a 2-byte octet string. For example, 80:05.

Designated Cost - Displays the Path Cost of the Designated Port of the segment connected to the port.

This value ranges between 1 and 200000000.

Regional Root - Displays the unique identifier of the bridge recorded as the CIST regional root in the configuration BPDUs transmitted.

This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Regional Root Priority - Displays the Bridge Priority that represents the priority of the bridge recorded as the CIST regional root in the configuration BPDUs transmitted.

This value ranges between 0 and 61440. Default value is 32768.

Regional Path Cost - Displays the port- s Path Cost that contributes to the cost of paths (including the port) towards the CIST Regional Root.

This value ranges between 1 and 200000000.

Type - Displays the operational Point-to-Point Status of the LAN segment attached to the port. The values can be:

* PointtoPoint - Port is treated as if it is connected to a point-to-point link.

* SharedLan **-** Port is treated as if it is having a shared media connection.

You can set the values directly or can set as Auto for the switch to decide about the point-to-point status, in the field Point-to-Point Status provided in the page CIST Settings.

Role - Displays the current role of the port for the spanning tree instance. The values can be:

* Disabled - Port is disabled manually (Port State)or automatically (Link). It does not take part in the spanning tree process.

* Alternate - Port acting as an alternate for the root port, is blocked and not used for traffic. It is enabled and declared as the root port, if the current root port is blocked.

* Backup - Port acting as a backup for a specific designated port. It is blocked and not used for traffic. It is enabled and declared as the designated port, if the active designated port is blocked.

* Root - Port is used to forward data to root bridge directly or through an upstream LAN segment.

* Designated - Port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.

Port State - Displays the current state of the port as defined by the common STP. The values can be:

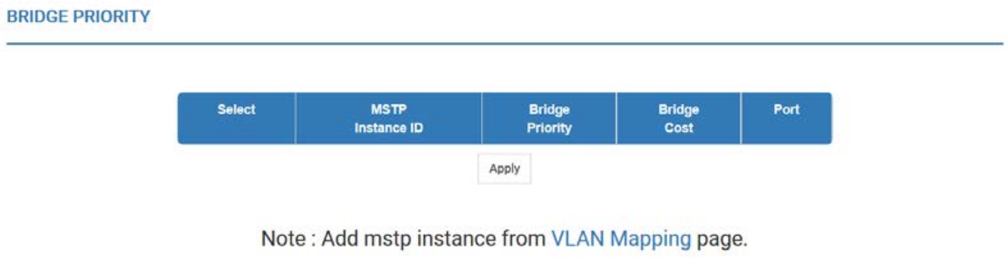
* Disabled - Port is disabled manually (Port State)or automatically (Link). It does not take part in the spanning tree process.

* Discarding - Port is included in the STP process and is ready to learn addresses and forward data.

* Learning - Port is learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data.

* Forwarding - Port is sending and receiving data based on the formed spanning tree topology which is loop free.

4.6.7 Bridge Priority



BRIDGE PRIORITY

Select	MSTP Instance ID	Bridge Priority	Bridge Cost	Port

Note : Add mstp instance from VLAN Mapping page.

Fig: Bridge Priority

The *Bridge Priority* link opens the **Bridge Priority** page.

This page allows the user to configure bridge priority for the MSTI.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

MSTP Instance ID - Displays an integer value that is used to uniquely identify an instance of the MSTP.

This value ranges between 1 and 64. The special value 4094 is used in a switch that supports PBB-TE. This special value represents PTETID that identifies VID, which can be used by ESPs.

>

* Any external agent can separately provide ESPs. The ESPs do not use spanning tree.

Bridge Priority - Enter the writable portion of the MSTI Bridge Identifier comprising of the first two octets.

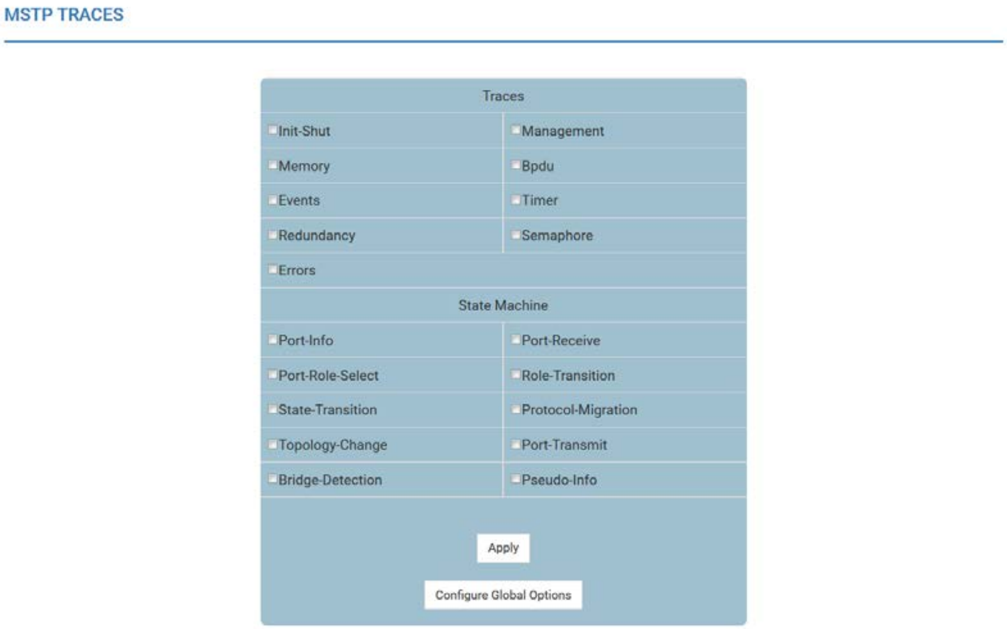
This value ranges between 0 and 61440. Default value is 32768.

This value should be set in steps of 4096.

Bridge Cost - Displays the cost of the path to the MSTI Regional Root as seen by this bridge.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

4.6.8 MSTP Traces



MSTP TRACES

Traces	
□Init-Shut	□Management
□Memory	□Bpdu
□Events	□Timer
□Redundancy	□Semaphore
□Errors	
State Machine	
□Port-Info	□Port-Receive
□Port-Role-Select	□Role-Transition
□State-Transition	□Protocol-Migration
□Topology-Change	□Port-Transmit
□Bridge-Detection	□Pseudo-Info

Fig: MSTP Traces

The *MSTP Traces* link opens the **MSTP Traces** page.

This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.

Traces - Select the traces for which debug statements is to be generated. The options are:

* Init-Shut - Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.

* Management - Generates debug statements for management traces. This trace is generated whenever you configure any of the STP features.

* Memory - Generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.

* Bpdu - Generates debug statements for BPDU related traces. This trace is generated on failed and successful reception, transmission and processing of BPDUs.

* Events - Generates debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.

* Timer - Generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of STP timers. The different STP timers are:

1. Forward delay timer
2. Hello timer
3. Migration delay timer
4. Recent backup while timer
5. Received information while timer
6. Recent root while timer
7. Topology change timer
8. Hold timer
9. Edge delay timer
10. Rapid age duration timer
11. Pseudo information hello timer

* Redundancy - Generates debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.

* Semaphore - Generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.

* Errors - Generates debug statements for all failure traces of the above mentioned traces.

State Machine - Select the SEMs (State Event Machines) for which debug statements is to be generated to denote the event and state of the selected SEM. The list contains:

* Port-Info - Generates debug statements for port information SEM.

* Port-Receive - Generates debug statements for port receive SEM.

* Port-Role-Select - Generates debug statements for role selection SEM.

* Role-Transition - Generates debug statements for role transition SEM.

* State-Transition - Generates debug statements for state transition SEM.

* Protocol-Migration - Generates debug statements for protocol migration SEM.

* Topology-Change - Generates debug statements for topology change SEM.

* Port-Transmit - Generates debug statements for port transmit SEM.

* Bridge-Detection - Generates debug statements for bridge detection SEM.

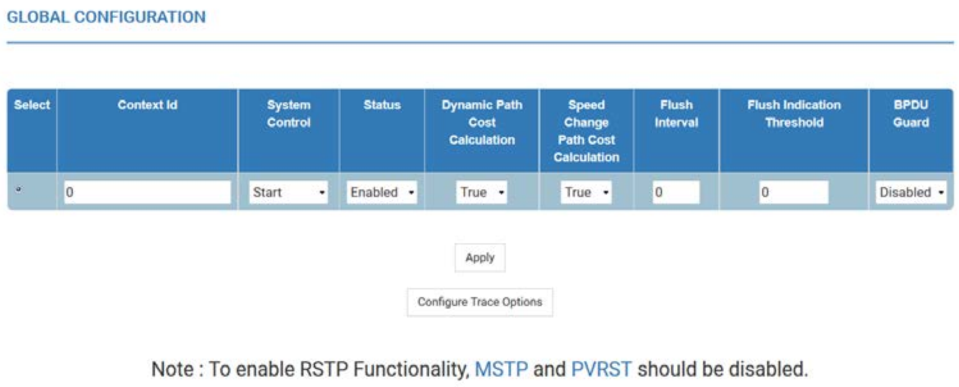
* Pseudo-Info - Generates debug statements for port receive pseudo information SEM.

4.7 RSTP

The RSTP link allows you to configure the RSTP settings for switch. User can configure RSTP on the following five pages.

- Global Settings
- Basic Settings
- Port Settings
- Port Status
- RSTP Traces

4.7.1 Global Settings



GLOBAL CONFIGURATION

Select	Context Id	System Control	Status	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
●	0	Start	Enabled	True	True	0	0	Disabled

Note : To enable RSTP Functionality, MSTP and PVRST should be disabled.

Fig: Global Configuration

The *Global Settings* link opens the **Global Configuration** page.

This page allows the user to configure, for each available virtual context, the RSTP module parameters that are used globally in the switch for all ports available in the switch.

The table below lists the fields present in this page.

Select - Click to select the context for which the configuration needs to be done.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

System Control - Select the administrative system control status requested by management for the RSTP feature.

This status allows the user to set the availability of the RSTP feature on all ports in the switch.

By default, system control is set as Shutdown. The list contains:

* Start - Activates the RSTP feature in the switch on all ports. The required memory is allocated for the feature.

* Shutdown - Stops the RSTP feature in the switch on all ports. The allocated memory is released and made available for other activities.

>

* The administrative status is grayed out and cannot be configured, if the RSTP Status is set as Enabled.

* The administrative status can be set as Shutdown, only if the RSTP Status is set as Disabled.

* The administrative status can be set as Start, only if the MSTP System Control and PVRST System Control are set as Shutdown.

Status - Select the administrative module status requested by management for the RSTP feature. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. By default, status is set as Disabled. The list contains:

* Enabled - Enables the RSTP feature in the switch on all ports.

* Disabled - Disables the RSTP feature in the switch on all ports.

> To enable RSTP globally in the switch, the RSTP System Control status should be set as Start.

Dynamic Path Cost Calculation - Select whether the dynamic path cost calculation is allowed. The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. According to the specification, path cost is calculated by dividing the speed with bandwidth of the segment connected to the port.

By default, the dynamic calculation is set as False. The list contains:

* True - Dynamically calculates path cost based on the speed of the ports whose Admin State is set as Up at that time. The path cost is not changed based on the operational status of the ports, once calculated.

* False - Dynamically calculates path cost based on the link speed at the time of port creation. The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation, if you have manually assigned Path Cost for the port.

> The dynamic path cost calculation is grayed out and cannot be configured, if the
RSTP Status is set as Disabled.

Speed Change Path Cost Calculation - Select whether the dynamic path cost is to be calculated for ports whose speed changes dynamically. This feature is mainly used for LA ports whose speed changes due to the addition and deletion of ports from the port channel.

By default, the speed change path cost calculation is set as False. The list contains:

* True - Dynamically calculates path cost for ports based on their speed at that time. The path cost is calculated, if the speed of the port changes.

* False - Does not dynamically calculate the path cost for ports based their speed at that time. The manually assigned path cost is used irrespective of the status (True or False) of the dynamic path cost calculation, if you have manually assigned Path Cost for the port.

Flush Interval - Enter the flush interval timer value (in centi-seconds), which controls the number of flush indications invoked from spanning-tree module per instance basis.

This value ranges between 0 and 500. Default value is 0.

> The flush interval is grayed out and cannot be configured, if the RSTP Status is set as Disabled.

Flush Interval Threshold - Enter the flush indication threshold value for a specific instance. This indicates the number of flush indications to go before the flush-interval timer method triggers.

This value ranges between 0 and 65535. Default value is 0.

> The flush interval threshold is grayed out and cannot be configured, if the RSTP Status is set as Disabled.

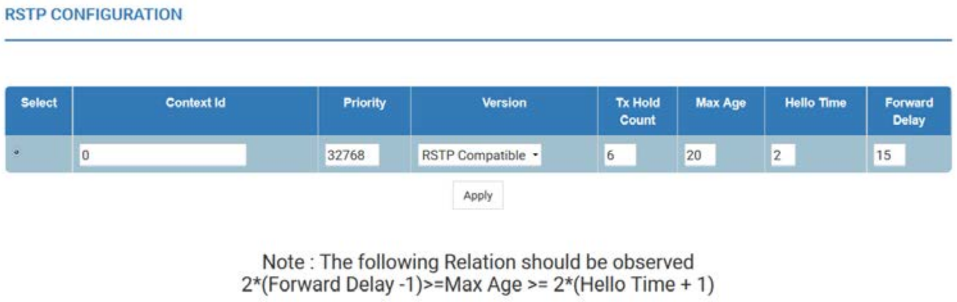
BPDU Guard - Select whether an interface in the error-disabled state when it receives a BPDU packet.

By default, the BPDU guard is set as Disabled. The list contains:

* Enabled - Enables bpduguard feature on all edge ports.

* Disabled - Disables bpduguard feature on all edge ports.

4.7.2 Basic Settings



RSTP CONFIGURATION

Select	Context Id	Priority	Version	Tx Hold Count	Max Age	Hello Time	Forward Delay
●	0	32768	RSTP Compatible	6	20	2	15

Note : The following Relation should be observed
2*(Forward Delay -1)>=Max Age >= 2*(Hello Time + 1)

Fig: RSTP Configuration

The *Basic Settings* link opens the **RSTP Configuration** page.

This page allows the user to configure the timers used in RSTP protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports.

The parameters in the page are not populated with the values (that is, the
page is blank), if the RSTP System Control status is set as Shutdown.

The table below lists the fields present in this page.

Select - Click to select the context for which the configuration needs to be done.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Priority - Enter the priority value that is assigned to the switch. This value is used during the election of root.

This value ranges between 0 and 61440. Default value is 32768.

The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

Version - Select the version of STP in which the switch is currently running. This allows the user to set the type of STP to be used by the switch for forming loop-free topology.

By default the version is set as RSTP Compatible. The list contains:

* STP Compatible - Removes the loop using the STP specified in IEEE 802.1D.

* RSTP Compatible - Removes the loop using the RSTP specified in IEEE

802.1w.

Tx Hold Count - Enter the maximum number of packets that can be sent in a given interval. This value is configured to avoid flooding. Port transmit state machine uses this value to limit the maximum transmission rate.

This value ranges between 1 and 10. Default value is 6.

Max Age - Enter the maximum expected arrival time (in seconds) of hello BPDUs. This value represents the time interval until which the information received in the RSTP BDPU is valid.

This value ranges between 6 and 40 seconds. Default value is 20 seconds.

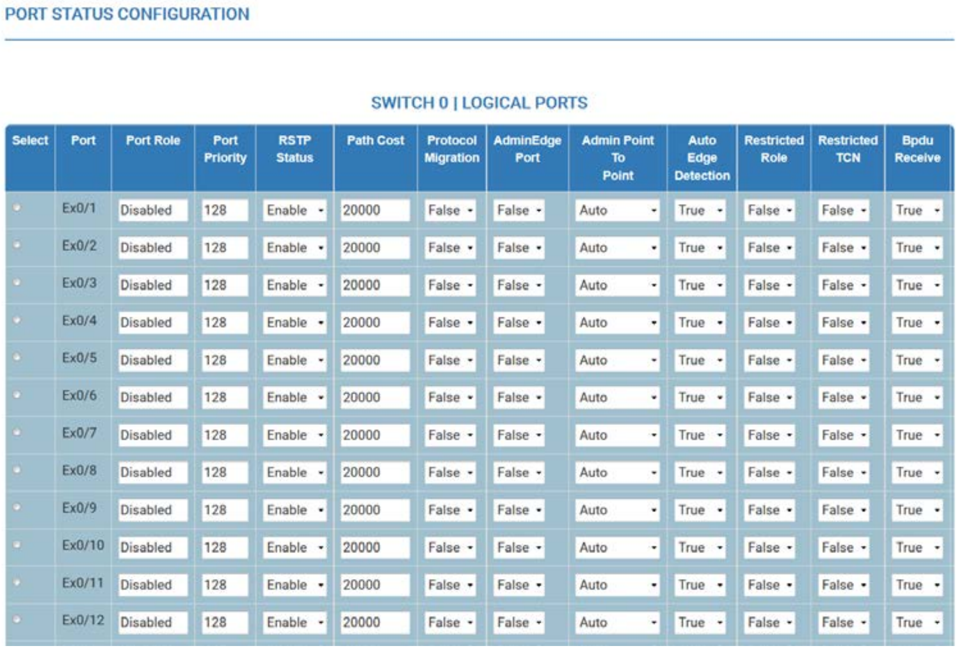
Hello Time - Enter the time interval (in seconds) between two successive configuration BPDUs generated by the root switch.

This value can be either 1 or 2 seconds. Default value is 2 seconds.

Forward Delay - Enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state.

This value ranges between 4 and 30 seconds. Default value is 15 seconds.

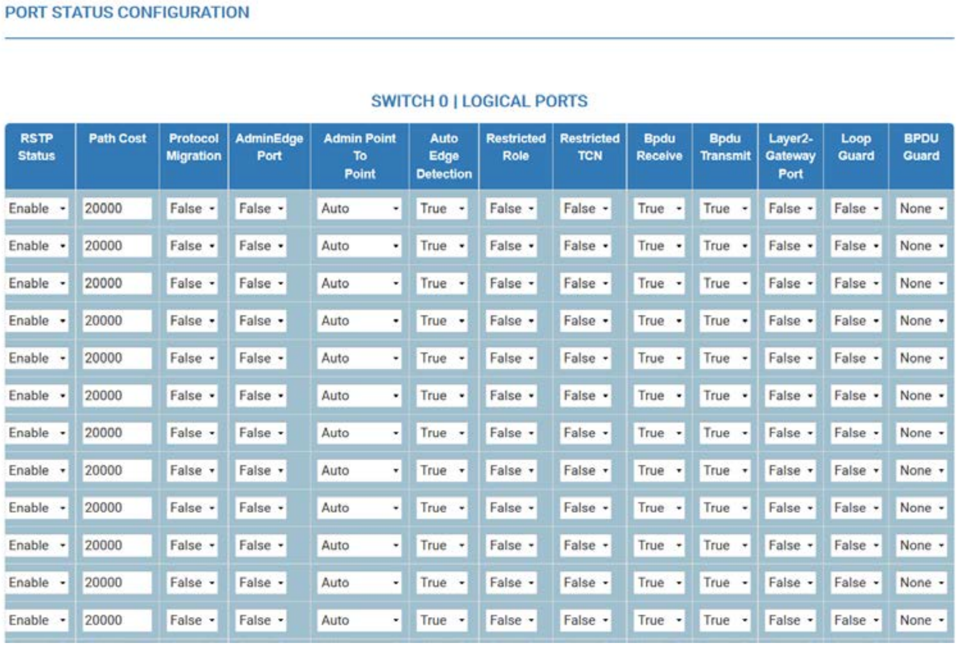
4.7.3 Port Settings



PORT STATUS CONFIGURATION

SWITCH 0 | LOGICAL PORTS

Select	Port	Port Role	Port Priority	RSTP Status	Path Cost	Protocol Migration	AdminEdge Port	Admin Point To Point	Auto Edge Detection	Restricted Role	Restricted TCN	Bpdu Receive
○	Ex0/1	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/2	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/3	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/4	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/5	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/6	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/7	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/8	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/9	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/10	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/11	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True
○	Ex0/12	Disabled	128	Enable	20000	False	False	Auto	True	False	False	True



PORT STATUS CONFIGURATION

SWITCH 0 | LOGICAL PORTS

RSTP Status	Path Cost	Protocol Migration	AdminEdge Port	Admin Point To Point	Auto Edge Detection	Restricted Role	Restricted TCN	Bpdu Receive	Bpdu Transmit	Layer2-Gateway Port	Loop Guard	BPDU Guard
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None
Enable	20000	False	False	Auto	True	False	False	True	True	False	False	None

Fig: Port Status Configuration

The *Port Settings* link opens the **Port Status Configuration** page.

This page allows the user to configure the port information for RSTP that is used during computation of loop-free topology.

The parameters in the page are not populated with the values (that is, the page is blank), if the RSTP System Control status is set as Shutdown.

The table below lists the fields present in this page.

Select - Click to select the port for which the configuration needs to be done.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Port Role - Displays the current role of the port for the spanning tree. The values can be:

* Disabled - Port is disabled manually (RSTP Status) or automatically (Link). It does not take part in the spanning tree process.

* Alternate - Port acting as an alternate for the root port. It is blocked and not used for traffic. It is enabled and declared as the root port, if the root port is blocked.

* Backup - Port acting as a backup for a specific designated port. It is blocked and not used for traffic. It is enabled and declared as the designated port, if the active designated port is blocked.

* Root - Port is used to forward data to root bridge directly or through an upstream LAN.

* Designated - Port is used to send and receive packets to / from a specific downstream LAN segment / device. Only one designated port is assigned for each segment.

Port Priority - Enter the priority value that is assigned to the port. This value is used during the Port Role selection process.

This value ranges between 0 and 240. Default value is 128.

This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on.

RSTP Status - Select the RSTP status of the port.

By default, the status is set as Enable. The list contains:

* Enable - Enables RSTP in the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data.

* Disable - Disables RSTP in the port. The port does not participate in the STP process and is not ready to transmit/receive BPDUs and data.

Path Cost - ter the path cost that contributes to the path cost of paths containing the port.

The paths- path cost is used during calculation of shortest path to reach the root.

The path cost represents the distance between the root port and designated port.

This value ranges between 1 and 200000000. Default value is 200000 for all physical ports and 199999 for port channels.

>

* The default value is used as the path cost, if you have not configured it, and the
Dynamic Path Cost Calculation and Speed Change Path Cost Calculation are set as False. The dynamically calculated path cost is used if you have not manually configured the path cost and one of these fields is set as True.

* The configured value is used as the path cost irrespective of the status (True or False) of the fields Dynamic Path Cost Calculation and Speed Change Path Cost Calculation, if you have configured it (except the value 0).

* The path cost value is calculated automatically based on the port speed maintained by CFA module, if the value is set as 0.

Protocol Migration - Select the protocol migration state of the port. This is used to control the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches.

By default, protocol migration is set as False. The list contains:

* True - Allows the port to transmit BPDUs based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit RSTP BPDUs.

* False - Does not perform protocol migration mechanism. The port always transmits the standard RSTP BPDUs.

>

* The protocol migration is grayed out and cannot be configured, if the RSTP Status is set as Disable.

* The protocol migration triggers the transmission of RSTP BPDUs only once, when set as True. The protocol migration changes automatically as False, once the RSTP BPDU is transmitted.

Admin Edge Port - Select the administrative value of the Edge Port parameter.

By default, admin edge port is set as False. The list contains:

* True - Sets the port as an edge port (that is, the Port State is immediately set as forwarding). It is connected directly to a single end station. It allows RSTP to converge faster and does not wait to receive BPDUs.

* False - Sets the port as a non-Edge port (that is, the spanning tree process is performed using the RSTP). It is connected to a routing device such as switch.

The value of the Edge Port parameter depends on the option selected in the field Auto Edge Detection. The value of the Edge Port parameter is automatically updated, if the Auto Edge Detection is set as True.

Admin Point-to-Point - Select the administrative point-to-point status of the LAN segment attached to the port.

By default, admin point-to-point is set as Auto. The list contains:

* ForceTrue - Always treats the port as if it is connected to a point-to-point link.

* ForceFalse - Always treats the port as if it is having a shared media connection.

* Auto - Treats the ports as having a shared media connection or a point-point link based on the prevailing conditions.

Port is considered to have a point-to-point link if,

1. It is an aggregator and all of its members can be aggregated.

2. The MAC entity is configured for full Duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as Auto).

Otherwise port is considered to have a shared media connection

Auto Edge Detection - Select whether the Edge Port parameter of the port is detected automatically or configured manually.

By default, auto edge detection is set as True. The list contains:

* True - Automatically detects and sets value for Edge Port parameter. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received by that port. This overrides the value set in the field Admin Edge Port, based on the reception of BPDU.

* False - Uses the manually configured value for the Edge Port parameter. The value set in the field Admin Edge Port is used for the Edge Port parameter.

Restricted Role - Select whether the selection of port Role as root can be blocked during the role selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology.

By default, the restricted role is set as False. The list contains:

* True - Blocks the port from being selected as root port for the topology, even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected. You can apply this option for ports that are not fully under your control.

> The blocking of port from being selected as a root port may cause lack of spanning tree connectivity.

* False - Includes all available ports of the topology, in the root selection process to select the root.

Restricted TCN - Select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core region of the network from causing address flushing in the region.

By default, the restricted TCN is set as False. The list contains:

* True - Blocks the port from propagating the received topology change notifications and topology changes to other ports.

> The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.

* False - Allows the port to propagate the received topology change notifications and topology changes to other ports.

Bpdu Receive - Select the processing status of the received RSTP BPDUs.

By default, this field is set as True. The list contains:

* True - Normally processes the RSTP BPDUs received on the port.

* False - Discards the RSTP BPDUs received on the port.

Bpdu Transmit - Select the BPDU transmission status of the port.

By default, this field is set as True. The list contains:

* True - Transmits the RSTP BPDUs from the port.

* False - Blocks the transmission of RSTP BPDUs from the port.

> This field should be set as False, for ports to be configured as Layer2-Gateway
Port.

Layer2-Gateway Port - Select whether the port acts as a normal port or as a L2GP. L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when Admin State is set as Up.

By default, this field is set as false. The list contains:

* True - Allows the port to operate as a L2GP.

* False - Allows the port to operate as a normal port.

>

* Bpdu Transmit should be set as False, before configuring the port as a Layer 2 gateway port.

* L2GP should not be enabled on ports whose Bridge Port Type is set as PIPs or
CBPs, as the effect is unknown.

* Restricted Role and Restricted TCN configuration are disabled for the port configured as L2GP.

* L2GP cannot be enabled on ports with SISP enabled interfaces.

* The Port State of the L2GP is always set as discarding.

Loop Guard - Select whether the loop guard feature is enabled or disabled. This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic.

By default, this field is set as False. The list contains:

* True - Enables the loop guard feature in the port.

* False - Disables the loop guard feature in the port.

BPDU Guard - Select whether the BPDU guard feature is enabled or disabled. This feature disables the port and puts the port in error-disabled state on receiving BPDU, if the portfast feature is enabled on the port. This feature prevents the devices connected to the port from participating in STP operation. Once disabled, the port can be enabled only manually.

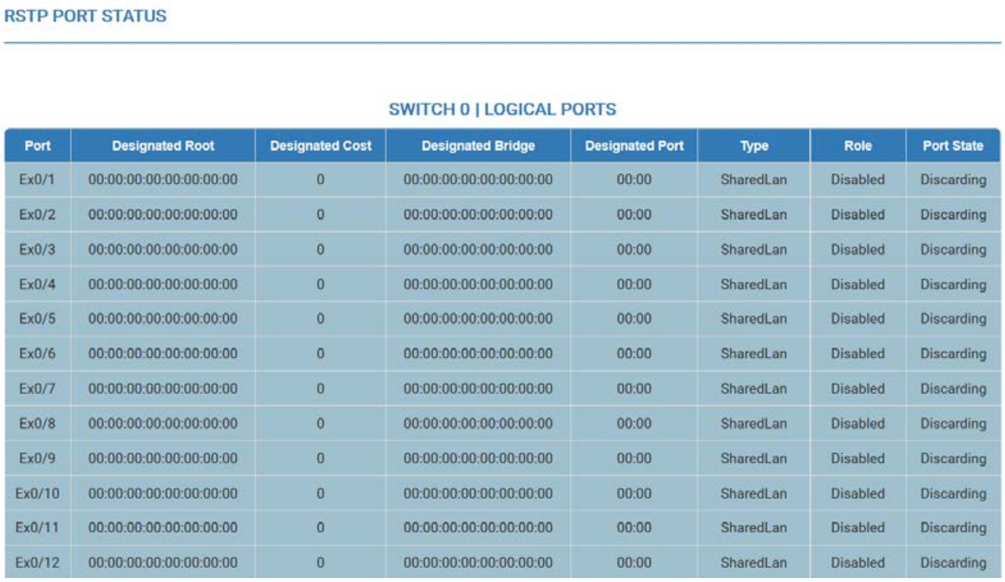
By default, this field is set as None. The list contains:

* None - Removes the BPDU guard feature.

* True - Enables the BPDU guard feature in the port.

* False - Disables the BPDU guard feature in the port.

4.7.4 Port Status



RSTP PORT STATUS

SWITCH 0 | LOGICAL PORTS

Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
Ex0/1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/8	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/9	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/11	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
Ex0/12	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding

Fig: RSTP Port Status

The *Port Status* link opens the **RSTP Port Status** page.

This page allows the user to view information maintained by every port of the switch for RSTP.

The table below lists the fields present in this page.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Designated Root - Displays the unique Identifier of the bridge recorded as the root for the segment to which the port is attached.

This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Designated Cost - Displays the Path Cost of the Designated Port of the segment connected to the port.

This value ranges between 1 and 200000000.

Designated Bridge - Displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment.

This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.

Designated Port - Displays the identifier of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment.

This value is a 2-byte octet string. For example, 80:05.

Type - Displays the operational Admin Point-to-Point of the LAN segment attached to the port. The values can be:

* Point-to-Point - Port is treated as if it is connected to a point-to-point link.

* SharedLan - Port is treated as if it is having a shared media connection.

You can set the values directly or can set as Auto for the switch to decide about the point-to-point status, in the field Admin Point-to-Point provided in the page Port Status Configuration.

Role - Displays the current role of the port for the spanning tree instance. The values can be:

* Disabled - Port is disabled manually (RSTP Status) or automatically (Link). It does not take part in the spanning tree process.

* Alternate - Port acting as an alternate for the root port. It is blocked and not used for traffic. It is enabled and declared as the root port, if the root port is blocked.

* Backup - Port acting as a backup for a specific designated port. It is blocked and not used for traffic. It is enabled and declared as the designated port, if the active designated port is blocked.

* Root - Port is used to forward data to root bridge directly or through an upstream LAN segment.

* Designated - Port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.

Port State - Displays the current state of the port as defined by the STP. The values can be:

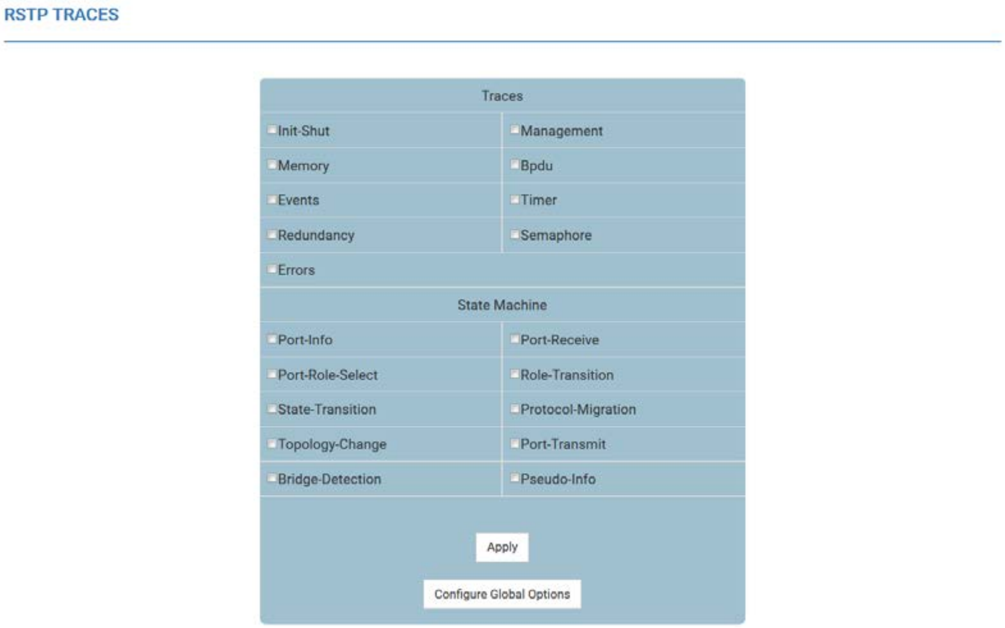
* Disabled - Port is disabled manually (RSTP Status) or automatically (Link). It does not take part in the spanning tree process.

* Discarding - Port is included in the STP process and is ready to learn addresses and forward data.

* Learning - Port is learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data.

* Forwarding - Port is sending and receiving data based on the formed spanning tree topology which is loop free.

4.7.5 RSTP Traces



RSTP TRACES

Traces	
□Init-Shut	□Management
□Memory	□Bpdu
□Events	□Timer
□Redundancy	□Semaphore
□Errors	
State Machine	
□Port-Info	□Port-Receive
□Port-Role-Select	□Role-Transition
□State-Transition	□Protocol-Migration
□Topology-Change	□Port-Transmit
□Bridge-Detection	□Pseudo-Info

Fig: RSTP Traces

The *RSTP Traces* link opens the **RSTP Traces** page.
This page allows the user to enable (that is, select) the required debug statements that will be useful during debug operation.

The debug messages are saved in the flash for technical support.
But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.
Traces - Select the traces for which debug statements is to be generated. The options are:
* Init-Shut - Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.
* Management - Generates debug statements for management traces. This trace is generated whenever you configure any of the STP features.
* Memory - Generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.
* Bpdu - Generates debug statements for BPDU related traces. This trace is generated on failed and successful reception, transmission and processing of BPDUs.

* Events - Generates debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.

* Timer - Generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of STP timers. The different STP timers are:

1. Forward delay timer
2. Hello timer
3. Migration delay timer
4. Recent backup while timer
5. Received information while timer
6. Recent root while timer
7. Topology change timer
8. Hold timer
9. Edge delay timer
10. Rapid age duration timer
11. Pseudo information hello timer

* Redundancy - Generates debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.

* Semaphore - Generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.

* Errors - Generates debug statements for all failure traces of the below mentioned traces.

State Machine - Select the SEMs for which debug statements is to be generated to denote the event and state of the selected SEM. The list contains:

* Port-Info - Generates debug statements for port information SEM.

* Port-Receive - Generates debug statements for port receive SEM.

* Port-Role-Select - Generates debug statements for role selection SEM.

* Role-Transition - Generates debug statements for role transition SEM.

* State-Transition - Generates debug statements for state transition SEM.

* Protocol-Migration - Generates debug statements for protocol migration SEM.

* Topology-Change - Generates debug statements for topology change SEM.

* Port-Transmit - Generates debug statements for port transmit SEM.

* Bridge-Detection - Generates debug statements for bridge detection SEM.

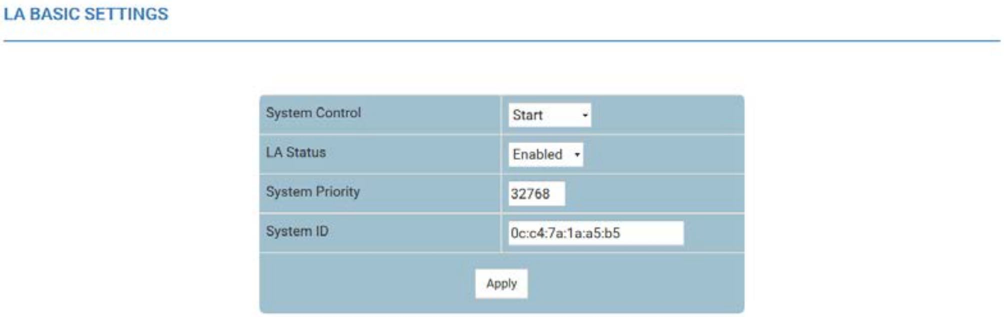
* Pseudo-Info - Generates debug statements for port receive pseudo information SEM.

4.8 LA

The LA link allows you to configure the LA settings for switch. User can configure LA on the following five pages.

- Basic Settings
- Interface settings
- PortChannelSettings
- Port Settings
- Load Balancing

4.8.1 Basic Settings



LA BASIC SETTINGS

System Control	Start
LA Status	Enabled
System Priority	32768
System ID	0c:c4:7a:1a:a5:b5

Fig: LA Basic Settings

The *Basic Settings* link opens the **LA Basic Settings** page.

This page allows the user to configure the LA module parameters that are used globally in the switch for all ports available in the switch.

The table below lists the fields present in this page.

System Control - Select the system control status of the LA in the switch.

By default, system control is set as Start. The list contains:

* Start - Starts the LA module and allocates the resources required by the LA module.

* Shutdown **-** Shutdowns the LA module and releases the allocated resources to the system.

> All the fields in this page are grayed out and cannot be configured, once the system control is set as Shutdown.

LA Status - Select the administrative status of the LA module. LA feature allows the user to aggregate individual point-to-point links into a LA group.

By default, the status is set as Disabled. The list contains:

* Enabled - Enables LA in the switch on all ports. The LA is enabled in the switch, only if the LA System Control is set as start.

* Disabled **-** Disables LA in the switch on all ports.

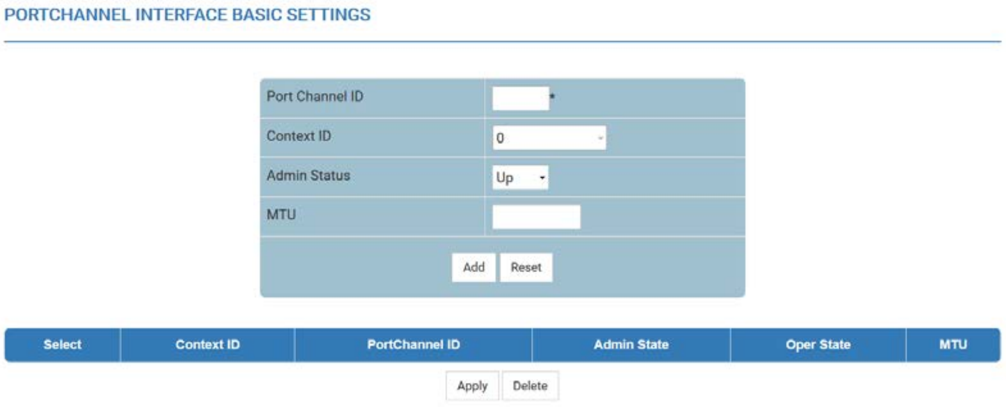
System Priority - Enter the priority value associated with the actor's system ID.

This value ranges between 0 and 65535. Default value is 32768.

System ID - Enter 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the aggregator.

Default value is the base MAC address assigned to the switch.

4.8.2 Interface Settings



PORTCHANNEL INTERFACE BASIC SETTINGS

Port Channel ID	*
Context ID	0
Admin Status	Up
MTU	

Select	Context ID	PortChannel ID	Admin State	Oper State	MTU

Fig: PortChannel Interface Basic Settings

The *Interface Settings* link opens the **PortChannel Interface Basic Settings** page.

This page allows the user to create port channel (that is, aggregator) and configure the port channel related parameters. The port channel is treated as a logical port that is used to aggregate several ports. The port channel related parameters are configured per context basis.

The port channel should be created and its related parameters should be configured, before aggregating the ports.

The port channel can be created, only if the LA System Control is set as start.

The table below lists the fields present in this page.

Port Channel ID - Enter the identifier that uniquely identifies a port channel to be created in the switch.

This value ranges between 1 and 65535.

Context - Select the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Admin Status - Select the desired admin status of the port channel. The list contains:

* Up - Allows the port channel to be available for aggregating the ports and to transmit/receive traffic.

* Down - Blocks the availability of the port channel for aggregating the ports and the transmission/reception of the traffic.

Oper State - Displays the current operational status of the port channel. The list contains:

* Up - Port channel is available for aggregating ports and for transmission/reception traffic.

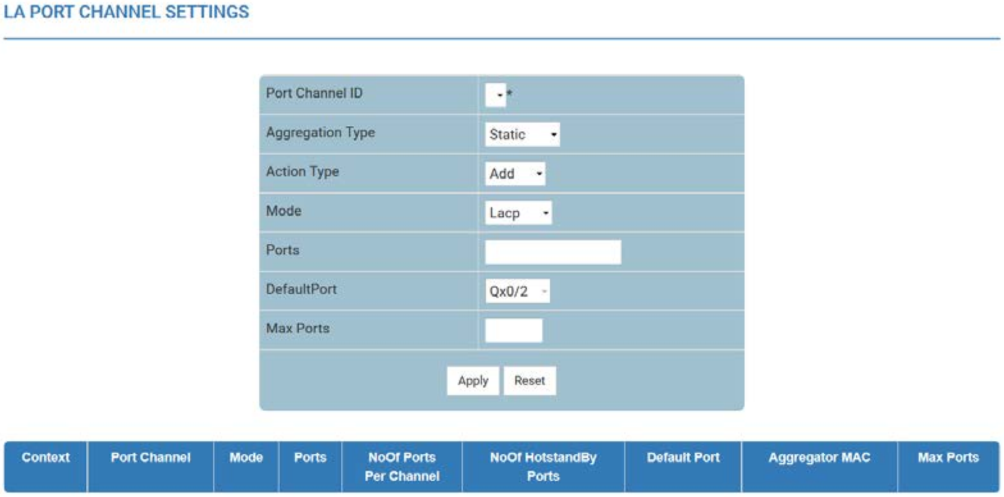
* Down - Port channel availability for aggregating ports and fortransmission/reception of traffic is blocked.

MTU - Enter the MTU for the port channel. This value defines the largest PDU that can be passed by the channel without any need for fragmentation.

This value ranges between 90 and 9202.

> The MTU value can be changed for the port channel, only if the Admin Status of the port channel is set as Down.

4.8.3 PortChannelSettings



LA PORT CHANNEL SETTINGS

Port Channel ID	*
Aggregation Type	Static
Action Type	Add
Mode	Lacp
Ports	
DefaultPort	Qx0/2
Max Ports	

Context	Port Channel	Mode	Ports	NoOf Ports Per Channel	NoOf HotstandBy Ports	Default Port	Aggregator MAC	Max Ports

Fig: LA Port Channel Settings

The *PortChannelSettings* link opens the **LA Port Channel Settings** page.

This page allows the user to add or delete aggregation of ports, Distributed Link aggregation and configure their related parameters for the port channels already created in the PortChannel Interface Basic Settings page.

Only one entry can be created for each port channels.

The table below lists the fields present in this page.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

>

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).

This value ranges between 0 and 65535. The default value is 0.

Port Channel ID - Select the port channel identifier to which the ports should be aggregated or from which aggregated ports should be removed.

The list contains the port channels created in the PortChannel Interface Basic Settings page.

Aggregation Type - Select the type of aggregation to be used in the port channel.

By default, the type is set as Static for all the ports and is set as Dynamic for the port that is configured as a Default Port of the port channel. The list contains:

* Static - Allows the port to participate only in static aggregation, that is, the port is a member of only the port channel to which it is configured. You have to manually assign the port channel with its member ports.

* Dynamic - Allows the port to participate only in dynamic aggregation selection, that is, the port is made as a part of best aggregation selected based on System ID and Admin key (that is, Port Channel ID).

> The fields Action Type, Mode, and Ports are grayed out and cannot be configured, once the aggregation type is set as Dynamic.

Action Type - Select the action to be performed for the Ports configured in this page.

The list contains:

* Add - Aggregates the mentioned Ports and configures them as a member for the selected Port Channel ID.

* Delete - Removes the mentioned Ports from the member list created for the selected Port Channel ID.

Mode - Select the operating mode to be set for the port channel.

The list contains:

* Lacp - Places the port channel into passive negotiation state, in which the port channel waits for its peer to initiate negotiation.

* Manual - Forces the port channel to enable channeling without waiting for its peer to start negotiation.

* Disable - Disables the channeling, that is, the LACP feature is disabled in the port channel.

Ports - Enter port or set of ports, which should be aggregated and set as member of the selected port channel. Use comma as a separator between the ports while configuring a list of ports.

The format of this entry is interface type slot number/port number. There is no space needed between these two entries.

Example: Gi0/1,Gi0/2

(Here Gi is interface type Gigabit Ethernet Interface

0 is slot number and

1 is port number)

This field is disabled and cannot be configured, if the Aggregation Type is set as Dynamic.

No Of Ports Per Channel - Displays the number of ports that are bundled for the port channel. For example, this value would be set as 3, if the value for the field Ports is entered as gi0/4,gi0/7,gi0/8.

No Of HotstandBy Ports - Displays the number of ports that are in standby state for the port channel. This represents the total number of ports that are capable to join in aggregation group, when any member port in the group goes down.

Default Port - Select the port that should be set as default port, which gets attached to the port channel and participates only in dynamic aggregation selection.

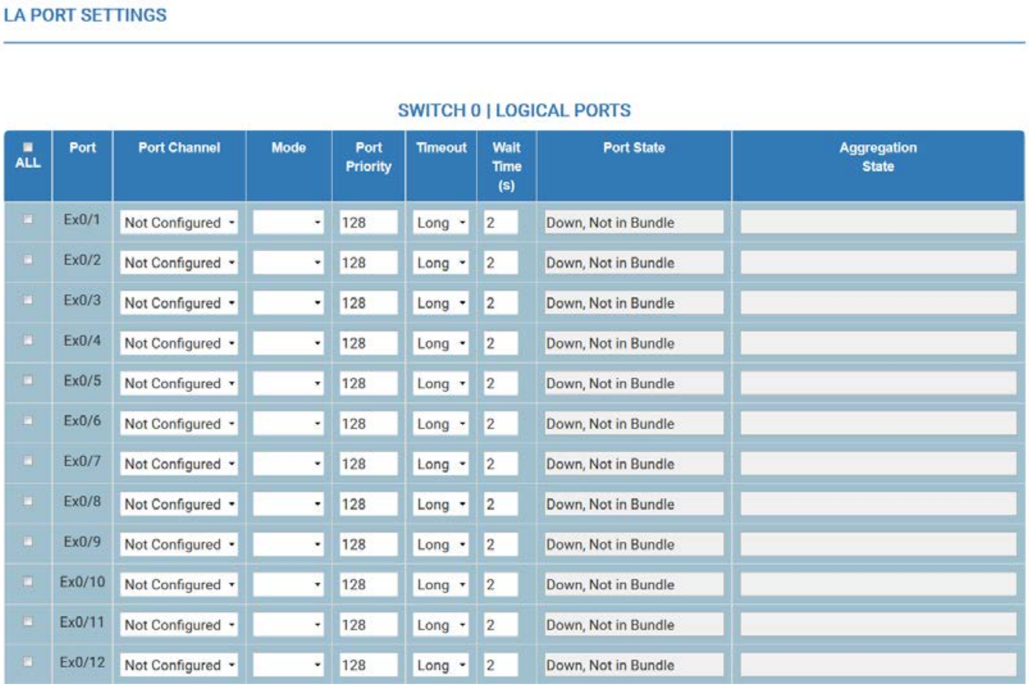
> This field is disabled (that is grayed out) and cannot be configured, if the Aggregation Type is set as Static.

Aggregator MAC - Displays the 6-octet MAC address that is assigned to the port channel. This MAC address is automatically assigned to the port channel.

Max Ports - Enter the maximum number of ports that can be attached to the port-channel. This value ranges between 2 and 8. Default value is 8.

The best ports are maintained in active state and other ports are maintained in standby state, if the total number of ports attached to the port-channel exceeds the configured value. The best port is calculated based on the Port Identifier and Port Priority.

4.8.4 Port Settings



LA PORT SETTINGS

SWITCH 0 | LOGICAL PORTS

■ ALL	Port	Port Channel	Mode	Port Priority	Timeout	Wait Time (s)	Port State	Aggregation State
□	Ex0/1	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/2	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/3	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/4	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/5	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/6	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/7	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/8	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/9	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/10	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/11	Not Configured		128	Long	2	Down, Not in Bundle	
□	Ex0/12	Not Configured		128	Long	2	Down, Not in Bundle	

Fig: LA Port Settings

The *Port Settings* link opens the **LA Port Settings** page.

This page allows the user to configure the LA control configuration parameters for each port in the switch. These parameters allow you to control the bundling of physical ports.

The parameters in the page are not populated with the values (that is, the page is blank), if the LA System Control is set as Shutdown.

The table below lists the fields present in this page.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Port Channel - Select the port channel identifier to which the ports should be aggregated or from which aggregated ports should be removed.

The list contains the port channels created in the PortChannel Interface Basic Settings page.

Mode - Select the operating mode to be set for the port.

By default, the configuration set in the field Mode in the page LA Port Channel Settings is displayed. The list contains:

* On **-** Forces the interface to channel without waiting for its peer to start.

This is equivalent to manual aggregation.

* Active - Starts LACP negotiation un-conditionally.

* Passive - Starts LACP negotiation only when LACP packet is received from peer.

> The field Activity is grayed and cannot be configured, if the mode is set as On or Disable.

Port Priority - Enter the priority value assigned to the aggregation port. This value is used in combination with Port Identifier during the identification of best ports in the port channel.

This value ranges between 0 and 65535. Default value is 128.

Activity Select the LACP activity for the port. The list contains:

* Active - Generates LACPDUs without waiting for any LACPDU from the partner port.

* Passive - Generates LACPDU only when an LACPDU is received from the partner port.

Timeout - Select the time within which LACPDUs should be received on a port to avoid timing out of the aggregated link.

By default, timeout is set as Long. The list contains:

* Short - Sets the value as 3 seconds for the port to time out of the port channel.

* Long - Sets the value as 90 seconds for the port to time out of the port channel.

Wait Time (secs) - Enter the waiting time for a port after receiving partner information and before entering aggregation (that is, the time taken to attach to the port channel).

This value ranges between 0 and 10 seconds. Default value is 2 seconds.

Port State - Displays the current state of the port with respect to LA.

The list contains:

* Up In Bundle - The port is an active member of the port channel. The port is operationally up and actively takes part in aggregation.

* Standby - The port is a member of the port channel but is currently in standby state. The port is capable of joining in the port channel, when any of the ports in the port channel goes down.

* Down - The port is operationally down in lower layers or the port is operational in lower layers but temporarily not able to participate in aggregation because of different partner information in the same group.

* Up Individual - The port is operating individually and is not taking part in aggregation.

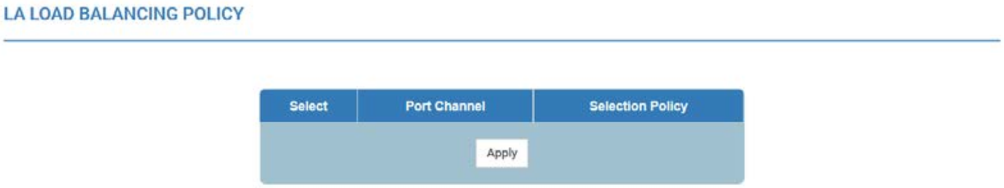
Aggregation State - Displays the type of aggregation in which the port participates.

By default, the type is set as Static for all the ports and is set as Dynamic for the port that is configured as a Default Port of the port channel. The list contains:

* Static - Allows the port to participate only in static aggregation, that is, the port is a member of only the port channel to which it is configured. You have to manually assign the port channel with its member ports in the LA Port Channel Settings page.

* Dynamic - Allows the port to participate only in dynamic aggregation selection, that is, the port is made as a part of best aggregation selected based on System ID and Admin key (that is, Port Channel ID).

4.8.5 Load Balancing


LA LOAD BALANCING POLICY

Select	Port Channel	Selection Policy

Fig: LA Load Balancing Policy

The *Load Balancing* link opens the **LA Load Balancing Policy** page.
This page allows the user to configure the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing.

The table below lists the fields present in this page.
Select - Click to select the port channel for which the configuration needs to be done.
Port Channel - Displays the identifier that uniquely identifies a port channel created in the switch. This value ranges between 1 and 65535.
Selection Policy - Select the rule for distributing the Ethernet traffic. The list contains:
* MAC Source - Uses the bits of the source MAC address in the packet to select the port in which the traffic should flow.
* MAC Destination - Uses the bits of the destination MAC address in the packet to select the port in which the traffic should flow.
* MAC Source and Destination - Uses the bits of the source and destination MAC address in the packet to select the port in which the traffic should flow.
* IP Source - Uses the bits of the source IP address in the packet to select the port in which the traffic should flow.
* IP Destination - Uses the bits of the destination IP address in the packet to select the port in which the traffic should flow.
* IP Source and Destination - Uses the bits of the source and destination IP address in the packet to select the port in which the traffic should flow.
* VLAN ID - Uses the VLAN ID in the packet to select the port in which the traffic should flow.
* ISID - Uses the ISID in the packet to select the port in which the traffic should flow. (Unsupported)
* MAC Source Vlan ID - Uses the VLAN ID and source MAC address in the packet to select the port in which the traffic should flow. (Unsupported)
* MAC Destination Vlan ID - Uses the VLAN ID and destination MAC address in the packet to select the port in which the traffic should flow. (Unsupported)

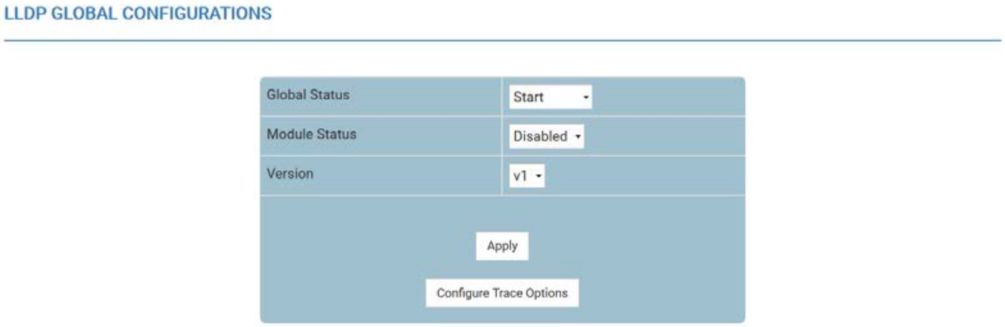
* MAC Source and Destination Vlan ID - Uses the VLAN ID, source MAC address and destination MAC address in the packet to select the port in which the traffic should flow. (Unsupported)
* MPLS VC Label - Uses the MPLS VC label in the packet to select the port in which the traffic should flow. (Unsupported)
* MPLS Tunnel Label - Uses the MPLS tunnel label in the packet to select the port in which the traffic should flow. (Unsupported)
* MPLS VC and Tunnel Label - Uses the MPLS VC and tunnel labels in the packet to select the port in which the traffic should flow. (Unsupported)
* Ipv6 Source - Uses the bits of the source IP6 address in the packet to select the port in which the traffic should flow. (Unsupported)
* Ipv6 Destination - Uses the bits of the destination IP6 address in the packet to select the port in which the traffic should flow. (Unsupported)
* L3 Protocol - Uses the bits of the Layer 3 protocol in the packet to select the port in which the traffic should flow. (Unsupported)
* Source L4 Port - Uses the bits of the source Layer 4 port in the packet to select the port in which the traffic should flow.
* Destination L4 Port - Uses the bits of the destination Layer 4 port in the packet to select the port in which the traffic should flow.

4.9 LLDP

The LLDP link allows you to configure the LLDP settings for switch. User can configure LLDP on the following seven pages.

- Global Settings
- Basic Settings
- Interfaces
- Neighbors
- Agent Info
- Agent Details
- Configured Traces

4.9.1 Global Settings



LLDP GLOBAL CONFIGURATIONS

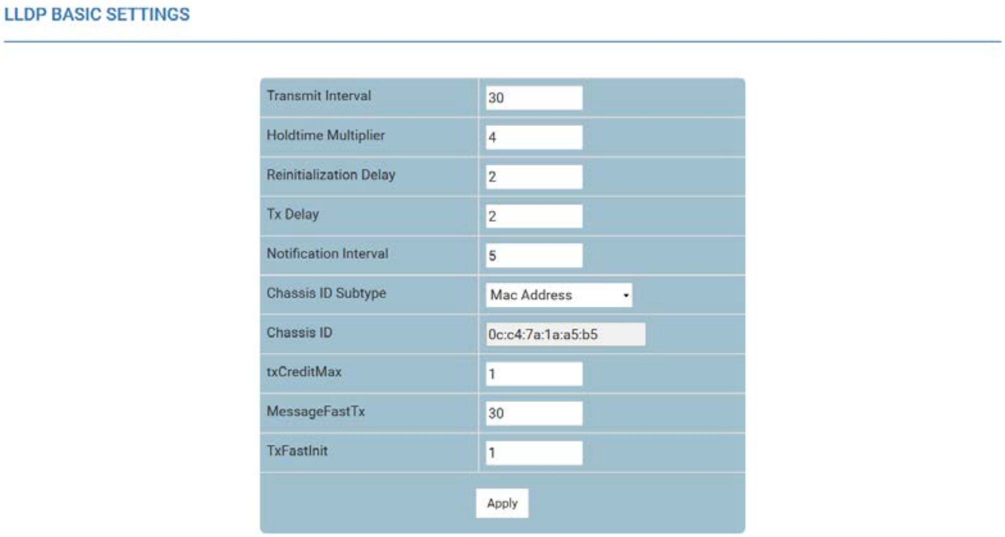
Global Status	Start
Module Status	Disabled
Version	v1

Fig: LLDP Global Configurations

The Global Settings link opens the **LLDP Global Configurations** page.
This page allows the user to enable or disable LLDP module globally and set the LLDP version number.

The table below lists the fields present in this page.
Global Status - Select the administrative system control status of LLDP. The list contains:
* Start - Indicates that all the resources required by LLDP module should be allocated and LLDP should be supported in the devices on all ports.
* Shutdown - Indicates that LLDP should be shut down in the device on all ports and all allocated memory must be released.
> If the Global Status is set as Shutdown, the Module Status cannot be enabled.
Module Status - Select the administrative module status of LLDP module. The list contains
* Enabled - Indicates that LLDP is enabled in the device and can be enabled port-wise
* Disabled - Indicates that LLDP is disabled in the device and also disabled on all ports.
Version - Select the Version of LLDP to be used on the system. By default the LLDP version is set as Version 1 (v1). The list contains;
* v1 - Enables LLDP version 1 (2005) on the port. When V1 is enabled the port can be assigned with only one MAC address.
* v2 - Enables LLDP version 2 (2009) on the port. When enabled mac-address can be assigned per port i.e. the user can have multiple lldp agents per port.

4.9.2 Basic Settings



LLDP BASIC SETTINGS

Transmit Interval	30
Holdtime Multiplier	4
Reinitialization Delay	2
Tx Delay	2
Notification Interval	5
Chassis ID Subtype	Mac Address
Chassis ID	0c:c4:7a:1a:a5:b5
txCreditMax	1
MessageFastTx	30
TxFastInit	1

Fig: LLDP Basic Settings

The *Basic Settings* link opens the **LLDP Basic Settings** page.

This page allows the user to configure the LLDP basic parameters.

The table below lists the fields present in this page.

Transmit Interval - Enter the time interval at which the LLDP frames are transmitted on behalf of this LLDP agent. The value should be restored from non-volatile storage after a re-initialization of the management system.

The value ranges from 5 to 32768 By default Transmit Interval value is set as 30 seconds.

Holdtime Multiplier - Enter the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. This value ranges from 2 to 10. By default the Holdtime Multiplier value is set as 4.

The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula:

TTL = min (65535, Transmit Interval * Holdtime Multiplier).

For example.

If the value of Transmit Interval is 30 and value of Holdtime Multiplier is 4 then value - 120- is encoded in TTL field of LLDP header.

The value of this object must be restored from non-volatile storage after a re-initialization of the management system.

Reinitialization Delay - Enter the delay from when the port admin status becomes 'disabled' until re-initialization will be attempted. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.

This value ranges from 1 to 10. By default Reinitialization Delay value is set as 2 seconds.

Tx Delay - Enter the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems objects. This value ranges between 1 and 8192. The value should be lesser than or equal to (0.25 * Transmit Interval) By default Tx Delay value is set as 2 seconds.

Notification Interval - Enter the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, then these trap- events must be suppressed by the agent. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. This value ranges from 5 to 3600. By default Notification Interval value is set as 5.

Chassis ID Subtype - Select the source of a chassis identifier. By default Chassis ID Subtype is set as Mac Address. The list contains:

* Chassis Component - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component

* Interface Alias - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.

* Port Component - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.

* Mac Address - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.

* Network Address - Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.

* Interface Name - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.

* Local - Represents a chassis identifier based on a locally defined value.

Chassis ID - Enter the chassis identifier string. This value ranges between 1 and 255.

This field is enabled only if the Chassis ID subtype is selected as anyone of the following:

* Chassis Component - The octet string identifies a particular instance of the entPhysicalAlias object for a chassis component.

* Port Component - The octet string identifies a particular instance of the entPhysicalAlias object for a port or backplane component within the containing chassis.

* Local - The Octet string identifies a locally assigned chassis ID.

txCreditMax - Enter the maximum number of consecutive LLDPDUs that can be transmitted any time by the port. This value ranges between 1 and 10.

By Default the txCreditMax is set as:

* 1 when LLDP Version is set as v1

* 5 when LLDP Version is set as v2

MessageFastTx - Enter the interval at which LLDP frames are transmitted on behalf of LLDP agent during fast transmission period. This value ranges between 1 and 3600 seconds.

By Default , MessageFastTx is set as;

* 30 when LLDP Version is set as v1

* 1 when LLDP Version is set as v2

TxFastInit - This command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode.

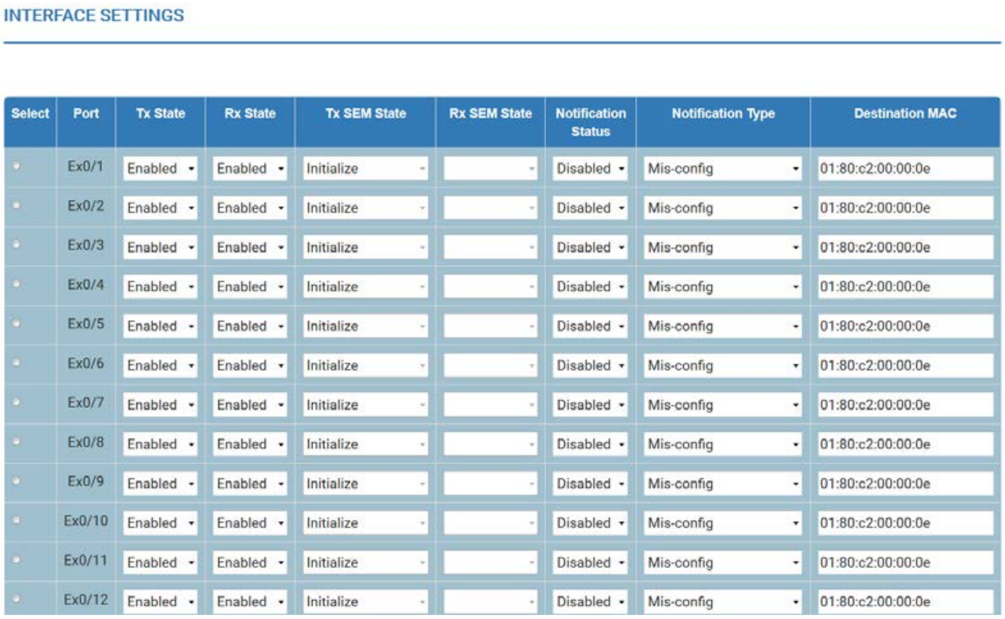
This value ranges between 1 and 8.

By Default, TxFastInit is set as ;

* 1 when LLDP Version is set as v1

* 4 when LLDP Version is set as v2

4.9.3 Interfaces



INTERFACE SETTINGS

Select	Port	Tx State	Rx State	Tx SEM State	Rx SEM State	Notification Status	Notification Type	Destination MAC
○	Ex0/1	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/2	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/3	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/4	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/5	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/6	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/7	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/8	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/9	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/10	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/11	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
○	Ex0/12	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e

Fig: Interface Settings

The *Interfaces* link opens the **Interface Settings** page.
This page allows the user to configure the each ports of the LLDP.

The parameters in the page are not populated with the values (that is, the page is blank), if the LLDP Global Status is set as Shutdown.

The table below lists the fields present in this page.
Select - Click to select the port for which the LLDP parameters need to be configured.
Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
Tx State - Select the status of the LLDP PDU transmitter. By default, the Tx State is set as Enabled. The list contains:
* Enabled: - Enables transmission of LLDPDU from one of the ports of the server to the LLDP module.
* Disabled - Disables transmission of LLDPDU from one of the ports of the server to the LLDP module.
Rx State - Select the status of the LLDP PDU receiver. By default, the Rx State is set as Enabled. The list contains:
* Enabled: - Enables reception of LLDPDU from one of the ports of the server to the LLDP module.

* Disabled - Enables reception of LLDPDU from one of the ports of the server to the LLDP module.

Tx SEM State - Displays current status of the TX state event machine.

Rx SEM State - Displays current status of the RX state event machine.

Notification Status - Select the notification status to be set. By default, the Notification status is set as Disabled. The list contains:

* Enabled - Enables the notification status.

* Disabled - Disables the notification status.

Notification Type - Select the notification type. By default the Notification Type is set as Mis-config.

The list contains:

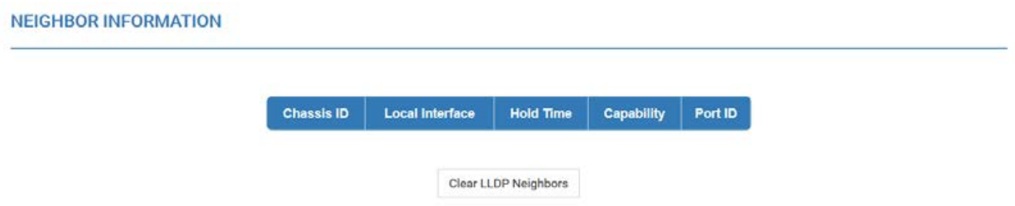
* Remote-Table-Change - LLDP agent sends trap notification to NMS whenever remote table change occurs.

* Mis-Config - LLDP agent sends trap notification to NMS whenever mis-configuration is identified.

* Both - LLDP agent sends trap notification to NMS whenever remote table change occurs or/and whenever mis-configuration is identified.

Destination MAC - Displays the destination mac-address to be used by the LLDP agent for transmission on this port.

4.9.4 Neighbors



NEIGHBOR INFORMATION

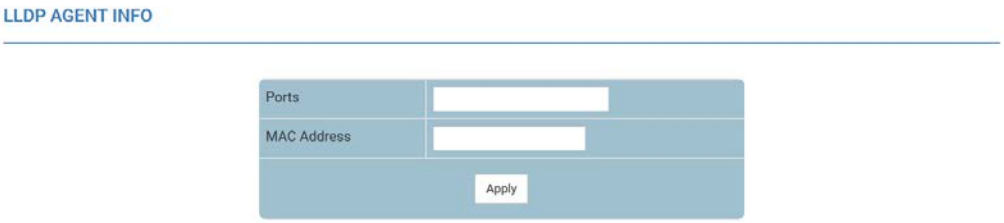
Chassis ID	Local Interface	Hold Time	Capability	Port ID

Fig: Neighbor Information

The *Neighbors* link opens the **Neighbor Information** page.
This page allows the user to obtain the information of the adjacent server connected with the LLDP.

The table below lists the fields present in this page.
Chassis ID - Displays the Chassis ID of the peer. This value is a string value with a maximum size of 255.
Local Interface - Displays the local port on which the peer information is learnt. This value is a string value with a maximum size of 255.
Hold Time - Displays the Hold Time advertized by the peer
Capability - Displays the capabilities advertized by the peer
Port ID - Displays the Port ID advertized by the peer

4.9.5 Agent Info


LLDP AGENT INFO

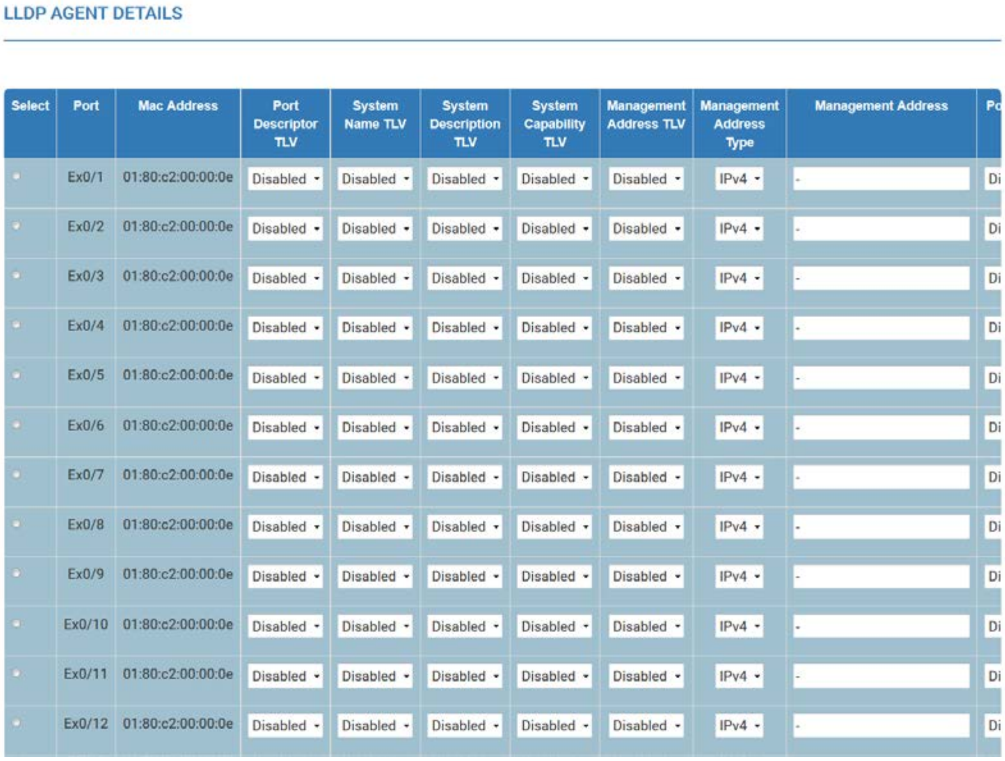
Ports	
MAC Address	

Fig: LLDP Agent Info

The *Agent Info* link opens the **LLDP Agent Info** page.
This page allows the user to configure the destination mac-address to be used by the LLDP agent for transmission on this port.

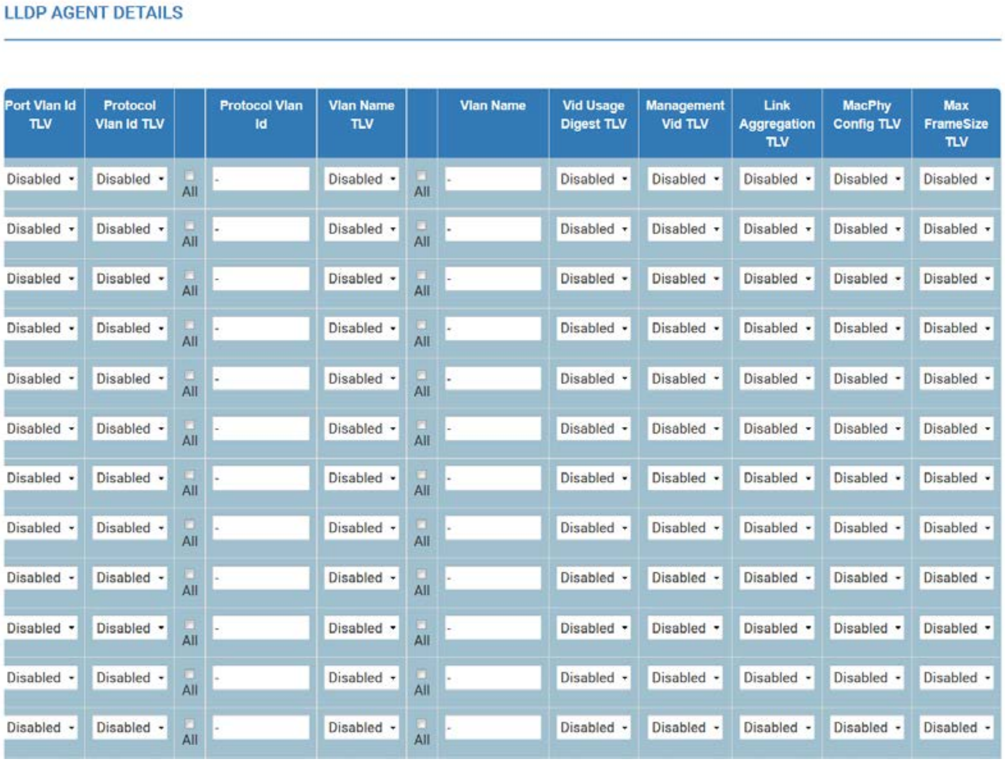
The table below lists the fields present in this page.
Ports - Enter a port or a set of ports for which the LLDP Agent info is to be configured. Use comma as a separator between the ports while configuring a list of ports.
The format of this entry is interface type slot number/port number. There is no space needed between these two entries.
Example: Gi0/1,Gi0/2
(Here Gi is interface type Gigabit Ethernet Interface
0 is slot number and
1 is port number)
Only support the physical interface.
MAC Address - Enter the MAC address to be used as LLDP agent MAC address by the LLDP agent on the specified port
> When LLDP Version is set as V1 only one MAC address can be assigned for a
port.
> When LLDP Version is set as V2 multiple mac-address can be assigned per port
i.e. the user can have multiple LLDP agent per port.

4.9.6 Agent Details



LLDP AGENT DETAILS

Select	Port	Mac Address	Port Descriptor TLV	System Name TLV	System Description TLV	System Capability TLV	Management Address TLV	Management Address Type	Management Address	Po
○	Ex0/1	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/2	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/3	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/4	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/5	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/6	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/7	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/8	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/9	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/10	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/11	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di
○	Ex0/12	01:80:c2:00:00:0e	Disabled	Disabled	Disabled	Disabled	Disabled	IPv4	-	Di



LLDP AGENT DETAILS

Port Vlan Id TLV	Protocol Vlan Id TLV		Protocol Vlan Id	Vlan Name TLV		Vlan Name	Vid Usage Digest TLV	Management Vid TLV	Link Aggregation TLV	MacPhy Config TLV	Max FrameSize TLV
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled
Disabled	Disabled	□ All	-	Disabled	□ All	-	Disabled	Disabled	Disabled	Disabled	Disabled

Fig: LLDP Agent Details

The *Agent Details* link opens the **LLDP Agent Details** page.

This page allows the user to configure the LLDP agent detail parameters.

The table below lists the fields present in this page.

Select - Click to select the port for which the LLDP agent detail parameters need to be configured.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

MAC Address - Enter the MAC address to be used as LLDP agent MAC address by the LLDP agent on the specified port

> When LLDP Version is set as V1 only one MAC address can be assigned for a port.

> When LLDP Version is set as V2 multiple mac-address can be assigned per port i.e. the user can have multiple LLDP agent per port.

Port Descriptor TLV - Select the ability to transmit port descriptor by LLDP agent.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

System Name TLV - Select the ability to transmit system name by LLDP agent.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

System Description TLV - Select the ability to transmit system description by LLDP agent.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

System Capability TLV - Select the ability to transmit system capability by LLDP agent.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Management Address TLV - Select the ability to transmit system management address instance for the specified port, destination, subtype and MAN address by LLDP agent.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Management Address TLV Type - Select the type of management address identifier encoding.

By default, the status is set as IPv4. The list contains:

* IPv4 - Management address identifier as IPv4 type.

* IPv6 - Management address identifier as IPv6 type.

* ALL - Management address identifier as no type.

Management Address - Enter the management address identifier.

Port Vlan Id TLV - Select the ability to transmit port VLAN TLV on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Protocol Vlan Id TLV - Select the ability to transmit protocol VLAN ID TLV on all LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Protocol Vlan Id - Enter the local protocol vlan identifier.

Vlan Name TLV - Select the ability to transmit the local system VLAN name instance on all LLDP transmission capable port.

By default, the status is set as Enabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Vlan Name - Enter the local system vlan identifier.

Vid Usage Digest TLV - Select the ability to transmit local system VID usage digest instance on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Management Vid TLV - Select the ability to transmit Management VID TLV on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

Link Aggregation TLV - Select the ability to transmit Link Aggregation TLV on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

MacPhy Config TLV - Select the ability to transmit MacPhy Config TLV on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

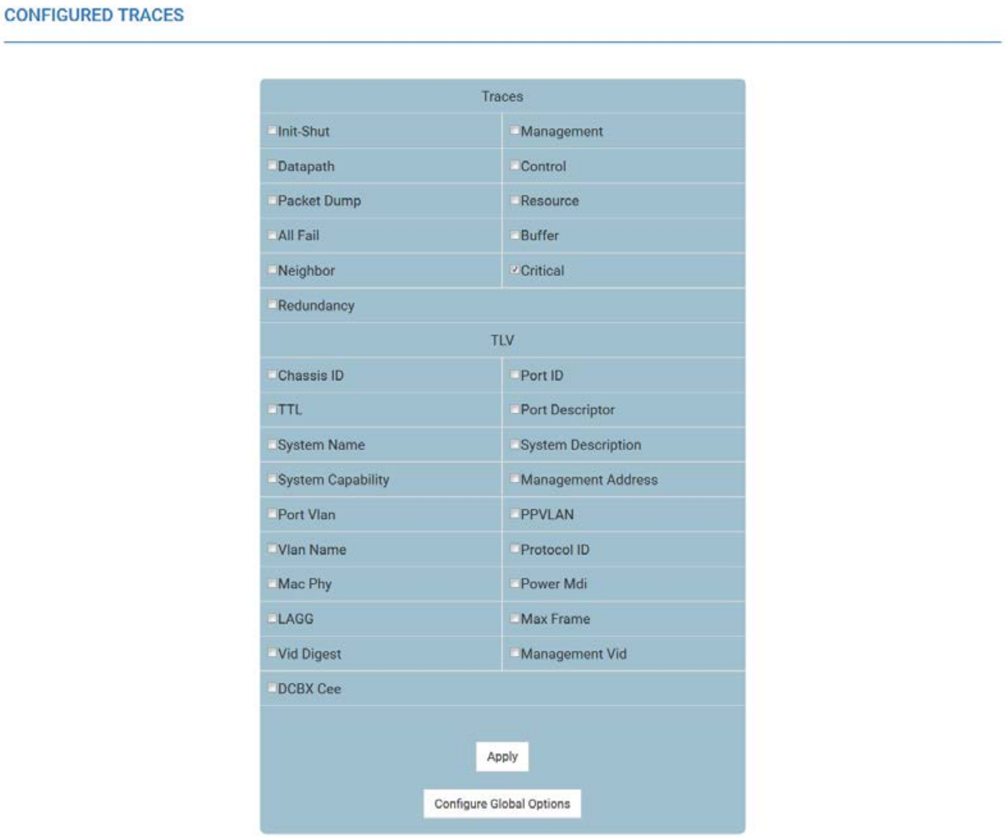
Max FrameSize TLV - Select the ability to transmit Max FrameSize TLV on a given LLDP transmission capable port.

By default, the status is set as Disabled. The list contains:

* Disabled - Disables the ability.

* Enabled - Enables the ability.

4.9.7 Configured Traces



CONFIGURED TRACES

Traces	
□ Init-Shut	□ Management
□ Datapath	□ Control
□ Packet Dump	□ Resource
□ All Fail	□ Buffer
□ Neighbor	☑ Critical
□ Redundancy	
TLV	
□ Chassis ID	□ Port ID
□ TTL	□ Port Descriptor
□ System Name	□ System Description
□ System Capability	□ Management Address
□ Port Vlan	□ PPVLAN
□ Vlan Name	□ Protocol ID
□ Mac Phy	□ Power Mdi
□ LAGG	□ Max Frame
□ Vid Digest	□ Management Vid
□ DCBX Cee	

Fig: Configured Traces

The *Configured Traces* link opens the **Configured Traces** page.

This page allows the user to enable the required debug statements useful during debug operation.

The debug messages are saved in the flash for technical support.

But the configuration in this page will be reset after reboot.

The table below lists the fields present in this page.

Traces - Select the traces for which debug statements is to be generated. The options are:

* Init-Shut - Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of LLDP related module and memory.

* Management - Generates debug statements for management traces. This trace is generated when any of the LLDP features is configured.

* Datapath - Generates the debug statements for datapath traces. This trace is generated during failure in packet processing.

* Control - Generates debug statements for Control functionality traces. This trace is generated during failure in modification or retrieving of LLDP entries

* Packet Dump - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.

* Resource - Generates debug statements for Traces with respect to allocation and freeing of all resource expect the buffers.

* All Fail - Generates debug statements for all failure traces of the below mentioned traces.

* Buffer - Generates debug statements for traces with respect to allocation and freeing of Buffer.

* Neighbor - Generates debug statements for neighbor traces.

* Critical - Generates debug statements for critical traces.

* Redundancy - Generates debug statements for redundancy traces.

TLV - Select the TLVs for which debug statements is to be generated to denote the event and state of the selected TLV. The options are:

* Chassis ID - Generates debug statements for chassis-id TLV traces.

* Port ID - Generates debug statements for port-id TLV traces.

* TTL - Generates debug statements for TTL TLV traces.

* Port Descriptor - Generates debug statements for port descriptor TLV traces.

* System Name - Generates debug statements for system name TLV traces.

* System Description - Generates debug statements for system description TLV traces.

* System Capability - Generates debug statements for system capability TLV traces.

* Management Address - Generates debug statements for management address TLV traces.

* Port Vlan - Generates debug statements for port vlan TLV traces.

* PPVLAN - Generates debug statements for port-protocol-vlan TLV traces.

* Vlan Name - Generates debug statements for vlan name TLV traces.

* Protocol ID - Generates debug statements for protocol id TLV traces.

* Mac Phy - Generates debug statements for mac or phy TLV traces.

* Power Mdi - Generates debug statements for power through MDI TLV traces.

* LAGG - Generates debug statements for link aggregation TLV traces.

* Max Frame - Generates debug statements for maximum frame size TLV traces.

* VID Digest - Generates debug statements for vid digest TLV traces.

* Management VID - Generates debug statements for management VID TLV traces.

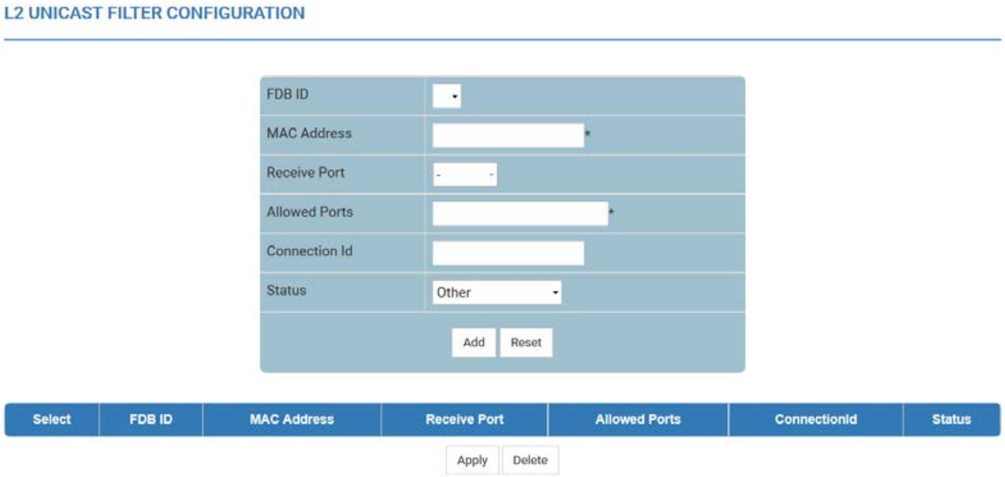
* DCBX Cee - Generates debug statements for DCBX (cee) TLV traces.

4.10 Filters

The Filters link allows you to configure the Filters settings for switch. User can configure Filters on the following two pages.

- Unicast Filters
- Multicast Filters

4.10.1 Unicast Filters



L2 UNICAST FILTER CONFIGURATION

FDB ID	
MAC Address	*
Receive Port	-
Allowed Ports	*
Connection Id	
Status	Other

Select	FDB ID	MAC Address	Receive Port	Allowed Ports	ConnectionId	Status

Fig: L2 Unicast Filter Configuration

The *Unicast Filters* link opens the **L2 Unicast Filter Configuration** page.

This page allows the user to configure the filter for controlling the unicast packets that the switch needs to process.

The table below lists the fields present in this page.

FDB ID - Select the specific identifier of Forwarding Database. FDB (Forwarding Database) ID.

MAC Address - Enter the destination MAC address of the received packet.

Receive Port - Select the port on which the packet is received. It is not supported on this platform.

Allowed Ports - Enter the list of ports on which the received packet (with the below set MAC address and received from the specified receive port if configured) should be forwarded.

Connection Id - Enter the MAC address which is used to associate backbone MAC address of peer backbone edge bridge with customer MAC addresses that can be reached through the peer backbone edge bridge.

Status - Select the status types. The list contains:

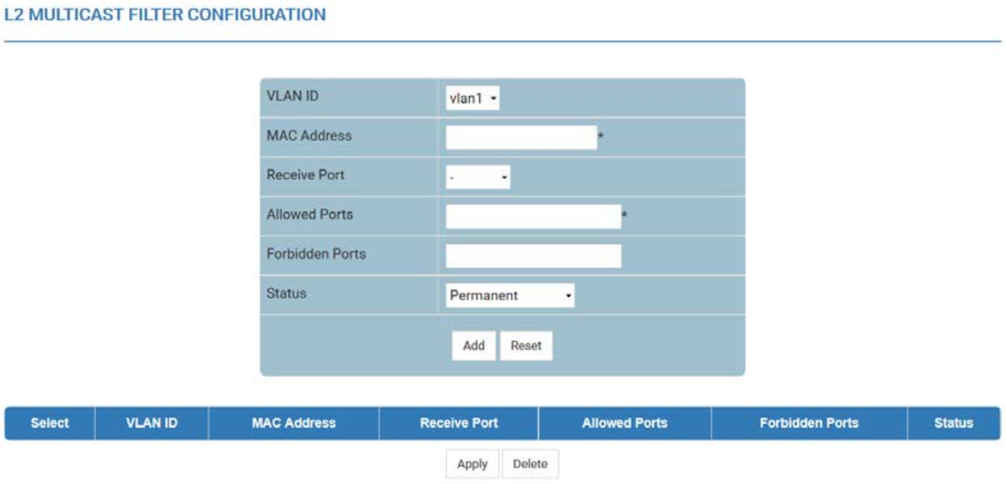
* Other - Currently in use, but the conditions under which it will remain so differ from the following values.

* Permanent - Entry resides even after restart of the switch.

* DeleteOnReset - Deletes the entry on restart of the switch.

* DeleteOnTimeout - Deletes the entry on expiry of the ageing timer.

4.10.2 Multicast Filters



L2 MULTICAST FILTER CONFIGURATION

VLAN ID	vlan1
MAC Address	*
Receive Port	-
Allowed Ports	*
Forbidden Ports	
Status	Permanent

Select	VLAN ID	MAC Address	Receive Port	Allowed Ports	Forbidden Ports	Status

Fig: L2 Multicast Filter Configuration

The *Multicast Filters* link opens the **L2 Multicast Filter Configuration** page.
This page allows the user to configure the filter for controlling the multicast packets that the switch needs to process. A multicast access profile is configured to filter incoming reports that can be commonly utilized by all the multicast protocols.

The table below lists the fields present in this page.
VLAN ID - Select the VLAN ID.
MAC Address - Enter the destination MAC address of the received packet.
Receive Port - Select the port on which the packet is received.
Allowed Ports - Enter the list of ports on which the received packet (with the below set MAC address and if received from the configured port) can be forwarded.
Forbidden Ports - Enter the list of ports on which the received packet (with the below set MAC address and if received from the configured port) must not be forwarded.
Status - Select the status types of filter. The list contains:
* Other - Currently in use, but the conditions under which it will remain so differ from the following values.
* Permanent - Entry resides even after restart of the switch.
* DeleteOnReset - Deletes the entry on restart.
* DeleteOnTimeout - Deletes the entry on expiry of the ageing timer.

4.11Link Tracking

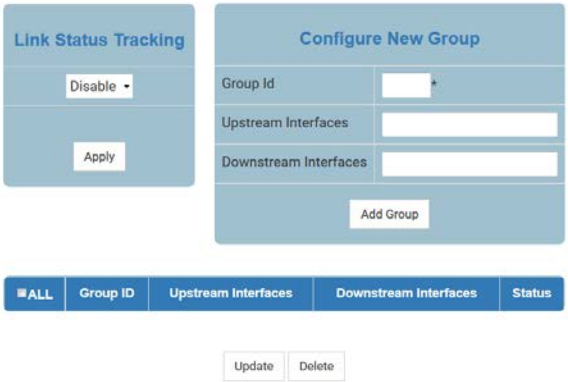


Fig: Link Status Tracking

The *Link Tracking* link opens the **Link Status Tracking** page.

This page allows the user to configure the link status tracking feature helps disabling or enabling downstream ports based on upstream ports.

The table below lists the fields present in this page.

Group - User can create multiple groups.

The group identifiers should be valid number between 1 to 1024.

Upstream Interfaces - Each group can have one or more upstream interfaces.

Physical ports (Gi/Ex) and port channel interfaces can be configured as upstream ports.

Downstream Interfaces - Each group can have one or more downstream interfaces.

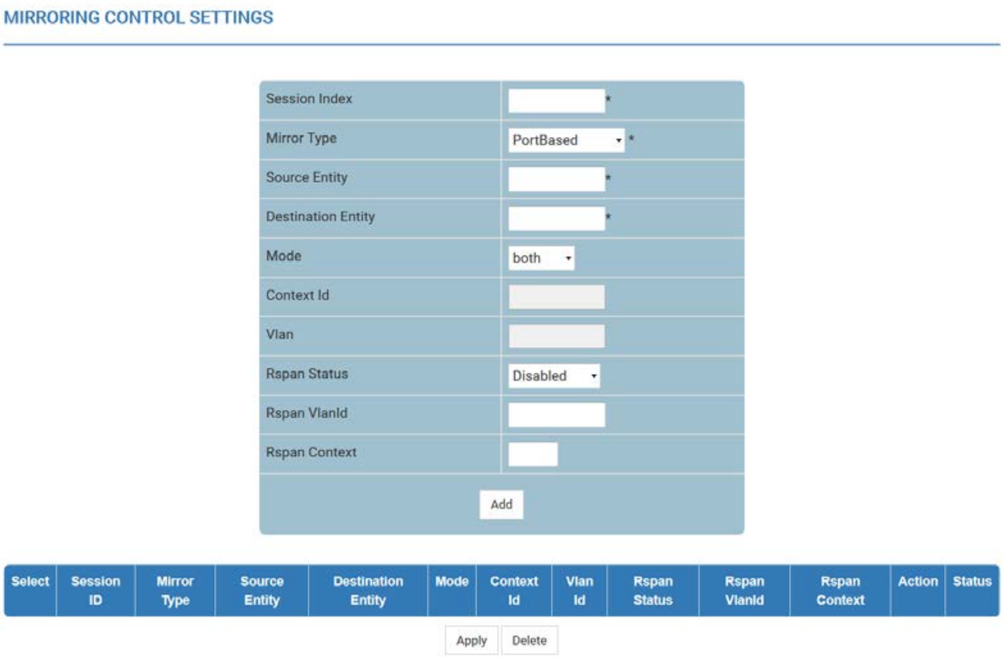
Physical ports (Gi/Ex) and port channel interfaces can be configured as downstream ports.

Group Status - Group status is combined status of all upstream ports in the group.

If any one of the upstream port is in UP state, group status will be UP.

If all upstream ports are down, group status will be down. When group status is down, all downstream ports will be disabled.

4.12 Mirroring



MIRRORING CONTROL SETTINGS

Session Index	*
Mirror Type	PortBased *
Source Entity	*
Destination Entity	*
Mode	both
Context Id	
Vlan	
Rspan Status	Disabled
Rspan VlanId	
Rspan Context	

Select	Session ID	Mirror Type	Source Entity	Destination Entity	Mode	Context Id	Vlan Id	Rspan Status	Rspan VlanId	Rspan Context	Action	Status

Fig: Mirroring Control Settings

The *Mirroring Control Settings* link opens the **Mirroring Control Settings** page.

This page allows the user to configure the mirroring control settings.

Mirroring feature is introduced in switches because of a fundamental difference that switches have with hubs. When a hub receives a packet on one port, the hub sends out a copy of that packet on all ports except on the one where the hub received the packet. After a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch receives. After this forwarding table is built, the switch forwards traffic that is destined for a MAC address directly to the corresponding port.

The table below lists the fields present in this page.

Select - Click to select the session ID for which the configurations have to be modified or the session needs to be deleted.

Session Index - Enter the index of the mirroring session. This value ranges between 1 and 20.

Mirror Type - Select the type of mirroring that the session supports. By default the Mirror Type value is set as PortBased. The list contains:

* PortBased - Receives / Transmits mirroring packets depending on mirroring mode (ingress/egress/both) on - source- port(s) to - destination- port(s).

* MacFlowBased - Receives / Transmits Mirroring packets with a given MAC- address and for a VLAN id to the destination port which can be on same switch or on remote switch connected by network or on different boards in stacked/chassis environment.

* VlanBased - Receives / Transmits Mirroring data on a particular VLAN to the destination port (Unsupported).

* IpFlowBased - Receives / Transmits Mirroring the packets on the source port for that flow to the destination port.

Source Entity - Enter the source ID which participates in a mirroring session. This value ranges between 1 and 65535.

This field is not valid for VlanBased Mirror Type.

Destination Entity - Enter the destination port id from which the packets will be transmitted. This value ranges between 1 and 65535.

Mode Select the mode of mirroring. By default the Mode is set as both. The list contains:

* ingress - Mirrors only traffic that is ingressing on the source ports.

* egress - Mirrors only traffic that is egressing on the source ports.

* both - Mirrors both traffic that is ingressing on the source ports and egressing out of source ports.

Context Id - Enter the context identifier to which the source entity belongs. This is used when specifying VLAN as the source. This field is valid only for VlanBased Mirror Type.

This value ranges between 1 and 64.

Value -1 indicates that this is not considered for the mirroring session.

This is enabled only when the Mirror Type is set as VlanBased.

Vlan - Enter the VLAN identifier from which the packets will be transmitted. This value ranges between 1 and 4094.

This is enabled only when the Mirror Type is set as VlanBased.

Rspan Status Select whether the session is enabled or disabled for Remote monitoring. By Default Rspan Status is set as Disabled. The list contains:

* Source - Enables Session for Remote monitoring and the source entities for the session are remotely monitored.

* Destination - Specifies that the session should monitor remote traffic mirrored with RSPAN (Remote Switched Port Analyzer) VLAN ID.

* Disabled - Disables Remote monitoring for the mirroring session.

Rspan VlanId Enter the Remote VLAN identifier used for achieving remote monitoring. This value ranges between 1 and 4094.

Rspan Context Enter the context identifier to which the Remote VLAN belongs.

Value -1 indicates that this is not considered for the mirroring session.

Action - Select the Action status for any VLAN entry for a session. The list contains:

* Add - Creates a VLAN entry for a session.

* Delete - Deletes a VLAN entry for a session.

Status - Displays the status of the Mirror Control Extension table entries. The list contains:

* Up - Indicates the status of the Mirror Control Extension table entries as enabled.

* Down - Indicates the status of the Mirror Control Extension table entries as disabled.

* Under creation - Indicates that the Mirror Control Extension table entries are under creation.

5 Layer 3 Management

Layer 3 Management covers the following features of Switch.

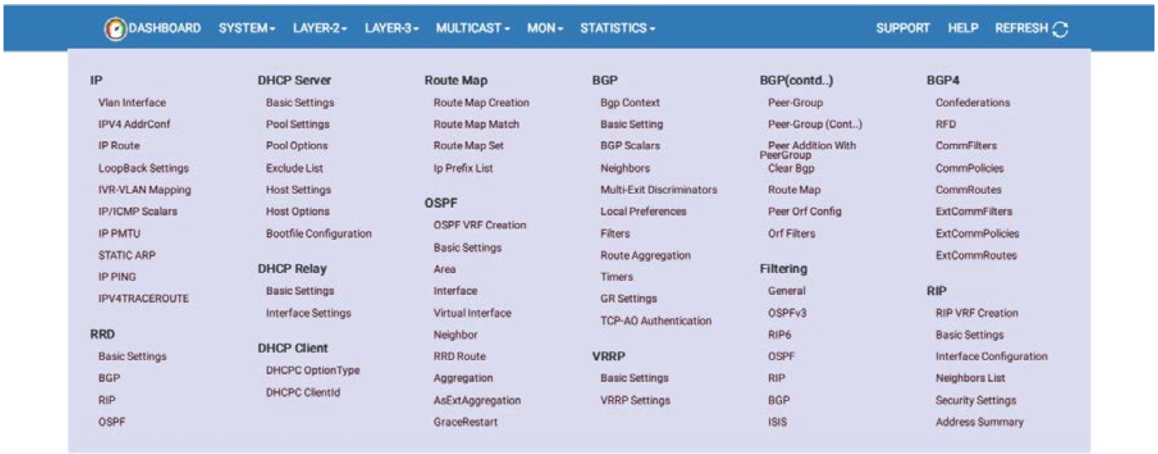


Fig: System Management

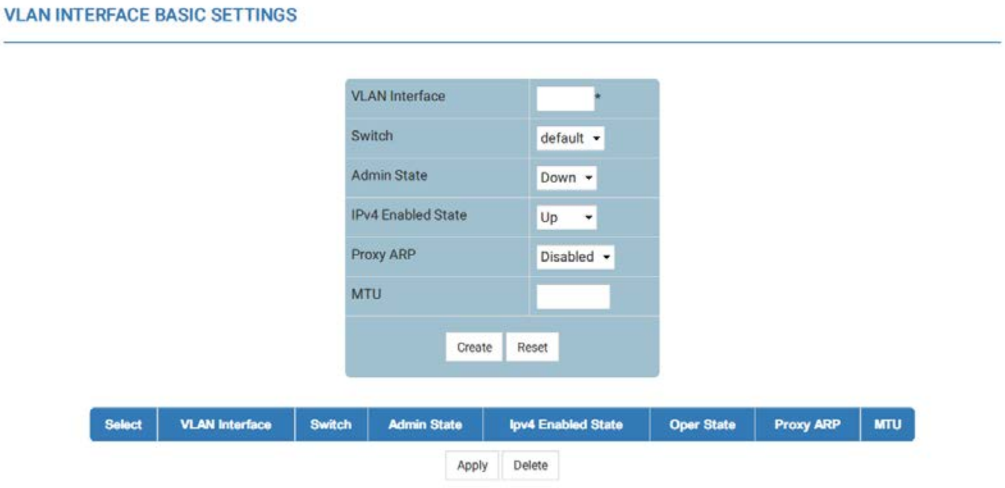
- IP
- RRD
- DHCP Server
- DHCP Relay
- DHCP Client
- Route Map
- OSPF
- BGP
- VRRP
- Filtering
- BGP4
- RIP

5.1 IP

The *IP* link allows you to configure the IP related parameters for switch. User can configure IP on the following 10 pages.

- Vlan Interface
- IPV4 AddrConf
- IP Route
- LoopBack Settings
- IVR-VLAN Mapping
- IP/ICMP Scalars
- IP PMTU
- STATIC ARP
- IP PING
- IPV4TRACEROUTE

5.1.1 Vlan Interface



VLAN INTERFACE BASIC SETTINGS

VLAN Interface	*
Switch	default
Admin State	Down
IPv4 Enabled State	Up
Proxy ARP	Disabled
MTU	

Select	VLAN Interface	Switch	Admin State	Ipv4 Enabled State	Oper State	Proxy ARP	MTU

Fig: VLAN Interface Basic Settings

The *Vlan Interface* link opens the **VLAN Interface Basic Settings** Page.

VLAN Interface Basic Settings page allows the user to configure the basic settings of the VLAN interface.

* The IPv4 enabled state is dependent on the Admin status. If Admin state is down, IPv4 Enabled state is down.

The table below lists the fields present in this page.

VLAN Interface - Enter the VLAN Interface that is to be created. The value ranges between 1 and 4094.

Switch - Specifies the name of the switch context.

Admin State - Select the Admin Status of the VLAN interface. The list contains:

* Up - Makes the IP interface administratively up. After Configuring the IP address the interface can be made admin UP

* Down - Makes the IP interface administratively down

By default, the value is down

IPv4 Enabled State - Select the status of IPv4 on the interface. The list contains:

* UP - Enables IPv4 on this interface

* Down - Disables IPv4 on this interface

Oper State - Displays the current operational status of the VLAN interface. The list contains:

* Up - Indicates interface is operationally up and ready to transmit and receive network traffic

* Down Indicates interface is operationally down.

Proxy ARP - Specifies the Proxy ARP admin status for the interface. Options are:

* Enabled - Proxy ARP feature is enabled.

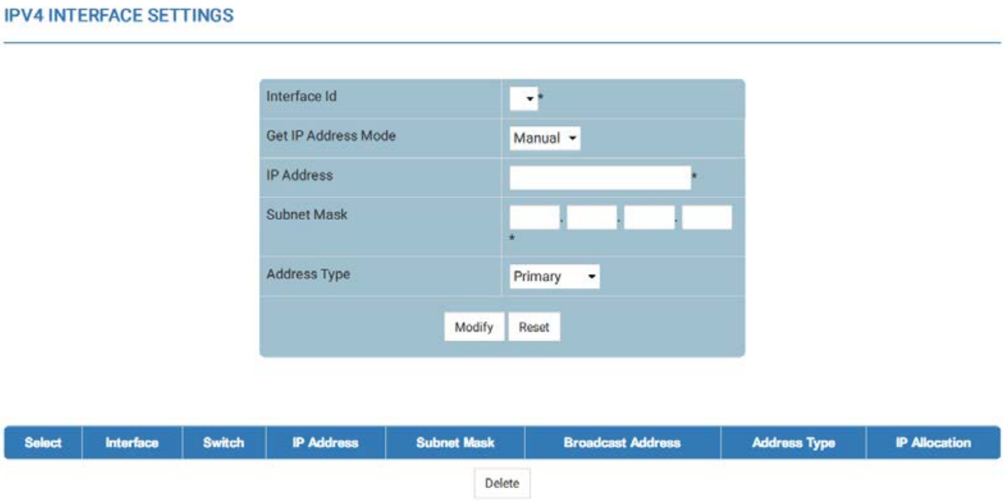
* Disabled - Proxy ARP feature is disabled.

By default, Proxy ARP is disabled.

MTU - Enter the Maximum Transmission Unit. The MTU for the interface as shown to the higher interface sub-layer (this value should not include the encapsulation or header added by the interface). If IP is operating over the interface, then this value indicates the IP MTU over this interface. For changing the MTU of any interface, the interface must be brought down first - changing MTU while the interface is administratively up is not permitted.

This value ranges between 90 and 9202.

5.1.2 IPV4 AddrConf



IPV4 INTERFACE SETTINGS

Interface Id	*
Get IP Address Mode	Manual
IP Address	*
Subnet Mask	. . . *
Address Type	Primary

Select	Interface	Switch	IP Address	Subnet Mask	Broadcast Address	Address Type	IP Allocation

Fig: IPv4 Interface Settings

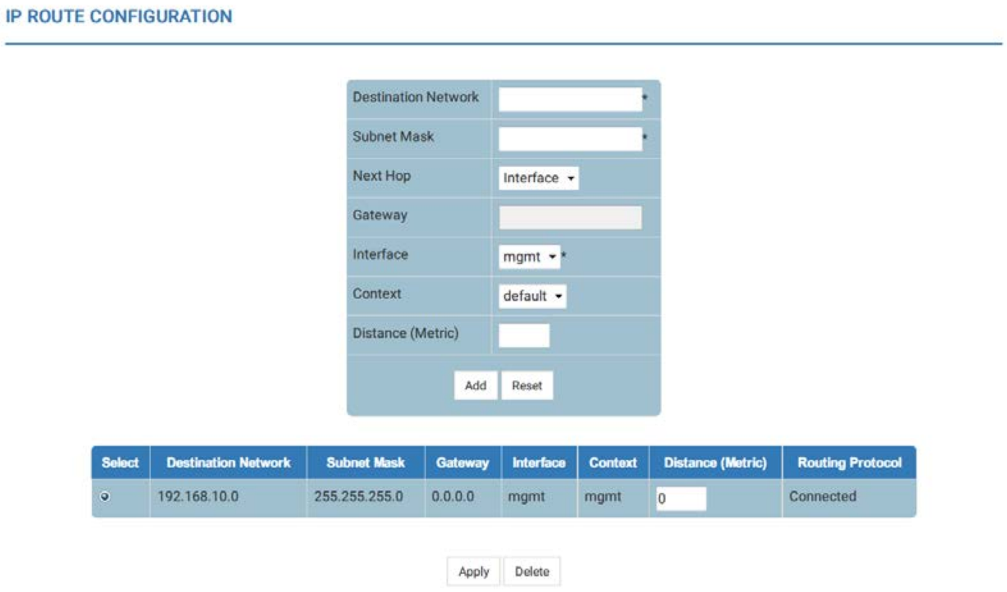
The *IPV4 AddrConf* link opens the **IPv4 Interface Settings** Page.
The IPv4 Interface Settings page allows user to configure the settings of the IPv4 interface.

The table below lists the fields present in this page.
Interface Id - Select the index value which uniquely identifies the VLAN interface to which this entry is applicable.
Get IP Address Mode - Select the protocol to be used to obtain the IP address from the interface. By default the value is RARP The list contains:
* Manual - The IP address is configured manually to a specified address by the user or administrator.
* RARP **-** The IP address is assigned to the system by a RARP (Reverse Address Resolution Protocol) server.
* DHCP **-** The IP address is assigned to the system by a DHCP (Dynamic Host Configuration Protocol) server. DHCP-client tries for dynamic IP address from server for maximum number of retries. If not successful in receiving any IP address, then rolls back to default IP address
Switch - Specifies the name of the switch context.
IP Address - Enter the IP Address of the interface. If the interface is not a network interface then the default value of 0.0.0.0 is assigned and the interface is treated as a non-numbered interface by IP.
Subnet Mask - Enter the subnet mask for the provided IP address.
Broadcast Address - Displays the broadcast address for the specified IP address.
Address Type - Select the type of address. The default address type is Primary. The list contains:

* Primary - Primary IP address of the Interface

* Secondary - Additional IP address that can be configured for the Interface. The secondary IP address can be created only if the primary IP address is already created for the interface

5.1.3 IP Route



IP ROUTE CONFIGURATION

Destination Network	*
Subnet Mask	*
Next Hop	Interface
Gateway	
Interface	mgmt *
Context	default
Distance (Metric)	

Select	Destination Network	Subnet Mask	Gateway	Interface	Context	Distance (Metric)	Routing Protocol
●	192.168.10.0	255.255.255.0	0.0.0.0	mgmt	mgmt	0	Connected

Fig: IP Route Configuration

The *IP Route* link opens the **IP Route Configuration** Page.

The IP Route Configuration page allows the user to configure IP route information.

The table below lists the fields present in this page.

Destination Network - Enter the destination IP address of the route. It denotes the Network Address for which the route is being added.

Subnet Mask - Enter the subnet mask for the Destination Network address.

Next Hop - Select the next hop mode. Options are:

* Gateway - Use a gateway for the next hop.

* Interface - Use a interface for the next hop.

Gateway - Enter the Next Hop gateway to reach the Destination Network.

Interface - Select the outgoing interface through which the Destination Network is reachable.

Context - Select routing context.

By default it as set as default. The list contains:

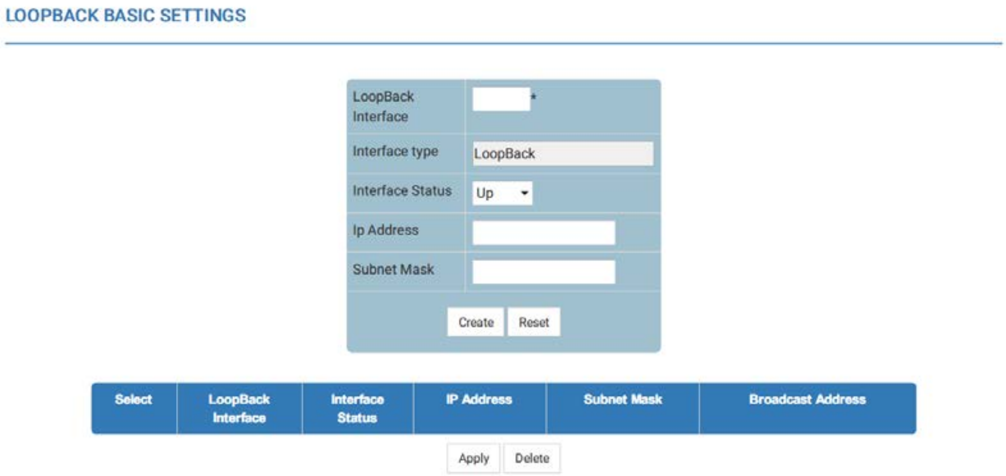
* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Distance (Metric) - Enter the Metric value of the destination. The semantics of this metric are determined by the routing-protocol. The value ranges between 1 and 255. The default value is 1.

Routing Protocol - Displays the status of the routing protocol through which the route was learnt, if the route is not a directly connected network or a static route.

5.1.4 LoopBack Settings



LOOPBACK BASIC SETTINGS

LoopBack Interface	*
Interface type	LoopBack
Interface Status	Up
Ip Address	
Subnet Mask	

Select	LoopBack Interface	Interface Status	IP Address	Subnet Mask	Broadcast Address

Fig: LoopBack Basic Settings

The *LoopBack Settings* link opens the **LoopBack Basic Settings** Page.

The LoopBack Basic Settings page allows the user to configure the basic loopback settings..

The table below lists the fields present in this page.

LoopBack Interface - Enter the Loopback Interface that is to be created.

Interface type - Displays the interface type as Loopback.

Interface Status - Select the Interface Status. The list contains:

* Up - Allows traffic through the interface.

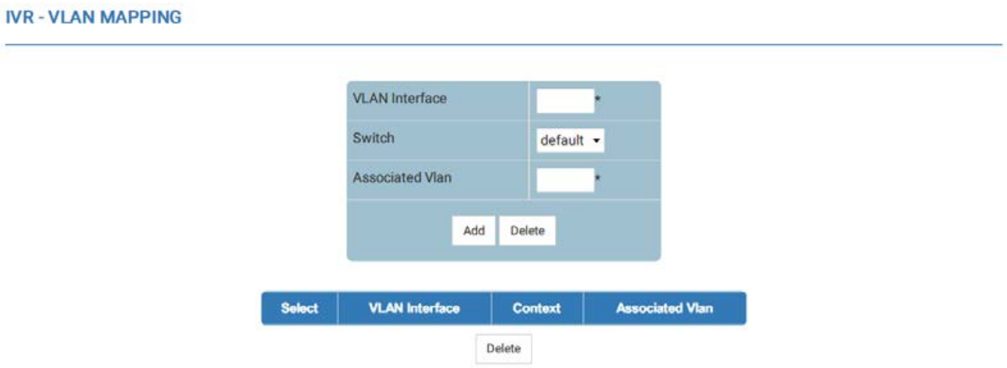
* Down - Does not allow traffic.

IP Address - Enter the IP Address for the Loopback interface.

Subnet Mask - Enter the Subnet mask for the given IP Address.

Broadcast Address - Displays the Broadcast address for the specified IP address.

5.1.5 IVR-VLAN Mapping



IVR - VLAN MAPPING

VLAN Interface	*
Switch	default
Associated Vlan	*

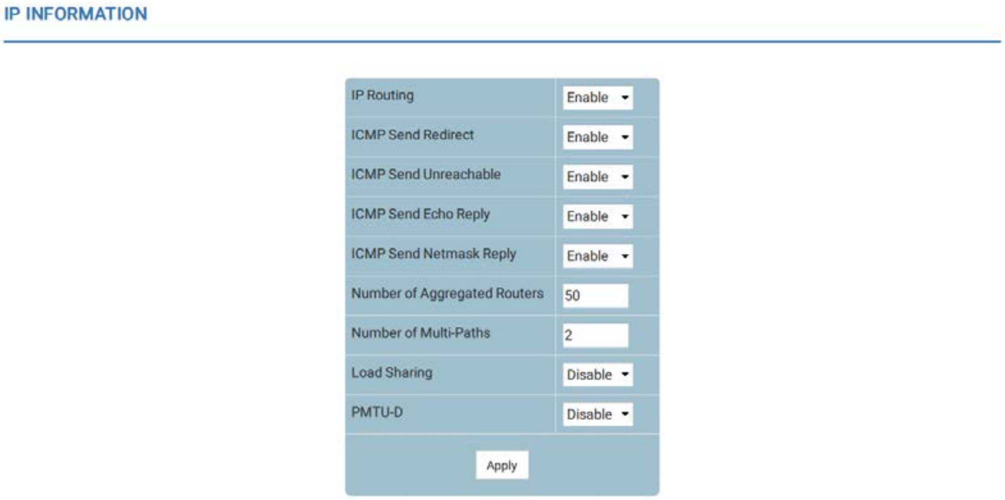
Select	VLAN Interface	Context	Associated Vlan

Fig: IVR - Vlan Mapping

The *IVR - Vlan Mapping* link opens the **IVR - Vlan Mapping** Page.
The IVR - Vlan Mapping page allows the user to configure the list of VLANs to be associated for an IVR interface.

The table below lists the fields present in this page.
VLAN Interface - Enter the primary IVR interface ID to which the VLAN or list of VLANs should be mapped. The interface ID uniquely identifies a specific VLAN created in the system through the VLAN Interface Basic Settings page.
This value ranges between 1 and 4094.
> The VLAN or list of VLANs can be mapped only to the IVR interfaces already created in the system.
Switch - Select the context name for which the IVR-VLAN mapping should be done.
This lists names of all contexts available in the system. By default, the context default is created in the system.
Associated Vlan - Enter the VLAN ID or list of VLAN IDs to be mapped with the specified IVR interface.
The format of this entry for VLAN list is VLAN ID, VLAN ID. Example: 2,7,9.
> The VLANs can be mapped to only one IVR interface. That is the VLAN associated to one IVR interface cannot be associated to another IVR interface.

5.1.6 IP/ICMP Scalars



IP INFORMATION

IP Routing	Enable
ICMP Send Redirect	Enable
ICMP Send Unreachable	Enable
ICMP Send Echo Reply	Enable
ICMP Send Netmask Reply	Enable
Number of Aggregated Routers	50
Number of Multi-Paths	2
Load Sharing	Disable
PMTU-D	Disable

Fig: IP Information

The *IP/ICMP Scalars* link opens the **IP Information** Page.

The IP Information page allows the user to configure the basic loopback settings.

The table below lists the fields present in this page.

IP Routing - Routing configuration

By default it is set as Enable. The list contains:

* Enable - Enable IP routing

* Disable - Disable IP routing

ICMP Send Redirect - Select the ICMP Send redirect status on an interface basis.

By default it is set as Enable. The list contains:

* Enable - Allows sending ICMP Redirect Message

* Disable - Does not allow sending ICMP Redirect Message

ICMP Send Unreachable - Select the ICMP Send unreachable status.

By default it is set as Enable. The list contains:

* Enable - Allows sending ICMP unreachable message

* Disable - Does not allow sending ICMP unreachable message

ICMP Send Echo Reply - Select the ICMP send Echo reply status.

By default it is set as Enable. The list contains:

* Enable - Allows sending ICMP Echo Reply Message

* Disable - Does not allow sending ICMP Echo Reply Message

ICMP Send Netmask Reply - Select the ICMP Send Netmask Reply status.

By default it is set as Enable. The list contains

* Enable - Allows sending ICMP Net Mask Reply Message

* Disable - Does not allow sending ICMP Net Mask Reply Message

Number of Aggregated Routers - Enter the number of aggregated routes that can be configured in the system. This value will come in to effect only after rebooting the router. The value ranges between 5 and 4095.

> Note the new value can only be smaller than the current value.

Number of Multi-Paths - Enter the number of multi-paths in the routing table.

The value ranges from 1 to 16. By default it is 2.

Load Sharing - Enter the load sharing status.

By default it is Disable. The list contains:

* Enable - Allows the distribution of the load available in the equal cost multi-paths

* Disable - Does not allow the distribution of the load available in the equal cost multi-paths

PMTU-D - Select this object to enable or disable the PMTU-D on all paths globally.

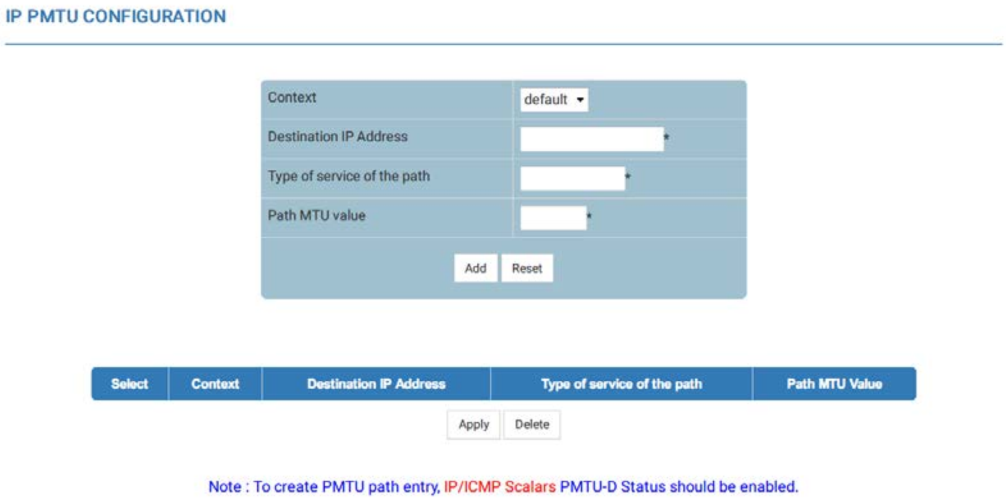
By default it is Disable. The list contains:

* Enable - Overrides the route-based and application-level requests for PMTU-D.

* Disable - PMTU-D is not done even if the application requests to do so.

> To configure IP PMTU, PMTU-D field should be enabled.

5.1.7 IP PMTU



IP PMTU CONFIGURATION

Context	default
Destination IP Address	*
Type of service of the path	*
Path MTU value	*

Select	Context	Destination IP Address	Type of service of the path	Path MTU Value

Note : To create PMTU path entry, IP/ICMP Scalars PMTU-D Status should be enabled.

Fig: IP PMTU Configuration

The *IP PMTU* link opens the **IP PMTU Configuration** Page.

The IP PMTU Configuration page allows the user to configure the IP PMTU.

The table below lists the fields present in this page.

Context - Select routing context.

By default it as set as default. The list contains:

* default - use the "default" VRF table for switch front ports

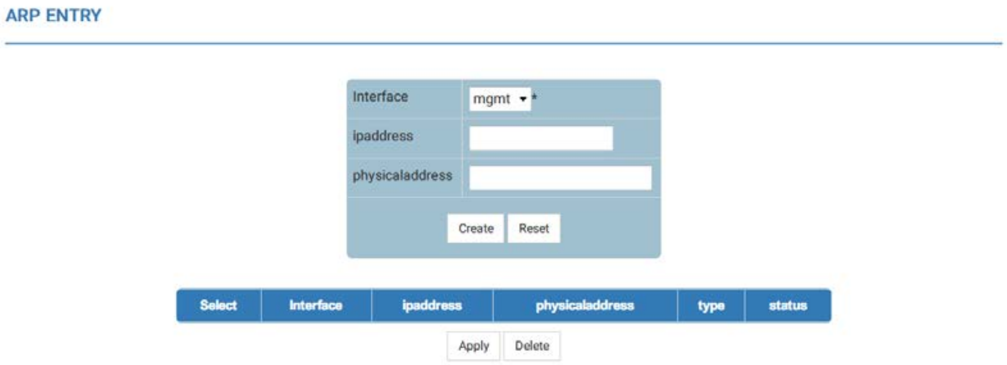
* mgmt - use the "mgmt VRF table for switch OOB port

Destination IP Address - Enter the destination IP address of the Path for which the discovery is made.

Type of service of the path - Enter the type of service of the path. The value ranges from 0 to 255.

Path MTU value - Enter the value of the path MTU discovered. If the admin changes this value, PMTU discovery on that path is stopped. The value ranges from 68 to 65535.

5.1.8 STATIC ARP


ARP ENTRY

Interface: mgmt *

ipaddress:

physicaladdress:

Select	Interface	ipaddress	physicaladdress	type	status

Fig: ARP ENTRY

The *STATIC ARP* link opens the **ARP ENTRY** Page.

The ARP ENTRY page allows the user to configure the static entry in the ARP cache.

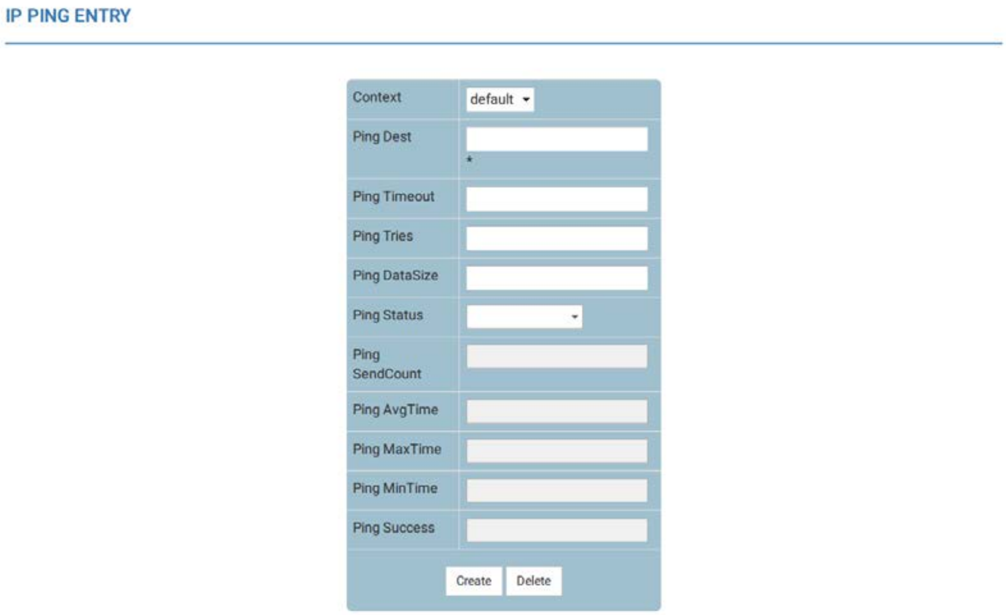
The table below lists the fields present in this page.

Interface - Select the interface to add a static entry in the ARP cache.

ipaddress - Enter the IP address to map to the specified MAC address.

physicaladdress - Enter the MAC address to map to the specified IP address.

5.1.9 IP PING


IP PING ENTRY

Context	default
Ping Dest	*
Ping Timeout	
Ping Tries	
Ping DataSize	
Ping Status	
Ping SendCount	
Ping AvgTime	
Ping MaxTime	
Ping MinTime	
Ping Success	

Fig: IP PING ENTRY

The *IP PING* link opens the **IP PING ENTRY** Page.

The IP PING ENTRY page allows the user to send ICMP echo request messages.

The table below lists the fields present in this page.

Context - Select routing context.

By default it as set as default. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Ping Dest - Enter the IP address of the node to be pinged.

Ping Timeout - Configures the time in seconds after which the entity waiting for the ping response times out. The value ranges between 1 and 100.

Ping Tries - Configures the packet count. The value ranges between 1 and 10.

Ping DataSize - Enter the size of the data portion of the PING PDU. This value ranges between 0 and 2080.

Ping Status - Indicates if the ping is in progress. Possible values are:

1 - not initiated

2 - in progress

3 - completed

Ping SendCount - Number of requests sent already.

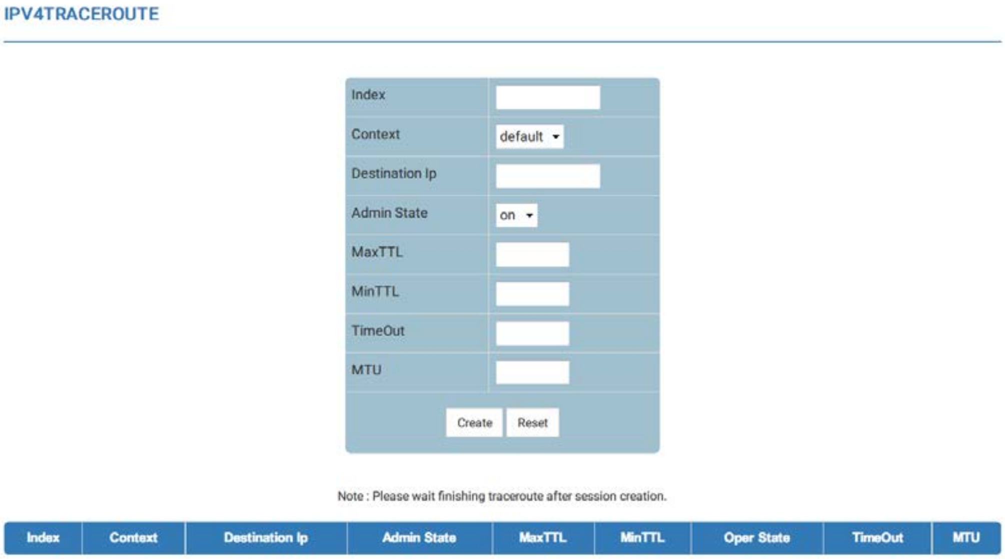
Ping AvgTime - Average time taken for successful replies.

Ping MaxTime - Max delayed pkt so far.

Ping MinTime - Time taken by the fastest reply received.

Ping Success - Total number of replies received.

5.1.10 IPV4TRACEROUTE


IPV4TRACEROUTE

Index	
Context	default
Destination Ip	
Admin State	on
MaxTTL	
MinTTL	
TimeOut	
MTU	

Note : Please wait finishing traceroute after session creation.

Index	Context	Destination Ip	Admin State	MaxTTL	MinTTL	Oper State	TimeOut	MTU

Fig: IPV4TRACEROUTE

The *IPV4TRACEROUTE* link opens the **IPV4TRACEROUTE** Page.

The IPV4TRACEROUTE page allows the user to trace route to the Destination IP.

The table below lists the fields present in this page.

Index - Specifies an integer which may be used as a new index in the table.

Context Name - Select routing context.

By default it as set as default. The list contains:

* default - use the "default" VRF table for switch front ports

* mgmt - use the "mgmt VRF table for switch OOB port

Destination Ip - Specifies the destination IPV4 address.

Admin State - Start or stop the Trace operation. Options are:

* on - Start the Trace operation

* off - Stop the Trace operation

MaxTTL - Maximum value (in seconds) of the TTL field to be filled up in the IP packets used for the trace route.

The value ranges between 1 and 99.

MinTTL - Minimum value (in seconds) of the TTL field to be filled up in the IP packets used for the trace route.

The value ranges between 1 and 99.

TimeOut - Timeout (in 0.1 seconds) to be used for tracing.

The value ranges between 1 and 100.

MTU - Size of the data to be sent with trace.

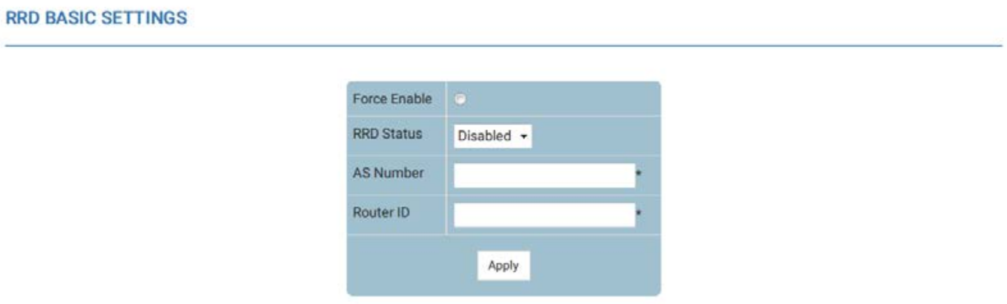
The value ranges between 1 and 100.

5.2 RRD

The *RRD* link allows you to configure the RRD related parameters for switch. User can configure RRD on the following four pages.

- Basic Settings
- BGP
- RIP
- OSPF

5.2.1 Basic Settings



RRD BASIC SETTINGS

Force Enable	○
RRD Status	Disabled ▾
AS Number	*
Router ID	*

Fig: RRD Basic Settings

The *Basic Settings* link opens the **RRD Basic Settings** Page.

The RRD Basic Settings page allows the user to enable or disable the RRD for a specific AS number and Router ID.

The table below lists the fields present in this page.

Force Enable - Click to forcefully reconfigure the AS number and Router Id for the RTM Virtual context.

RRD Status - Select the admin status of the RTM in the virtual context. By Default the value of RRD status is Disabled. The list contains:

* Enabled - Sets the RTM admin status as enabled in the virtual context.

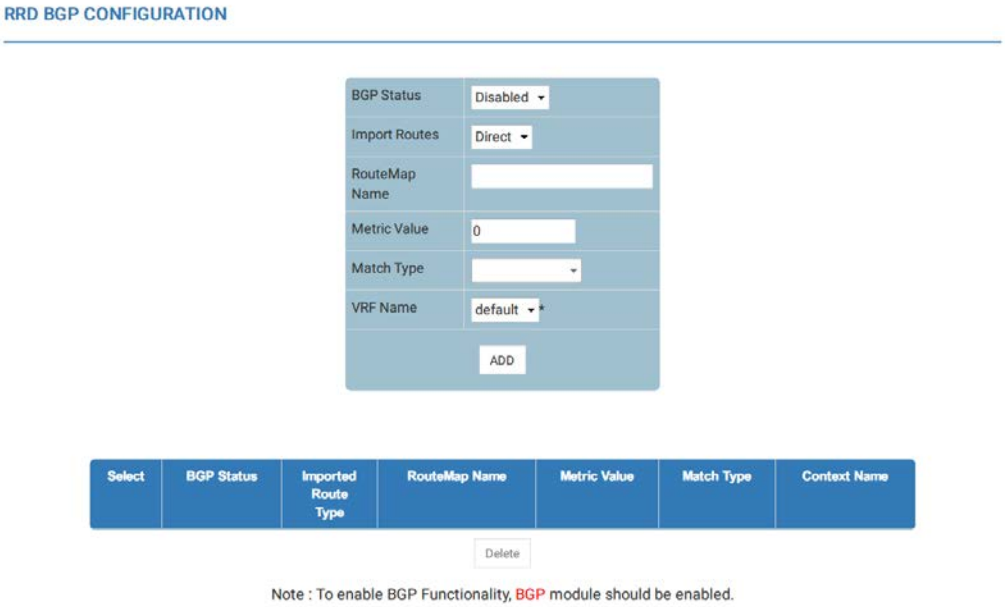
* Disabled - Sets RTM admin status as disabled in the virtual context.

AS number - Enter the Autonomous system number in which RTM Virtual context is running. This value ranges between 1 and 65535. By default the value of Autonomous system number is 0.

Router ID - Enter the BGP/OSPF Router ID for the RTM Virtual context.

> Router ID can only be configured once

5.2.2 BGP



RRD BGP CONFIGURATION

BGP Status	Disabled
Import Routes	Direct
RouteMap Name	
Metric Value	0
Match Type	
VRF Name	default *

Select	BGP Status	Imported Route Type	RouteMap Name	Metric Value	Match Type	Context Name

Note : To enable BGP Functionality, BGP module should be enabled.

Fig: RRD BGP Configuration

The *BGP* link opens the **RRD BGP Configuration** Page.

The RRD BGP Configuration page allows the user to configure the re-distribution of the routes that are learnt through other routing protocols to BGP.

The table below lists the fields present in this page.

Select - Click to select the BGP routes for which RRD status needs to be deleted.

BGP Status - Select the route redistribution status for BGP. By default BGP Status is set as Disabled. The list contains:

* Enabled - Imports the routes specified in the field import into BGP and distributes the BGP learnt routes to IGP (Interior Gateway Protocol) (RIP and OSPF). Redistributes route information for both internal and external Border Gateway Protocol

* Disabled - Removes the routes specified in the field import from BGP and does not distribute or import routes from IGP (RIP and OSPF).

Import Routes - Select the routes to import and control the redistribution of routes.

By default the import is set as Direct Routes. The list contains;

* Direct routes - Enables import of directly connected routes into BGP

* Static routes - Enables import of static routes into BGP.

* RIP routes - Enables import of RIP routes into BGP.

* OSPF routes - Enables import of OSPF routes into BGP.

Routemap Name - Enter the route map name that identifies the specified route-map in the list of route-maps. This value is a string with the maximum size as 20.

Metric Value - Enter the metric value that needs to be applied to the route before it is advertised into the BGP This value is the domain Metric used for generating the default route. If the metric value is not specified, the default metric value considered as 1. The value used is specific to the protocol. This value ranges between 0 and 4294967295.

Metric Type - Select the Metric type applied to the route before it is advertised into the OSPF domain

* External - Redistributes OSPF external routes

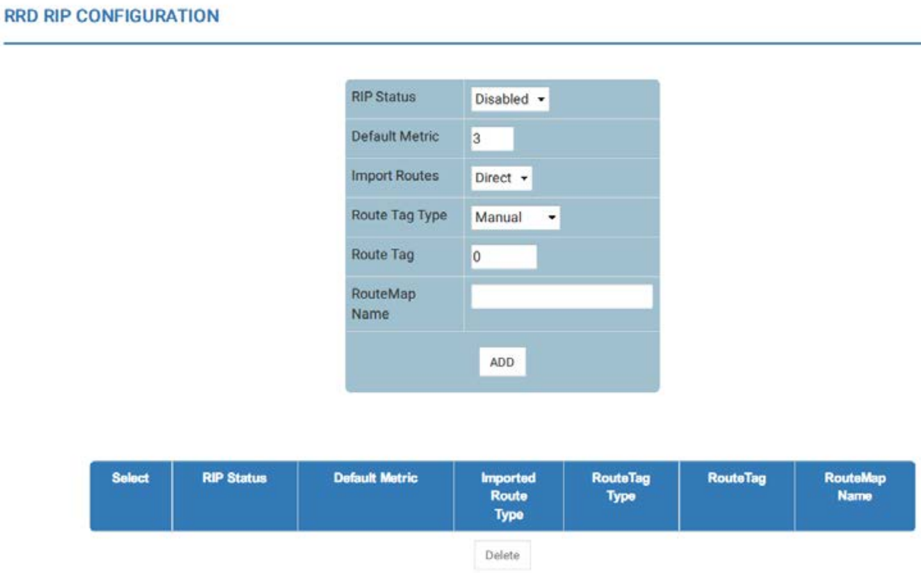
* internal - Redistributes OSPF internal routes

* NSSA-External - Redistributes OSPF NSSA external routes

> This field is enabled only when the import route is set as OSPF

VRF Name / Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.2.3 RIP



RRD RIP CONFIGURATION

RIP Status	Disabled
Default Metric	3
Import Routes	Direct
Route Tag Type	Manual
Route Tag	0
RouteMap Name	

Select	RIP Status	Default Metric	Imported Route Type	RouteTag Type	RouteTag	RouteMap Name

Fig: RRD RIP Configuration

The *RIP* link opens the **RRD RIP Configuration** Page.
The RRD RIP Configuration page allows the user to configure re-distribution of the routes that are learnt through other routing protocols to RIP.

The table below lists the fields present in this page.
Select - Click to select the RIP routes for which RRD status needs to be deleted.
RIP Status - Select the route redistribution status for RIP. By default the RIP status is Disabled. The options are:
* Enabled - Sets the route redistribution status as enabled.
When enabled, it advertises the routes learned by other protocols and redistributes route information for both internal and external Routing Information Protocol
* Disabled - Sets the route redistribution status as disabled and stops redistribution of routes but sends updates to the RTM.
Default Metric - Enter the default metric for the imported routes. This value ranges between 0 and 16. By Default the Default Metric value is set as 3.
Import Routes - Select the protocol from which the routes are to be imported to RIP. By default the RIP status is set as Direct The list contains:
* Direct routes - Enables import of directly connected routes into RIP
* Static routes - Enables import of static routes into RIP.
* OSPF routes - Enables import of OSPF routes into RIP.
* BGP routes - Enables import of BGP routes into RIP.

Route Tag Type - Select whether the tag is manually configured or automatically generated. By Default the Route Tag Type is set as Manual. The list contains:

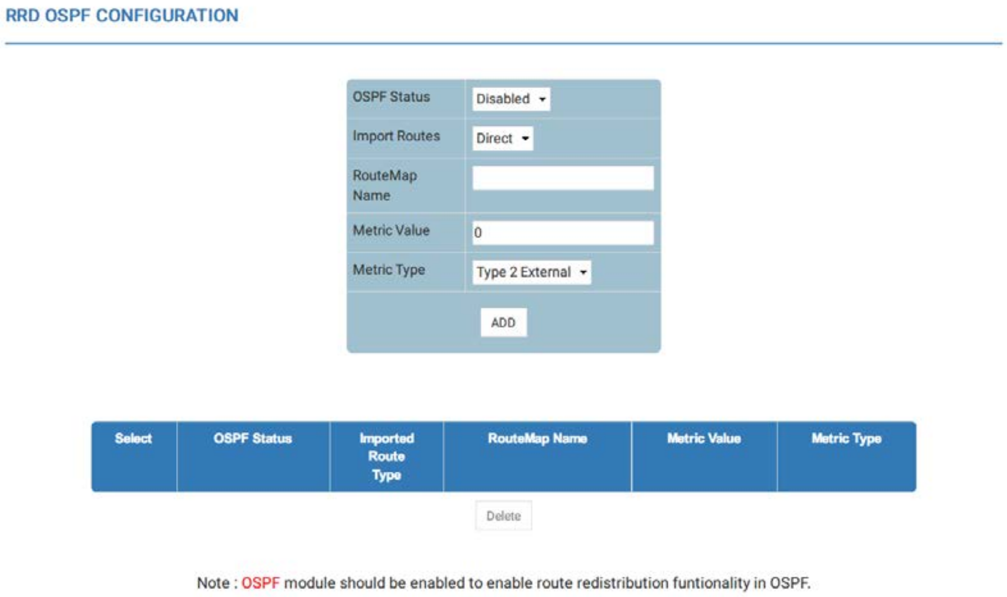
* Manual - Generates the tags manually.

* Automatic - Generates the tag automatically.

Route Tag - Enter the route tag if the route tag type is selected as Manual. This value ranges between 0 and 65535. By default the route tag value is set as 0.

Route Map Name - Enter the name that identifies the specified route-map in the list of route-maps. This is a unique string value with size between 1 and 20.

5.2.4 OSPF



RRD OSPF CONFIGURATION

OSPF Status	Disabled
Import Routes	Direct
RouteMap Name	
Metric Value	0
Metric Type	Type 2 External
	ADD

Select	OSPF Status	Imported Route Type	RouteMap Name	Metric Value	Metric Type

Delete

Note : OSPF module should be enabled to enable route redistribution funtionality in OSPF.

Fig: RRD OSPF Configuration

The *OSPF* link opens the **RRD OSPF Configuration** Page.

The RRD OSPF Configuration page allows the user to configure the redistribution of the routes that are learnt through other routing protocols to OSPF.

The table below lists the fields present in this page.

Select - Click to select the OSPF routes for which RRD status needs to be deleted.

OSPF Status - Select the status of route redistribution for OSPF. By Default OSPF status is set as Disabled. The options are:

* Enabled - Sets the OSPF status as enables. When enabled the advertises the routes learnt by other protocols.

* Disabled - Stops the redistribution of the routes but updates the Common Routing Table using the queue interface.

Import Routes / Imported Route Type - Select the source protocols from which routes are imported to OSPF. By Default routes are Imported from Direct routes The list contains:

* Direct routes - Enables import of directly connected routes into OSPF

* Static routes - Enables import of static routes into OSPF.

* RIP routes - Enables import of RIP routes into OSPF.

* BGP routes - Enables import of BGP routes into OSPF.

Route Map Name - Enter the name that identifies the specified route-map in the list of route-maps. This is a unique string value with size between 1 and 20.

Metric Value - Sets the Metric Type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain.

Metric Type - Select the Metric type applied to the route before it is advertised into the OSPF domain. By default Metric Type is set to Type 2 External. The list contains:

* Type 1 External - Sets metric type as type 1

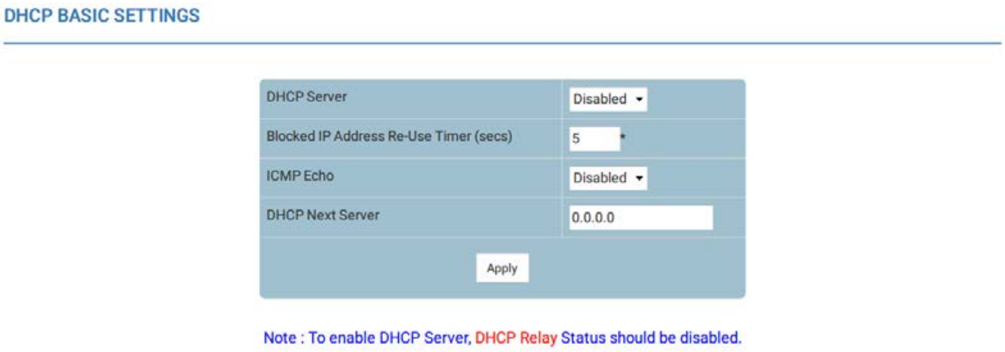
* Type 2 External - Sets metric type as type 2

5.3 DHCP Server

The *DHCP Server* link allows you to configure the DHCP Server related parameters for switch. User can configure DHCP Server on the following 7 pages.

- Basic Settings
- Pool Settings
- Pool Options
- Exclude List
- Host Settings
- Host Options
- Bootfile Configuration

5.3.1 Basic Settings



DHCP BASIC SETTINGS

DHCP Server	Disabled
Blocked IP Address Re-Use Timer (secs)	5 *
ICMP Echo	Disabled
DHCP Next Server	0.0.0.0

Note : To enable DHCP Server, DHCP Relay Status should be disabled.

Fig: DHCP Basic Settings

The *Basic Settings*link opens the **DHCP Basic Settings**Page.

The DHCP Basic Settingspage allows the user to configure the basic DHCP settings.

* To enable DHCP Server, DHCP Relay Status should be disabled.

The table below lists the fields present in this page.

DHCP-Server - Select the DHCP server status in the router.

By default, the DHCP Server is set as Disabled. The list contains:

* Enabled - Enables the DHCP server in the router and it start serving the serverwith the IP addresses. It will open the UDP socket and start listening for DHCP Discover messages from Clients

* Disabled - Disables the DHCP server in the router.

> The DHCP server can be set as Enabled, only if the Service DHCP-Relay is set as Disabled.

Blocked IP Address Re-Use Timer (secs) - Enter the Reuse timeout value in seconds that is used by DHCP. It denotes the amount of time the DHCP server entity would wait for the DHCP REQUEST from the client, before reusing the offer, like the blocked IP address. The value zero disables this timer.

This value ranges between 1 and 120 seconds. Default value is 5 seconds.

ICMP Echo - Select the status of ICMP (Internet Control Message Protocol) Echo feature. Echo means ICMP Echo Request message. This object controls the server to probe for the IP address before allocating the IP address to a client through the ICMP echo message.

By default ICMP Echo is set as Disabled. The list contains:

* Enabled - Enables the ICMP Echo feature. Before allocating an IP Address to client, the server will broadcast ICMP Echo Request (Ping Packet) to check whether any other machine/host is using this IP. If there is no response received, the Server will allocate the IP to the client.

* Disabled - Disables the ICMP Echo feature. The ICMP Echo Request packet mechanism will not be used. The IP will be directly allocated to the client

DHCP Next Server - Enter the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded in a DHCP client. This boot server acts as a secondary server. The DHCP server is used as the boot server, if no TFTP server is configured as the boot server. Default value is 0.0.0.0 (No boot server is defined. DHCP server is used as the boot server)

5.3.2 Pool Settings

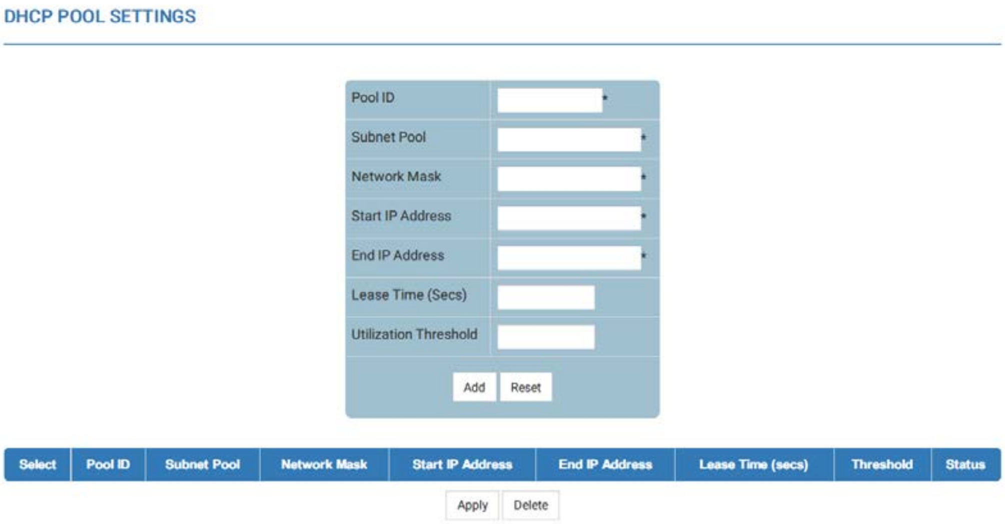


Fig: DHCP Pool Settings

The *Pool Settings* link opens the **DHCP Pool Settings** Page.

The DHCP Pool Settings page allows the user to configure the IP address pool that can be used by the DHCP server to allocate IP addresses.

The table below lists the fields present in this page.

Pool ID - Enter the pool Id to index among the different subnet pools configured. The range of the pool ID is between 1 and 2147483647.

Subnet Pool - Enter the subnet of the IP address in the pool.

Network Mask - Enter the Network mask. It denotes the client- s subnet mask of the IP address in the pool.

Start IP Address - Enter the first IP address in the address pool that is used for dynamic allocation by the DHCP server. This specifies the lower limit for IP address in an address pool.

End IP Address - Enter the last IP address in the address pool that is used for dynamic allocation by the DHCP server. This specifies the upper limit for IP address in an address pool.

Lease Time (Secs) - Enter the time interval for which the IP address is valid. It specifies the amount of time that the client can use the IP address assigned by the server. It is specific to each IP address pool. Every IP address allocated from a pool will be returned to the pool, if the client does not renew it. This value ranges between 60 and 2147483647 seconds. Default value is 3600 seconds.

Utilization threshold - Enter the DHCP Pool utilization threshold value in percentage. This specifies the upper limit for the address pool utilization, after which a notification will be sent to SNMP manager.

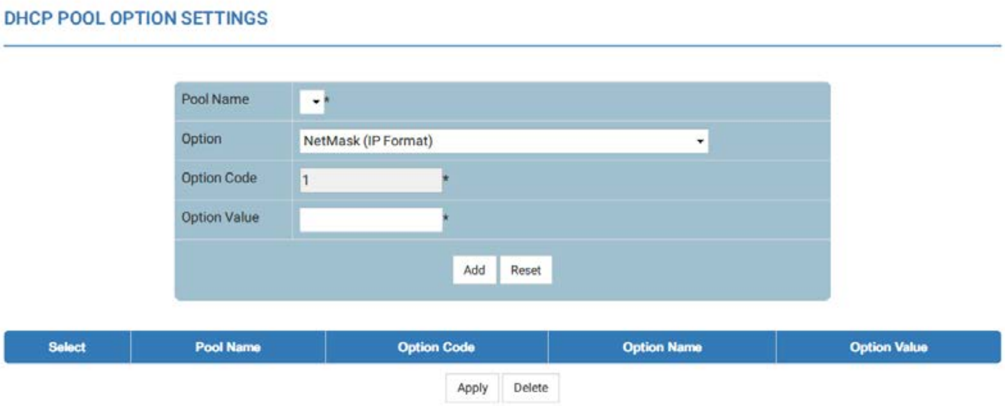
The utilization threshold ranges between 0 and 100 percentage. Default value is 75 percentages.

Status - Select the status of the entry. It denotes the status of address pool configuration and allocation of IP address. Options are

* UP: Address pool is configured successfully and IP address allocation can take place.

* Down: Address pool is not configured successfully and no IP address allocation can take place

5.3.3 Pool Options



DHCP POOL OPTION SETTINGS

Pool Name	*
Option	NetMask (IP Format)
Option Code	1 *
Option Value	*

Select	Pool Name	Option Code	Option Name	Option Value

Fig: DHCP Pool Options Settings

The *Pool Options* link opens the **DHCP Pool Options Settings** Page.

The DHCP Pool Options Settings page allows the user to set the DHCP server pool options related configuration. The configured options are sent to DHCP client in DHCP offer packet.

The table below lists the fields present in this page.

Pool Name - Select the pool name from the list for which DHCP pool options related configuration needs to be applied.

Option - Select the DHCP pool option that is to be set to the selected pool name.

Option Code - Displays the corresponding DHCP option code for the DHCP option selected in the field Option.

Option Value - Enter the value to be set for the DHCP option selected in the field Option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.

5.3.4 Exclude List

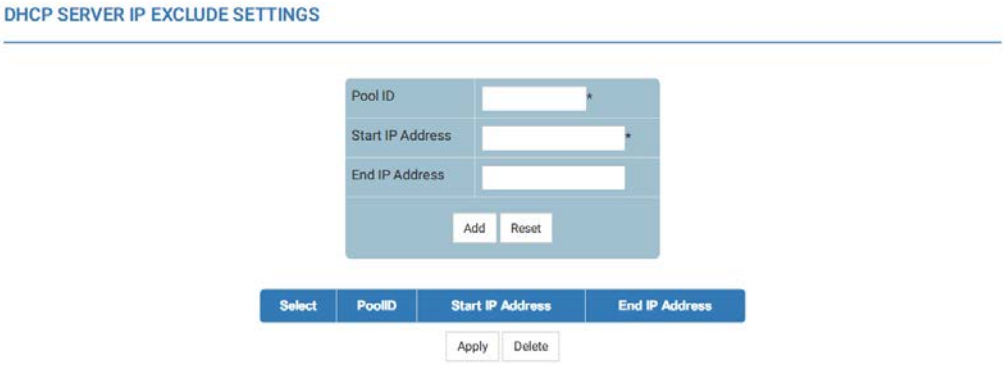


Fig: DHCP Server IP Exclude Settings

The *Exclude List* link opens the **DHCP Server IP Exclude Settings** Page.

The DHCP Server IP Exclude Settings page allows the user to configure the DHCP server IP address to be excluded from the DHCP server address pool. The addresses in the created list are not allocated to the DHCP client while performing dynamic IP allocation.

The table below lists the fields present in this page.

Pool id - Enter the pool ID for which exclude list is to be created.

Start IP address - Enter the start IP address for the exclude list. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool.

This IP address should be:

* low than the end IP address of the exclude list, and

* in the same network of the subnet pool- s start IP address.

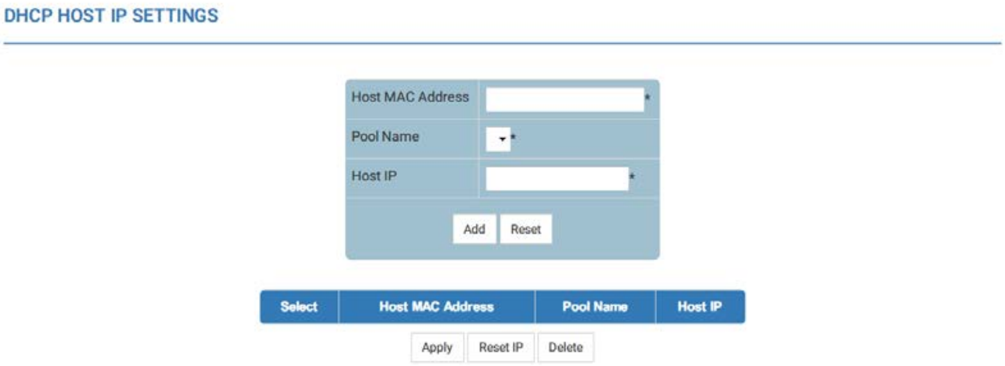
End IP address - Enter the end IP address for the exclude list. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool.

This IP address should be:

* high than the start IP address of the exclude list, and

* within or equal to the subnet pool- s end IP address.

5.3.5 Host Settings



DHCP HOST IP SETTINGS

Host MAC Address	*
Pool Name	*
Host IP	*

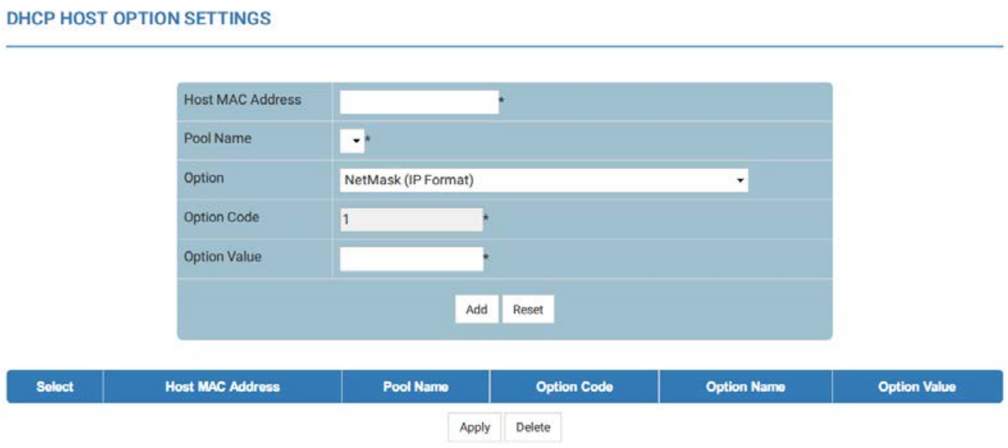
Select	Host MAC Address	Pool Name	Host IP

Fig: DHCP Host IP Settings

The *Host Settings* link opens the **DHCP Host IP Settings** Page.
The DHCP Host IP Settings page allows the user to configures the DHCP Server Host-IP to assign a static IP address for a specific MAC address.

The table below lists the fields present in this page.
Host MAC Address - Enter the Host MAC address to be assigned a static IP address.
Pool Name - Select the pool name from the list for which DHCP Host-IP related configuration needs to be applied.
Host IP - Enter the static IP address assigned for a specific MAC.

5.3.6 Host Options


DHCP HOST OPTION SETTINGS

Host MAC Address	*
Pool Name	*
Option	NetMask (IP Format)
Option Code	1 *
Option Value	*

Select	Host MAC Address	Pool Name	Option Code	Option Name	Option Value

Fig: DHCP Host Option Settings

The *Host Options* link opens the **DHCP Host Option Settings** Page.

The DHCP Host Option Settings page allows the user to set the DHCP server host options related configuration. The configured options are sent to the configured DHCP client in DHCP offer packet.

The table below lists the fields present in this page.

Host MAC Address - Enter the Host MAC address to be configured.

Pool Name - Select the pool name from the list for which DHCP host options related configuration needs to be applied.

Option - Select the DHCP host option that is to be set to the Host MAC Address.

Option Code - Displays the corresponding DHCP option code for the DHCP option selected in the field Option.

Option Value - Enter the value to be set for the DHCP option selected in the field Option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP option.

5.3.7 Bootfile Configuration

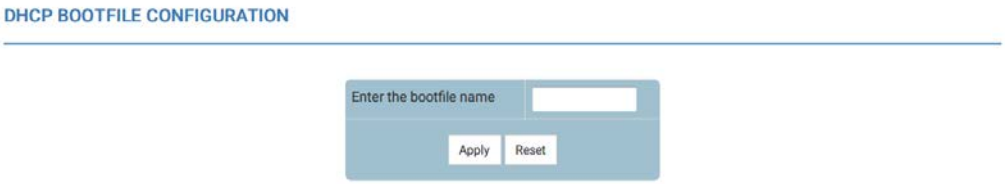


Fig: DHCP Bootfile Configuration

The *Bootfile Configuration* link opens the **DHCP Bootfile Configuration** Page.

The DHCP Bootfile Configuration page allows the user to configure the name of the initial boot file to be loaded in a DHCP client. The boot file contains the boot image that is used as the operating system for the DHCP client.

The table below lists the fields present in this page.

Enter the bootfile name - Enter the name of the boot image file to be downloaded.

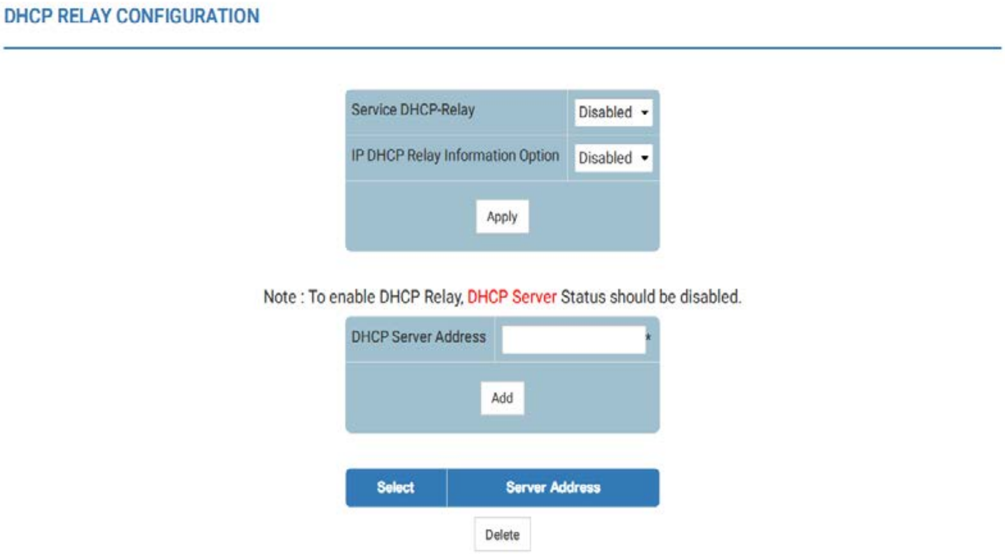
The file name is a string whose maximum size is 63.

5.4 DHCP Relay

The *DHCP Relay* link allows you to configure the DHCP Relay related parameters for switch. User can configure DHCP Relay on the following 2 pages.

- Basic Settings
- Interface Settings

5.4.1 Basic Settings



DHCP RELAY CONFIGURATION

Service DHCP-Relay: Disabled

IP DHCP Relay Information Option: Disabled

Note : To enable DHCP Relay, DHCP Server Status should be disabled.

DHCP Server Address: *

Select	Server Address

Fig: DHCP Relay Configuration

The *Basic Settings* link opens the **DHCP Relay Configuration** Page.

The DHCP Relay Configuration page allows the user to configure basic DHCP Relay information.

* To enable DHCP Relay, DHCP-Server Status should be disabled..

The table below lists the fields present in this page.

Service DHCP-Relay - Select the DHCP relay status in the switch. Options are:

* Enabled - Enables the DHCP relay status in the switch. The Relay Agent forwards the packets from the client to a specific DHCP server.

* Disabled - Disables the DHCP relay status in the switch.

By default, this is Disabled.

> The service DHCP relay can be set as Enabled, only if the DHCP-Server is set as Disabled.

IP DHCP Relay Information Option - Select the controlling status of the processing related to the Relay Agent Information options.

By default, the relay information option is set as Disabled. The list contains:

* Enabled - Enables the controlling status of the processing related to the Relay Agent Information options for inserting the necessary information while relaying a packet from a client to a server and examining/stripping of the inserted information when relaying a packet from a server to a client.

* Disabled - Disables the controlling status of the processing related to the Relay Agent Information options.

DHCP Server Address - Enter the IP address of the DHCP Server to which the Relay Agent needs to forward the packets from the client. A maximum of 5 servers can be configured. If no servers are configured, then the DHCP packets will be broadcast to entire network, except the network from which packet was received.

5.4.2 Interface Settings

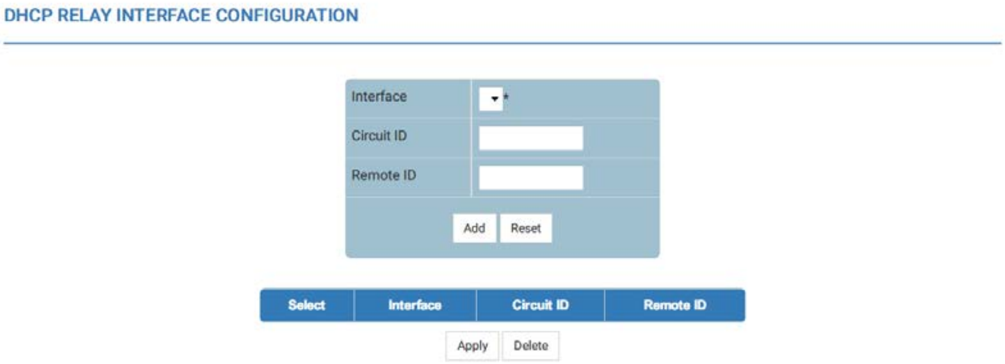


Fig: DHCP Relay Interface Configuration

The *Interface Settings* link opens the **DHCP Relay Interface Configuration** Page.

The DHCP Relay Interface Configuration page allows the user to configure the interface settings of the DHCP Relay.

The table below lists the fields present in this page.

Interface - Select the Interface.

Circuit ID - Enter the Circuit ID that is to be configured for this interface. Values other than interface indices can be configured for this object. Configuring with zero value will reset the circuit id configuration for this interface.

This value ranges between 1 and 2147483647. The minimum value configurable for circuit-id is system's maximum default interfaces + 1.

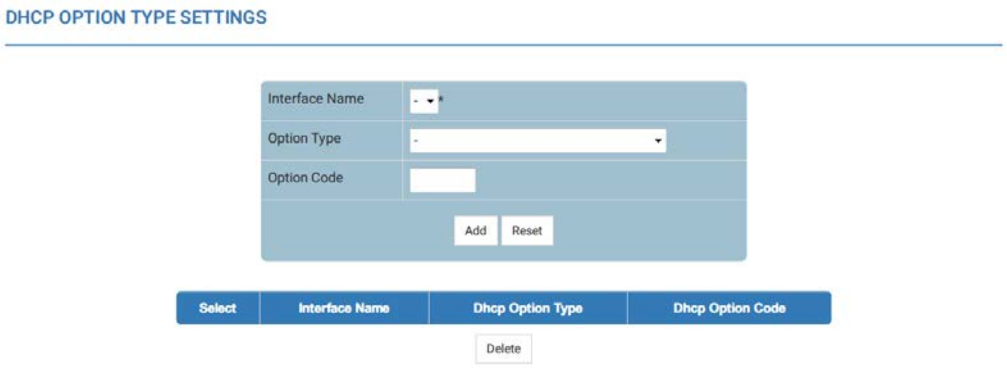
Remote ID - Enter the Remote ID that is to be configured for this interface. String of length zero will reset the configuration. Value other than the default value internally can be configured for this object.

5.5 DHCP Client

The *DHCP Client* link allows you to configure the DHCP Client related parameters for switch. User can configure DHCP Client on the following 2 pages.

- DHCPC OptionType
- DHCPC ClientId

5.5.1 DHCPC OptionType


DHCP OPTION TYPE SETTINGS

Select	Interface Name	Dhcp Option Type	Dhcp Option Code

Fig: DHCP Option type Settings

The *DHCPC OptionType* link opens the **DHCP Option type Settings** Page.
The DHCP Option type Settings page allows the user to configure DHCP option type to request the server. This is required to send DHCP request to get the tftp server name and Boot file name.

The table below lists the fields present in this page.
Select - Click to select an interface for which DHCP option type configurations need to be modified or deleted.
Interface Name - Select an interface for which DHCP option type settings need to be configured from the list of vlan interfaces already created in the system.
Option Type - Select the DHCP Client Option Type for the specified interface created in the system.
The list contains;
* TFTP Server Name (IP Format/String) - Sends the DHCP requests to get the TFTP server's domain name
* Bootfile Name (String) - Sends the DHCP requests to get the boot File Name
Option Code - Displays the Option code for the specified interface created in the system.
When option code is displayed as:
* 66 - Indicates TFTP Server Name (IP Format/String) is set. This allows to identify a TFTP server when the same field in the DHCP header is used for DHCP options
* 67 - Indicates Bootfile Name (String) is set. This allows to identify a bootfile when the file field in the DHCP header is used for DHCP options.
* 0 - Indicates no option type is set for the interface

5.5.2 DHCPC ClientId

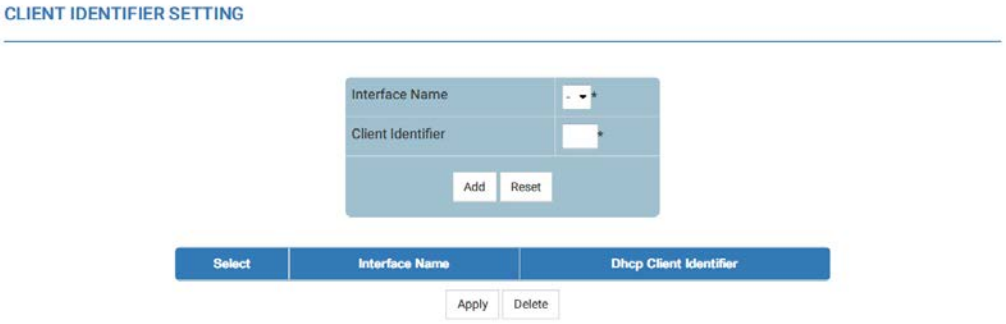


Fig: Client Identifier Setting

The *DHCPC ClientId* link opens the **Client Identifier Setting** Page.
The Client Identifier Setting page allows the user to configure DHCP client identifiers for the interfaces created in the system. This client-id is advertised in the DHCP control packets.

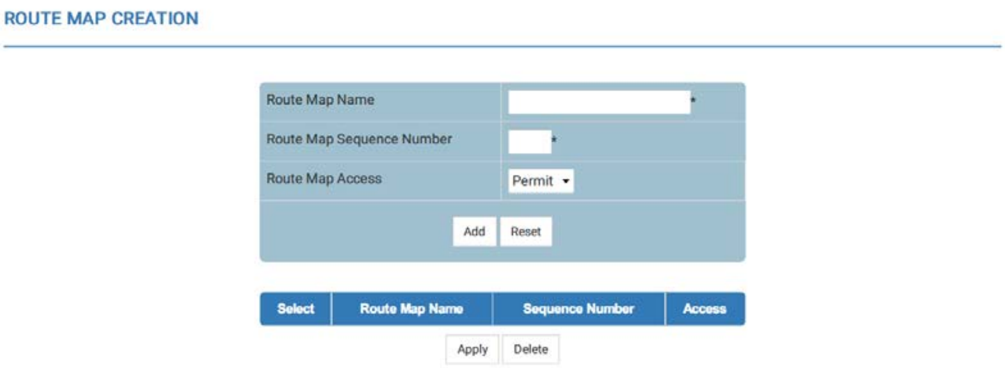
The table below lists the fields present in this page.
Select - Click to select an interface for which DHCP option type configurations need to be modified or deleted.
Interface Name - Select an interface for which DHCP option type settings need to be configured from the list of vlan interfaces already created in the system.
Client Identifier - Enter the unique identifier of DHCP client for the specified interface created in the system. Client Id is used in all DHCP client messages. This identifier will be used in dhcp server to maintain client information. This identifier can be mac address or any string.

5.6 Route Map

The *Route Map* link allows you to configure the Route Map related parameters for switch. User can configure Route Map on the following 4 pages.

- Route Map Creation
- Route Map Match
- Route Map Set
- Ip Prefix List

5.6.1 Route Map Creation



ROUTE MAP CREATION

Route Map Name	*
Route Map Sequence Number	*
Route Map Access	Permit

Select	Route Map Name	Sequence Number	Access

Fig: Route Map Creation

The *Route Map Creation* link opens the **Route Map Creation** Page.

The Route Map Creation page allows the user to create Route Map.

The table below lists the fields present in this page.

Route Map Name - Enter the specified route-map name in the list of route-maps. The length of the name ranges between 1 and 20.

Route Map Sequence Number - Enter the position of a new route map in the list of route maps already configured with the same name. The range for the number is between 1 and 10.

Route Map Access - Select the access type associated with the sequence number in a route-map.

Options are:

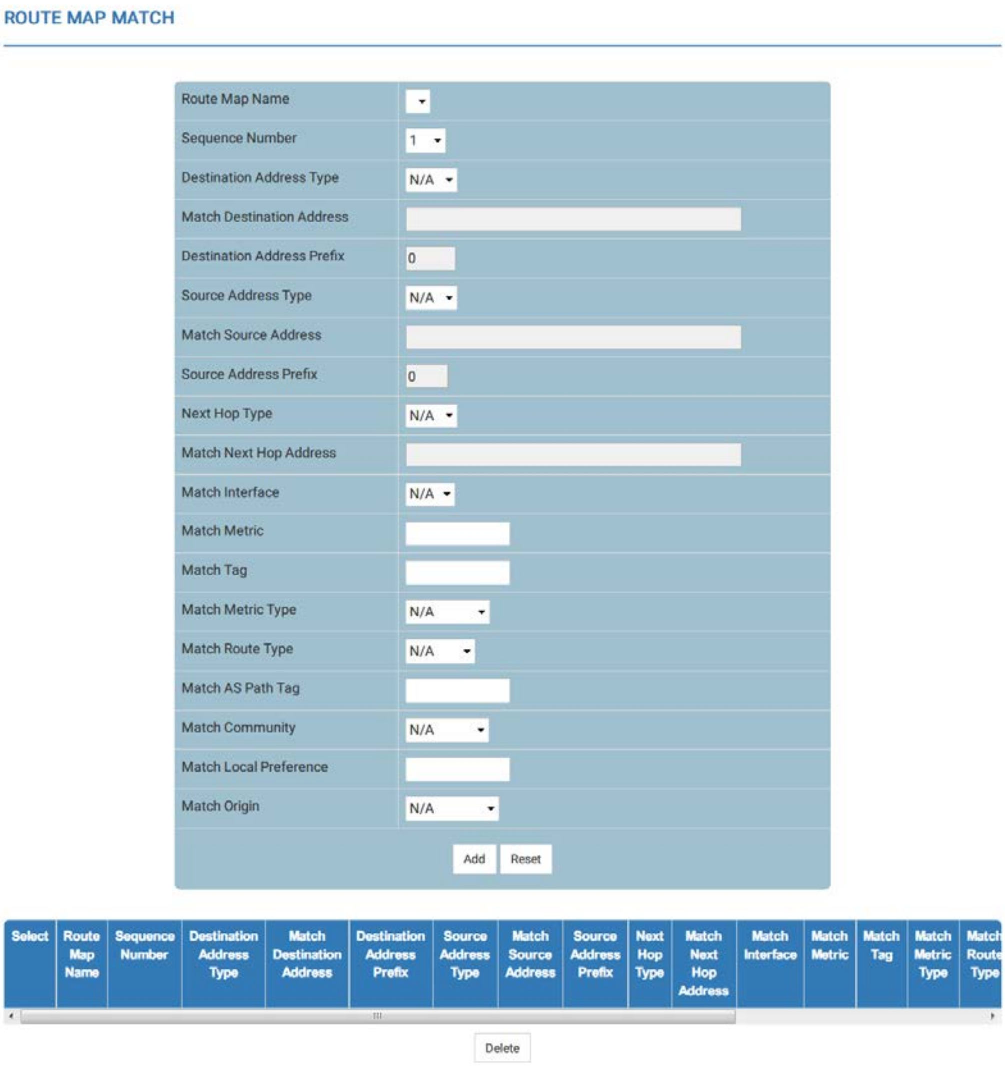
* Permit - Permits the route entry matching the match entry rules

* Deny - Denies the route entry matching the match entry rules

By default, Permit is selected.

> Once an instance of this object is created, its value cannot be changed.

5.6.2 Route Map Match



ROUTE MAP MATCH

Route Map Name	
Sequence Number	1
Destination Address Type	N/A
Match Destination Address	
Destination Address Prefix	0
Source Address Type	N/A
Match Source Address	
Source Address Prefix	0
Next Hop Type	N/A
Match Next Hop Address	
Match Interface	N/A
Match Metric	
Match Tag	
Match Metric Type	N/A
Match Route Type	N/A
Match AS Path Tag	
Match Community	N/A
Match Local Preference	
Match Origin	N/A

Select	Route Map Name	Sequence Number	Destination Address Type	Match Destination Address	Destination Address Prefix	Source Address Type	Match Source Address	Source Address Prefix	Next Hop Type	Match Next Hop Address	Match Interface	Match Metric	Match Tag	Match Metric Type	Match Route Type

Fig: Route Map Match

The *Route Map Match* link opens the **Route Map Match** Page.

The Route Map Match page allows the user to match the Route Maps.

The table below lists the fields present in this page.

Route Map Name - Select the specified route-map in the list of route-maps. The value is of string type with maximum length of 20 characters.

Sequence Number - Select the position of a new route map in the list of route maps already configured with the same name. The value is of string type with maximum length of 10 characters.

Destination Address Type - Select the address type of the destination network. The list contains:

* IPv4 - Sets the destination network address type as Internet Protocol Version 4.

* IPv6 - Sets the destination network address type as Internet Protocol Version 6.

Please also configure Match Destination Address and Prefix at the same time.

They are a set of Match Destination.

Match Destination Address - Specifies a destination network address, which is matched against the permitted range of addresses.

Destination Address Prefix - Specifies the prefix length, which gives the range of the network addresses.

Source Address Type - Select the address type of the source network. The list contains:

* IPv4 - Sets the source network address type as Internet Protocol Version 4.

* IPv6 - Sets the source network address type as Internet Protocol Version 6.

Please also configure Match Source Address and Prefix at the same time.

They are a set of Match Source.

Match Source Address - Specifies a source network address, which is matched against the permitted range of addresses.

Source Address Prefix - Specifies the prefix length, which gives the range of the network addresses.

Next Hop Type - Select the address type of the Next Hop. The list contains:

* IPv4 - Sets the Next Hop address type as Internet Protocol Version 4.

* IPv6 - Sets the Next Hop address type as Internet Protocol Version 6.

Please also configure Match Next Hop Address.

Match Next Hop Address - Specifies the next hop router address and matches the routes having the specified address.

Match Interface - Identifies the interface index value, which identifies the local interface through which the next hop can be reached.

Match Metric - Enter the metric, which is matched with the metric specified in the route-map. The metric value ranges between 1 and 16777215.

Match Tag - Enter the tag value, which is matched with the tag specified in the route-map.

Match Metric Type - Select the metric type, which is matched with the metric type specified in the route-map. Options are:

* external-type-1 - matches the ospf routes with metric type as external type 1 routes

* external-type-2 - matches the ospf routes with metric type as external type 2 routes

* intra-area - matches the ospf intra area routes

* inter-area - matches the ospf inter area routes.

Match Route Type - Select the route-type, which is matched with the route-type specified in the route-map. Options are:

* Local - Matches the local routes.

* Internal - Matches the routes internal to the autonomous system.

Match AS Path Tag - Enter the AS (Autonomous System) path tag of the route with the existing AS path in BGP. Applies only when redistributing routes into BGP.

The AS path tag ranges between 1 and 214748367.

Match Community - Select the BGP communities attribute to be matched in the route with the specified community. Options are:

* internet - Internet community - Advertise this route to the Internet community; all routers in the network belong to it

* local-as - Local AS community - Send this route to peers in other subautonomous systems within the local confederation. Do not advertise this route to an external system

* no-advt - No advertisement community - All routes received carrying a communities attribute containing this value MUST NOT be advertised to other BGP peers

* no-export - No export community - All routes received carrying a communities attribute containing this value MUST NOT be advertised outside a BGP confederation boundary

* comm-num - Community number

* none - No community - Removes the match community entry from the match entry list

Match Local Preference - Enter preference value for the autonomous system path. The preference is sent to all routers in the local autonomous system only. The Local preference ranges between 1 and 214748367.

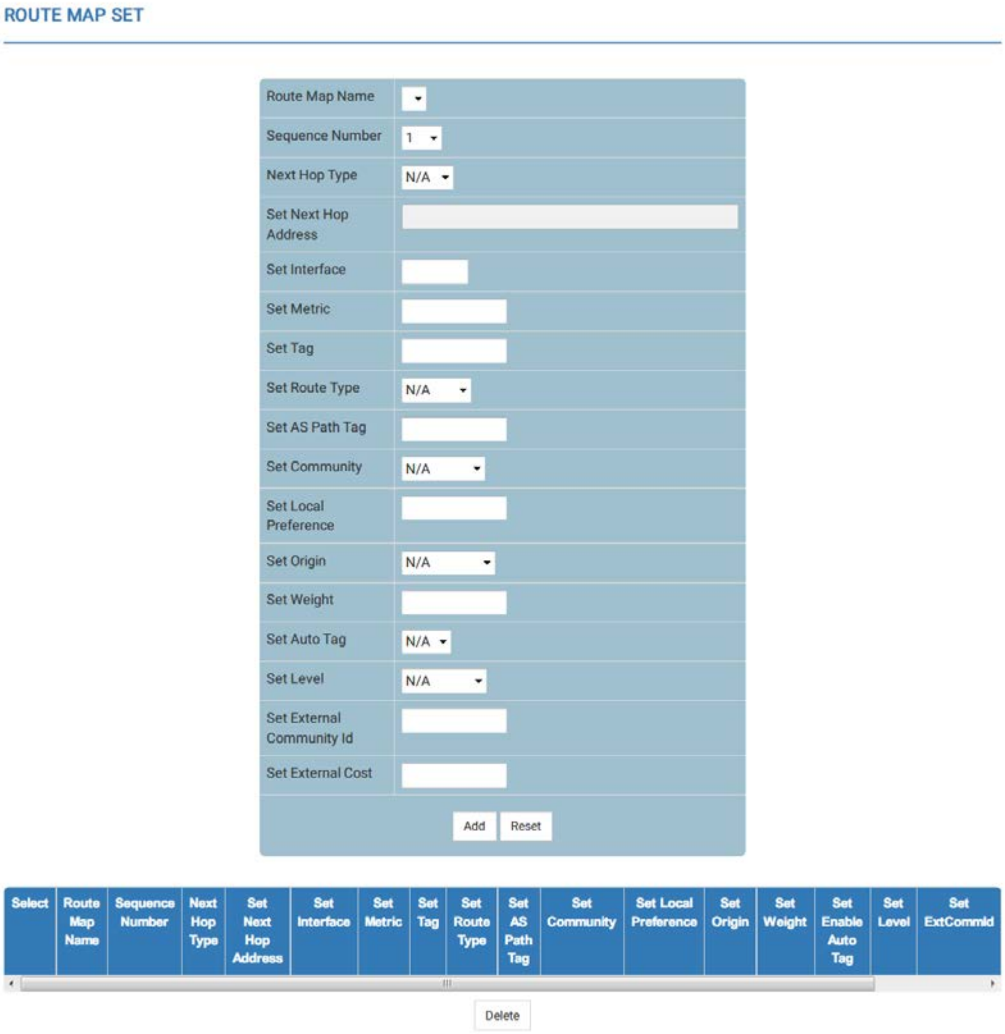
Match Origin - Select the origin of the route in BGP. Options are:

* IGP - Specifies that the route is originated through Interior Gateway Protocol.

* EGP - Specifies that the route is originated through Exterior Gateway Protocol.

* Incomplete - Specifies that the route is originated through unknown heritage.

5.6.3 Route Map Set



ROUTE MAP SET

Route Map Name	
Sequence Number	1
Next Hop Type	N/A
Set Next Hop Address	
Set Interface	
Set Metric	
Set Tag	
Set Route Type	N/A
Set AS Path Tag	
Set Community	N/A
Set Local Preference	
Set Origin	N/A
Set Weight	
Set Auto Tag	N/A
Set Level	N/A
Set External Community Id	
Set External Cost	

Select	Route Map Name	Sequence Number	Next Hop Type	Set Next Hop Address	Set Interface	Set Metric	Set Tag	Set Route Type	Set AS Path Tag	Set Community	Set Local Preference	Set Origin	Set Weight	Set Enable Auto Tag	Set Level	Set ExtCommId

Fig: Route Map Set

The *Route Map Set* link opens the **Route Map Set** Page.

The Route Map Set page allows the user to set the Route Map information.

The table below lists the fields present in this page.

Route Map Name - Select the specified route-map in the list of route-maps.

The length of the name ranges between 1 and 20.

Sequence Number - Select the position of a new route map in the list of route maps already configured with the same name.

This value ranges between 1 and 10.

Next Hop Type - Select the address type of the Next Hop. The list contains:

* IPv4 - Sets the Next Hop address type as Internet Protocol Version 4

* IPv6 - Sets the Next Hop address type as Internet Protocol Version 6.

Set Next Hop Address - Enter the next hop IP address and sets the address for a route- that satisfies the match conditions.

Set Interface - Select the local interface through which the next hop can be reached and sets the interface for a route that satisfies the match conditions.

Set Metric - Enter the primary routing metric.

Set Tag - Enter the tag value of the routing protocol. This value ranges between 1 and 214748367.

Set Route Type - Select the route-type as per RFC 2096 . This is set during the process of policy routing or route redistribution

* local - Sets the connected routes.

* remote - Sets the non-connected routes (static / routing protocol installed routes).

Set AS Path Tag - Enter the tag of a route into an AS path. Applies only when redistributing routes into BGP. This value ranges between 1 and 214748367.

Set Community - Select the BGP communities attribute which is to be set in the route. Options are:

* internet - Internet community - Advertise this route to the Internet community; all routers in the network belong to it

* local-as - Local AS community - Send this route to peers in other subautonomous systems within the local confederation. Do not advertise this route to an external system

* no-advt - No advertisement community - All routes received carrying a communities attribute containing this value MUST NOT be advertised to other BGP peers

* no-export - No export community - All routes received carrying a communities attribute containing this value MUST NOT be advertised outside a BGP confederation boundary

* comm-num - Community number

* none - No community - Removes the match community entry from the match entry list

Set Local Preference - Enter a preference value for the AS path in the route. The preference is sent to all routers in the local AS only. This value ranges between 1 and 214748367.

Set Origin - Select the origin of the route in BGP. Options are:

* igp - Specifies that the route is originated through Interior Gateway Protocol.

* egp - Specifies that the route is originated through Exterior Gateway Protocol.

* incomplete - Specifies that the route is originated through unknown heritage.

Set Weight - Enter the BGP weight for the routing table.. This value ranges between 1 and 0xffff(65535). This is set during the process of policy routing or route redistribution

Set Auto Tag - Select automatic tag generation. This is set during the process of policy routing or route redistribution. Options are:

* 1 - Enables automatic computing of tag table when redistributing routes from BGP into IGP.

* 2 - Disables automatic computing of tag table when redistributing routes from BGP into IGP.

Set Level - Select the level for routes that are advertised into the specified area of the routing domain. This is set during the process of policy routing or route redistribution. Options are:

* level-1 - Imports routes into a Level 1 area.

* level-2 - Imports routes into a Level 2 subdomain.

* level-1-2 - Imports routes into Level 1 and Level 2.

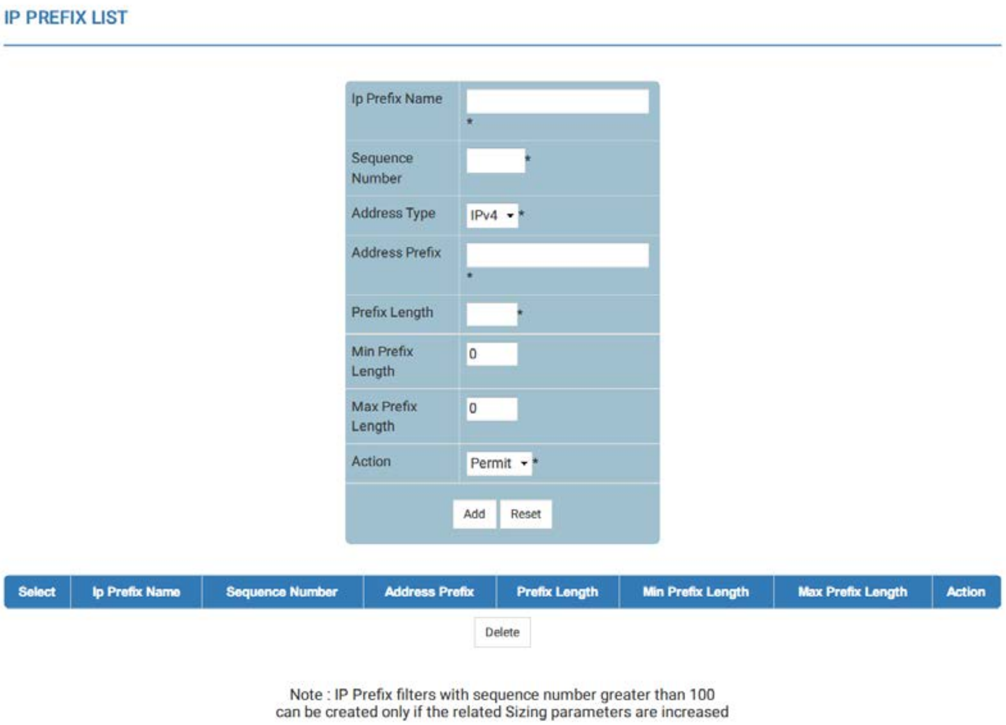
* level-stub-area - Imports routes into an OSPF (Open Shortest Path First) NSSA (not-so-stubby area).

* level_backbone - Imports routes into an OSPF backbone area.

Set External Community Id - Specifies the extended cost community Id attribute whose value is used in determining the BGP best route when external cost is same for the routes. Route with lower cost is preferred. It is a type of the opaque extended community.

Set External Cost - Specifies the extended cost community value that is used to determine the BGP best route.

5.6.4 Ip Prefix List



IP PREFIX LIST

Ip Prefix Name	*
Sequence Number	*
Address Type	IPv4 *
Address Prefix	*
Prefix Length	*
Min Prefix Length	0
Max Prefix Length	0
Action	Permit *

Select	Ip Prefix Name	Sequence Number	Address Prefix	Prefix Length	Min Prefix Length	Max Prefix Length	Action

Note : IP Prefix filters with sequence number greater than 100 can be created only if the related Sizing parameters are increased

Fig: Ip Prefix List

The *Ip Prefix List* link opens the **Ip Prefix List** Page.

The Ip Prefix List page allows the user to create Ip Prefix List.

The table below lists the fields present in this page.

Ip Prefix Name - Enter the specified Ip Prefix name in the list of Ip Prefixes. The length of the name ranges between 1 and 20.

Sequence Number - Enter the position of a new Ip Prefix in the list of Ip Prefixes already configured with the same name. The range for the number is between 1 and 100.

Address Type - Select the address type of the Ip Prefix. The list contains:

* IPv4 - Sets the Ip Prefix address type as Internet Protocol Version 4

* IPv6 - Sets the Ip Prefix address type as Internet Protocol Version 6

Address Prefix - Specifies the prefix, which gives the range of the network addresses.

Prefix Length - Specifies the prefix length, which gives the range of the network addresses.

Min Prefix Length - Minimum prefix length (should be greater than prefix length and less than or equal to max prefix length)

Max Prefix Length - Maximum prefix length (should be greater than prefix length and greater than or equal to min prefix length)

Action Select the access type associated with sequence number in a IP Prefix.

Options are:

* permit - Specify packets to forward

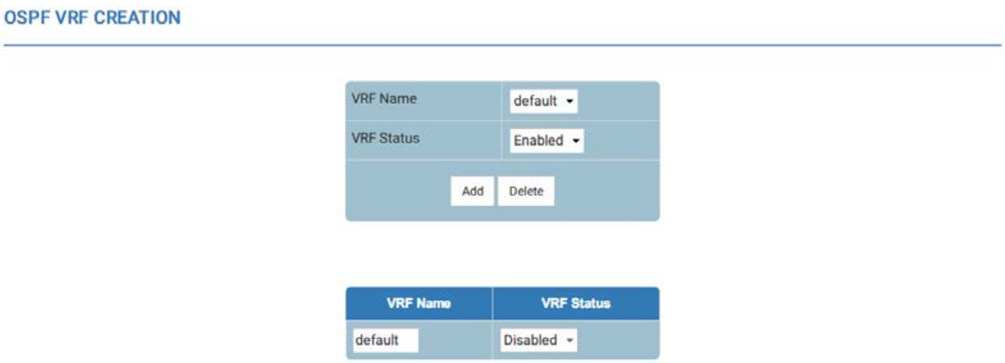
* deny - Specify packets to reject

5.7 OSPF

The *OSPF* link allows you to configure the OSPF related parameters for switch. User can configure OSPF on the following 10 pages.

- OSPF VRF Creation
- Basic Settings
- Area
- Interface
- Virtual Interface
- Neighbor
- RRD Route
- Aggregation
- AsExtAggregation
- GraceRestart

5.7.1OSPF VRF Creation



OSPF VRF CREATION

VRF Name	default
VRF Status	Enabled

VRF Name	VRF Status
default	Disabled

Fig: Ospf VRF Creation

The *OSPF VRF Creation* link opens the **Ospf VRF Creation** Page.

The Ospf VRF Creation page allows the user to configure the virtual context of the OSPF.

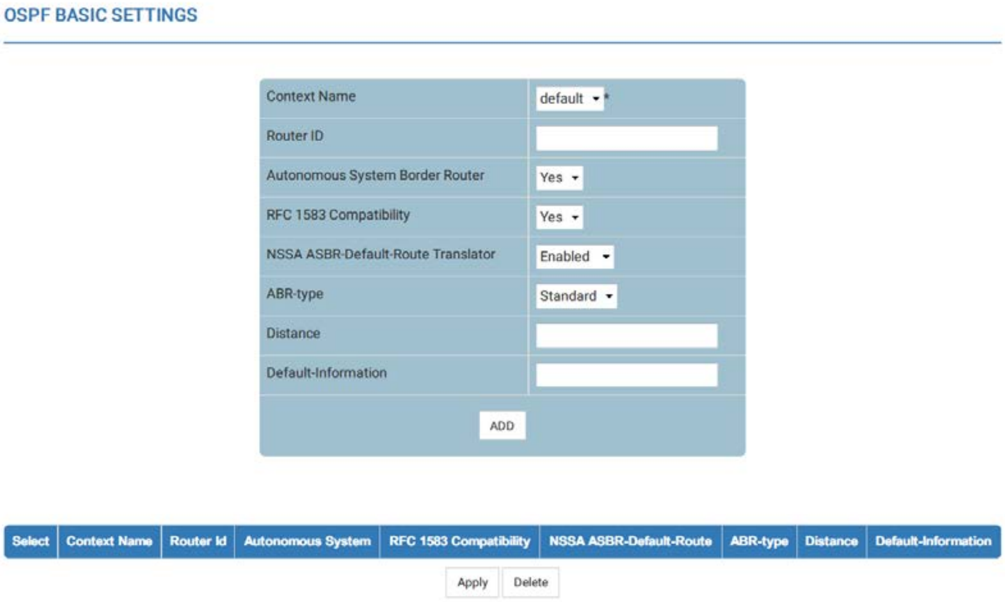
The table below lists the fields present in this page.

VRF Name - Specifies the OSPF virtual context name. This is a string of size 32.

VRF Status - Specifies the admin status of OSPF virtual context. Options are:

* Enabled - OSPFv3 virtual context is enabled.

5.7.2Basic Settings



OSPF BASIC SETTINGS

Context Name	default *
Router ID	
Autonomous System Border Router	Yes
RFC 1583 Compatibility	Yes
NSSA ASBR-Default-Route Translator	Enabled
ABR-type	Standard
Distance	
Default-Information	

Select	Context Name	Router Id	Autonomous System	RFC 1583 Compatibility	NSSA ASBR-Default-Route	ABR-type	Distance	Default-Information

Fig: OSPF Basic Settings

The *Basic Settings* link opens the **OSPF Basic Settings** Page.

The OSPF Basic Settings page allows the user to configure the basic settings of the OSPF.

The table below lists the fields present in this page.

Context Name - Select the OSPF virtual context name.

Router ID - Specifies a 32-bit integer uniquely identifying the router in the AS (Autonomous System).

Autonomous System Border Router - Specifies whether the router is configured as an ASBR (AS Border Router) or not.

The options are:

* Yes - Configures the router as an ASBR.

* No - Does not configure the router as an ASBR.

RFC 1583 Compatibility - Specifies whether the preference rules specified by the RFC 1583 or RFC 2178 to be set. The options are:

* Yes - Sets the preference rules specified by the RFC 1583.

* No - Sets the preference rules specified by the RFC 2178.

The default value is Yes.

NSSA ASBR Default Route Translator - Specifies the P-Bit setting for the default Type-7 LSA (Link State Advertisement) generated by ASBR (which is not ABR (Area Border Router)). The options are:

* Enabled - Sets the P-Bit in the generated Type-7 default LSA.

* Disabled - Clears the P-Bit in the generated default LSA.

The default value is Disabled.

ABR Type - Specifies the types of ABRs supported. The options are:

* Standard - Supports Standard ABR.

* CISCO - Supports CISCO ABR.

* IBM - Supports IBM ABR.

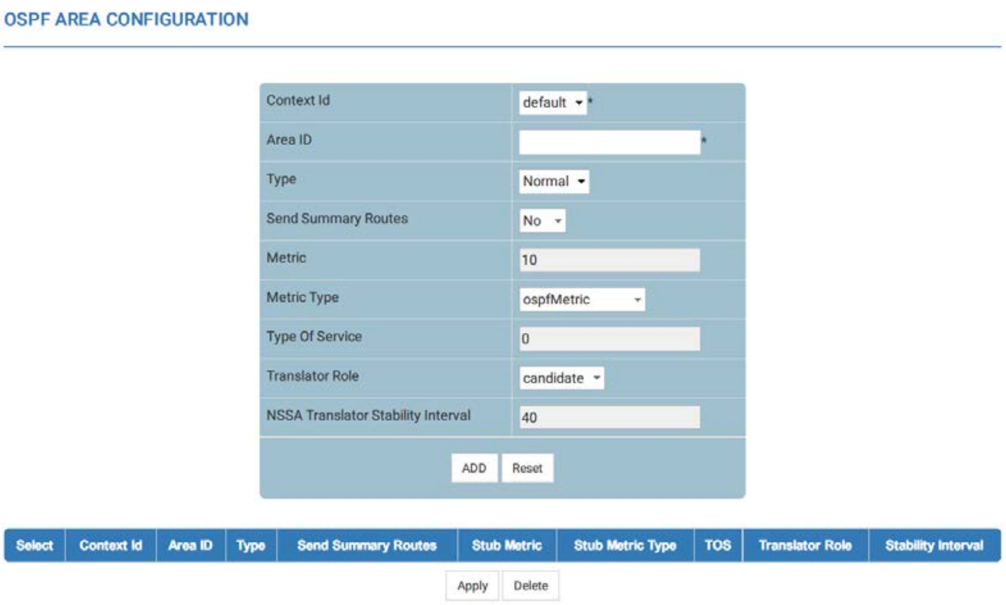
The default value is Standard.

Distance - Specifies administrative distance (Metric to reach destination).

The range for the number is between 1 and 255.

Default-Information - Specifies the metric value applied at generation of a default external route into an OSPF routing domain.

5.7.3Area



OSPF AREA CONFIGURATION

Context Id	default *
Area ID	*
Type	Normal
Send Summary Routes	No
Metric	10
Metric Type	ospfMetric
Type Of Service	0
Translator Role	candidate
NSSA Translator Stability Interval	40

Select	Context Id	Area ID	Type	Send Summary Routes	Stub Metric	Stub Metric Type	TOS	Translator Role	Stability Interval

Fig: OSPF Area Configuration

The *Area* link opens the **OSPF Area Configuration** Page.

The OSPF Area Configuration page allows the user to configure the parameters of the router's attached areas.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Area ID - Specifies a 32-bit integer uniquely identifying an area.

Type - Specifies the required type for an area. The options are:

* Normal - Allows all the external LSAs (Type 5 LSA) to be flooded through the area.

* Stub - Does not allow the external LSA to be flooded into the area.

* NSSA - Allows only limited number of Type 5 external LSA to be translated into Type 7 LSA and flooded into the area.

Send Summary Routers - Specifies the status of send summary routers This field is used to control the import of summary LSAs to the stub areas. This field does not have any impact on other areas.

The options are:

* Yes - Router will summarize and propagate summary LSAs.

* No - Router does not originate or propagate summary LSAs.

The default value is No.

Metric - Specifies the metric value applied at the indicated type of service. This is applicable to stub and NSSA area. This value ranges between 0 and 16777215. The default value is 10.

Metric Type - Specifies the type of metric advertised as a default route. This is applicable to stub and NSSA area. The options are:

* ospfMetric

* comparableCost

* nonComparable

The default value is ospfMetric.

Type of Service - Specifies the type of service associated with the metric. This is applicable to stub and NSSA area. The default value is zero.

Translator Role - Specifies an NSSA border router's ability to perform NSSA translation of Type-7 LSAs to Type-5 LSAs. The options are:

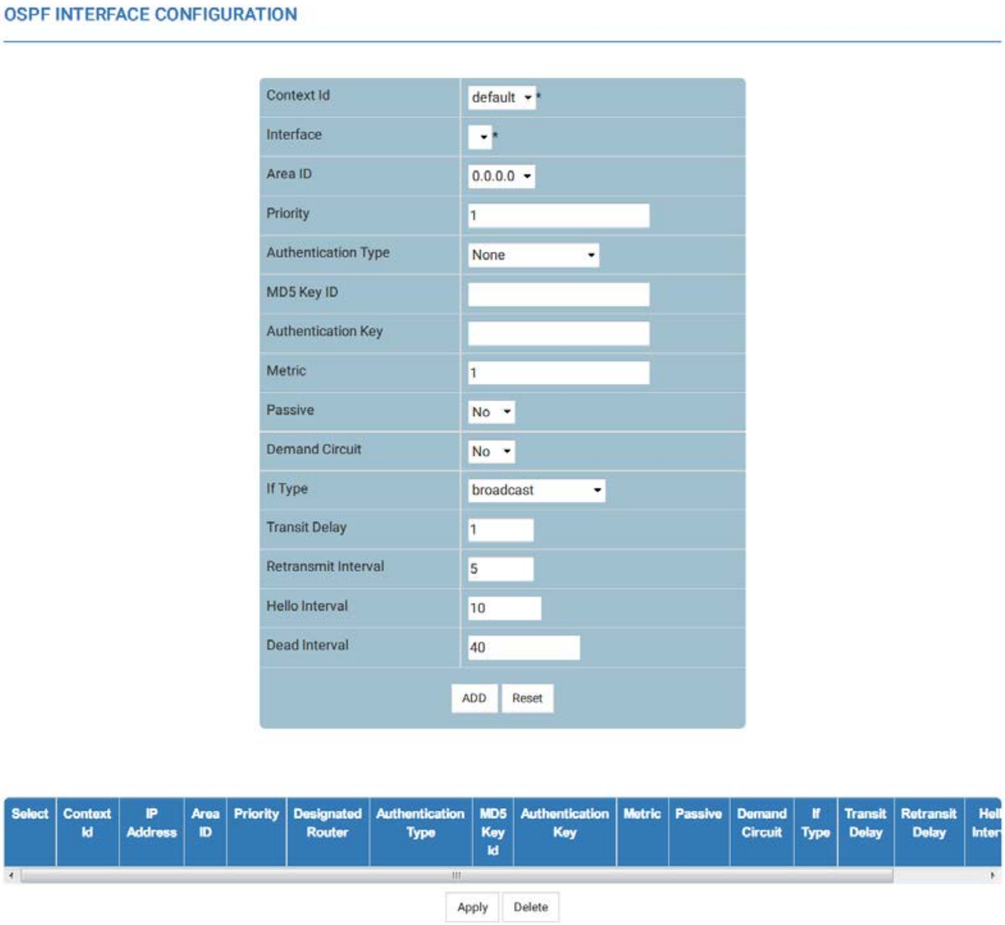
* Always

* Candidate

The default value is Candidate.

NSSA Translator Stability Interval - Specifies the number of seconds after which an elected translator determines its services are no longer required, that it should continue to perform its translation duties. This value ranges between 0 and 2147483647. The default value is 40 seconds.

5.7.4Interface



OSPF INTERFACE CONFIGURATION

Context Id	default *
Interface	*
Area ID	0.0.0.0
Priority	1
Authentication Type	None
MD5 Key ID	
Authentication Key	
Metric	1
Passive	No
Demand Circuit	No
If Type	broadcast
Transit Delay	1
Retransmit Interval	5
Hello Interval	10
Dead Interval	40

Select	Context Id	IP Address	Area ID	Priority	Designated Router	Authentication Type	MD5 Key Id	Authentication Key	Metric	Passive	Demand Circuit	If Type	Transit Delay	Retransit Delay	Hel Inter

Fig: OSPF Interface Configuration

The *Interface* link opens the **OSPF Interface Configuration** Page.

The OSPF Interface Configuration page allows the user to configure the interfaces-related OSPF parameters.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Interface - Specifies the interface index of the port.

Area ID - Specifies the 32-bit integer uniquely identifying the area to which the interface connects.

Priority - Specifies the priority of this interface, which is used in the DR (Designated Router) election algorithm. This value ranges between 0 and 255. The default value is 1.

Authentication

Type - Specifies the type of authentication used on the interface. The options are:

* None - No authentication.

* Simple Password - Simple password type authentication.

* MD5 - Message Digest 5 based authentication.

The default value is None.

MD5 Key ID - Specifies the secret key used to create the message digest appended to the OSPF packet if the authentication type is MD5. This value ranges between 0 and 255.

Authentication Key - Specifies the key required for authentication, if authentication is enabled on this interface.

Metric - Specifies the metric of using the type of service on the interface. The default value is 10.

Passive - Sets the interface as passive or normal. The options are:

* Yes - Sets the interface as passive.

* No - Sets the interface as normal.

The default value is No.

Demand Circuit - Specifies whether Demand OSPF procedures should be performed on this interface.

The options are:

* No

* Yes

The default value is No.

If Type - Specifies the OSPF interface type. The options are

* broadcast

* nbma

* point-to-point

* point-to-multipoint

The default value is broadcast.

Transit Delay - Specifies the number of seconds taken to transmit a link state update packet over the interface. This value ranges between 0 and 3600 seconds. The default value is one second.

Retransmit Interval - Specifies the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. This value ranges between 0 and 3600 seconds. The default value is five seconds.

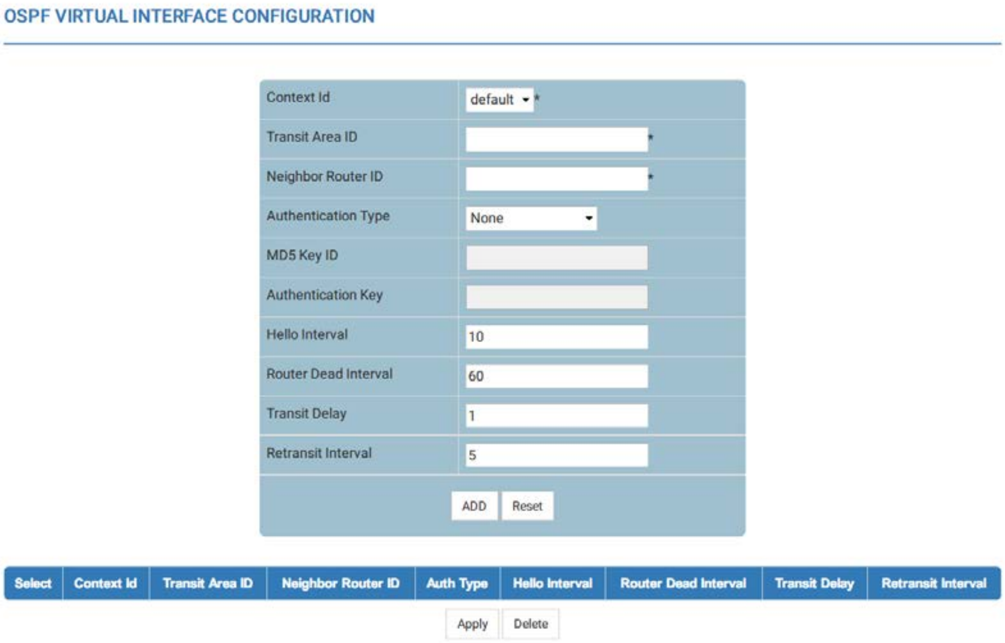
Hello Interval - Specifies the length of time, in seconds, between the Hello packets send on the interface. This value ranges between 1 and 65535 seconds. The default value is 10 seconds.

Dead Interval - Specifies the number of seconds that a router's Hello packets have not been seen before its neighbors declare the router as down. This value ranges between 0 and 2147483647 seconds. The default value is 40 seconds.

IP Address - Indicates the IP Address of the OSPF interface. This is a read-only field.

Designated Router - Specifies the IP Address of the Designated Router. This is a read-only field.

5.7.5Virtual Interface



OSPF VIRTUAL INTERFACE CONFIGURATION

Context Id	default *
Transit Area ID	*
Neighbor Router ID	*
Authentication Type	None
MD5 Key ID	
Authentication Key	
Hello Interval	10
Router Dead Interval	60
Transit Delay	1
Retransit Interval	5

Select	Context Id	Transit Area ID	Neighbor Router ID	Auth Type	Hello Interval	Router Dead Interval	Transit Delay	Retransit Interval

Fig: OSPF Virtual Interface Configuration

The *Virtual Interface* link opens the **OSPF Virtual Interface Configuration** Page.
The OSPF Virtual Interface Configuration page allows the user to configure the parameters related to router's virtual interfaces.

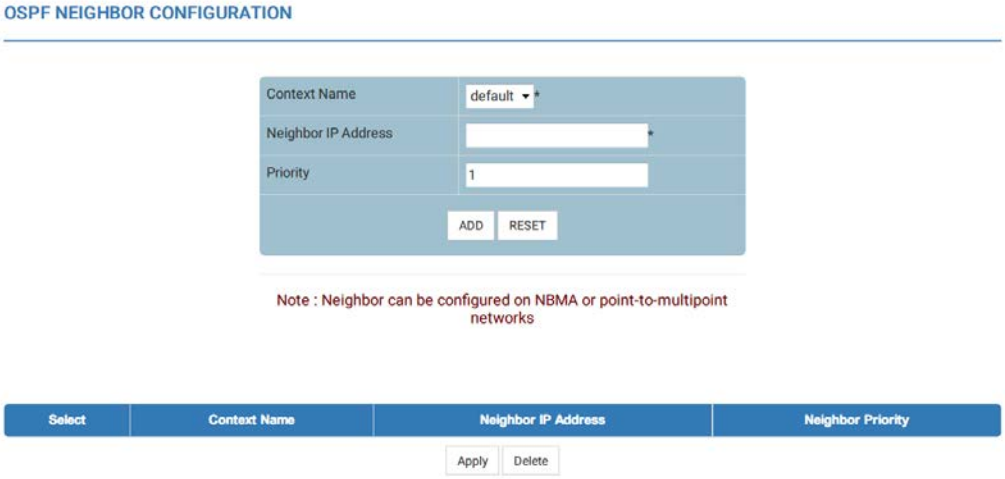
The table below lists the fields present in this page.
Context Id - Select the OSPF virtual context name.
Transit Area ID - Specifies the 32-bit integer uniquely identifying an area, which is traversed by the virtual link.
Neighbor Router ID - Specifies the router ID of the virtual neighbor.
Authentication Type - Specifies the type of authentication used on the interface. The options are:
* None - No authentication.
* Simple Password - Simple password type authentication.
* MD5 - Message Digest 5 based authentication.
MD5 Key ID - Specifies the secret key used to create the message digest appended to the OSPF packet if the authentication type is md5. This value ranges between 1 and 65535.
Authentication Key - Specifies the key required for authentication, if authentication is enabled on this interface.
Hello Interval - Specifies the length of time, in seconds, between the Hello packets send on the interface. This value ranges between 1 and 65535 seconds. The default value is 10 seconds.

Router Dead Interval - Specifies the number of seconds that a router's Hello packets have not been seen before its neighbors declare the router as down. This value ranges between 0 and 2147483647 seconds. The default value is 60 seconds.

Transit Delay - Specifies the number of seconds taken to transmit a link state update packet over the interface. This value ranges between 1 and 3600 seconds. The default value is one second.

Retransmit Interval - Specifies the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. This value ranges between 1 and 3600 seconds. The default value is five seconds.

5.7.6Neighbor



OSPF NEIGHBOR CONFIGURATION

Context Name	default *
Neighbor IP Address	*
Priority	1

Note : Neighbor can be configured on NBMA or point-to-multipoint networks

Select	Context Name	Neighbor IP Address	Neighbor Priority

Fig: OSPF Neighbor Configuration

The *Neighbor* link opens the **OSPF Neighbor Configuration** Page.

The OSPF Neighbor Configuration page allows the user to configure non-virtual neighbor parameters.

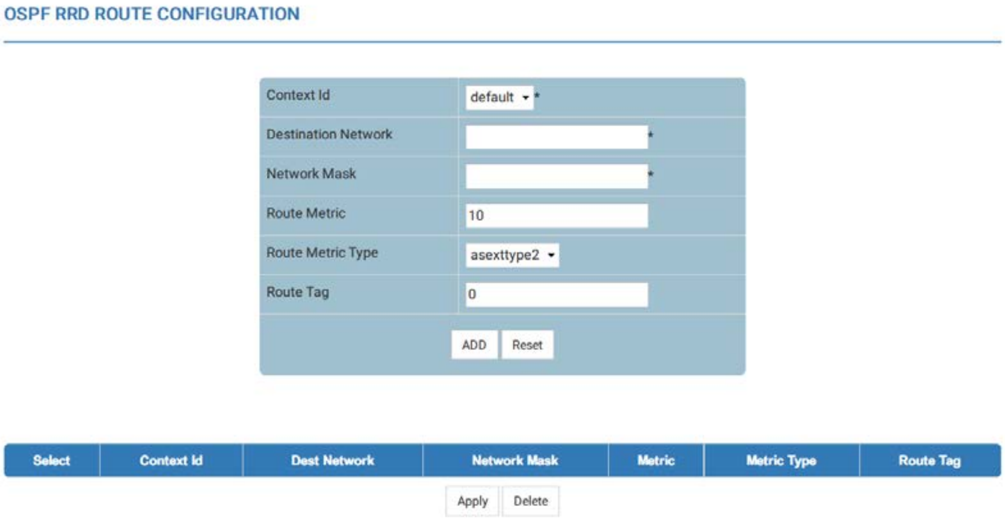
The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Neighbor IP Address - Specifies the IP address used by the neighbor in the IP source address.

Priority - Specifies the priority of the neighbor in the designated router election algorithm. This value ranges between 0 and 255. The default value is one.

5.7.7RRD Route



OSPF RRD ROUTE CONFIGURATION

Context Id	default *
Destination Network	*
Network Mask	*
Route Metric	10
Route Metric Type	asexttype2
Route Tag	0

Select	Context Id	Dest Network	Network Mask	Metric	Metric Type	Route Tag

Fig: OSPF RRD Route Configuration

The *RRD Route* link opens the **OSPF RRD Route Configuration** Page.

The OSPF RRD Route Configuration page allows the user to configure metric cost and route type information to be applied to the routes learnt from the RTM.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Destination Network - Specifies the IP address of the destination route.

Network Mask - Specifies the mask of the destination route.

Route Metric - Specifies the metric value applied to the route before it is advertised into the OSPF domain. This value ranges between 0 and 16777215. The default value is 10.

Route Metric Type - Specifies the metric type applied to the route before it is advertised into the OSPF domain. The options are:

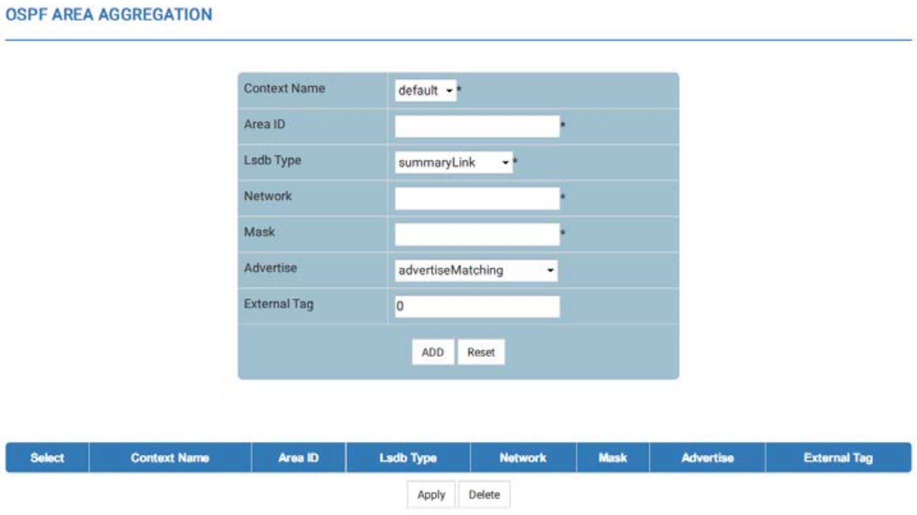
* asexttype1

* asexttype2

The default value is asexttype2.

Route Tag - Specifies the route tag. This value ranges between 0 and 4294967295. The default value is zero.

5.7.8Aggregation



OSPF AREA AGGREGATION

Context Name	default *
Area ID	*
Lsdb Type	summaryLink *
Network	*
Mask	*
Advertise	advertiseMatching
External Tag	0

Select	Context Name	Area ID	Lsdb Type	Network	Mask	Advertise	External Tag

Fig: OSPF Area Aggregation

The *Aggregation* link opens the **OSPF Area Aggregation** Page.

The OSPF Area Aggregation page allows the user to configure External Tag for configured Type-7 address ranges.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Area ID - Specifies the 32-bit integer uniquely identifying the area in which the address aggregate is to be found.

Lsdb Type - Specifies the Lsdb type of the address aggregate. The options are:

* summaryLink

* nssaExternalLink

The default value is summaryLink.

Network - Specifies the IP address of the Net or Subnet indicated by the range.

Mask - Specifies the Subnet Mask that pertains to the Net or Subnet.

Advertise - Specifies whether the subnets are advertised outside the area or not. The options are:

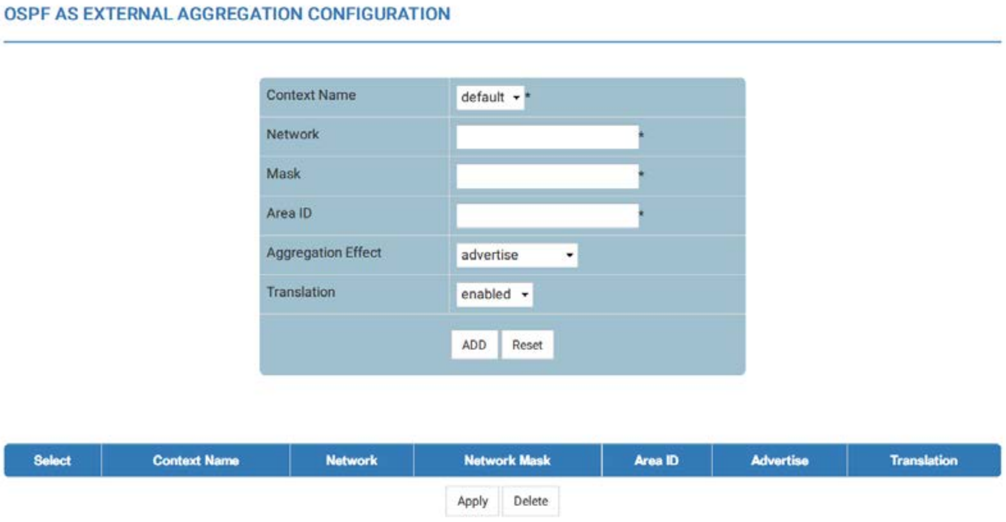
* advertiseMatching - Allows the subnets subsumed by ranges to trigger the advertisement of the indicated aggregate.

* doNotAdvertiseMatching - Does not advertise subnets outside the area.

The default value is advertiseMatching.

External Tag - Specifies a 32-bit filed attached to the external route. This tag is used to communicate information between AS boundary routers. The default value is zero.

5.7.9AsExtAggregation



OSPF AS EXTERNAL AGGREGATION CONFIGURATION

Context Name	default *
Network	*
Mask	*
Area ID	*
Aggregation Effect	advertise
Translation	enabled

Select	Context Name	Network	Network Mask	Area ID	Advertise	Translation

Fig: OSPF AS External Aggregation Configuration

The *AsExtAggregation* link opens the **OSPF AS External Aggregation Configuration** Page. The OSPF AS External Aggregation Configuration page allows the user to configure Type-5 / Type-7 address ranges specifying whether for the configured range, Type-5 / Type-7 LSA will be aggregated or not generated.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Network - Specifies the IP address of the Net.

Mask - Specifies the Subnet mask.

Area ID - Specifies the 32-bit integer uniquely identifying an area.

Aggregation Effect - Specifies whether Type-5/Type-7 will be aggregated or not. The options are:

* advertise - Generates aggregated Type-5 if the associated AreaID is 0.0.0.0. Generates aggrgeated Type-7 in the corresponding NSSA area if Area ID is other than 0.0.0.0.

* doNotAdvertise - Generates aggregated Type-7 in all attached NSSA areas if the associated Area ID is 0.0.0.0. Does not generate aggregated Type-7 in the corresponding NSSA area if the Area ID is other than 0.0.0.0.

* allowAll - Generates aggregated Type-5 for the specified range and generates aggregated Type-7 in all attached NSSA areas, if the associated Area ID is 0.0.0.0. This option is not valid for Area ID other than 0.0.0.0.

* denyAll - Does not generate Type-5 or Type-7 for the specified range. This option is not valid for Area ID other than 0.0.0.0.

The default value is advertise.

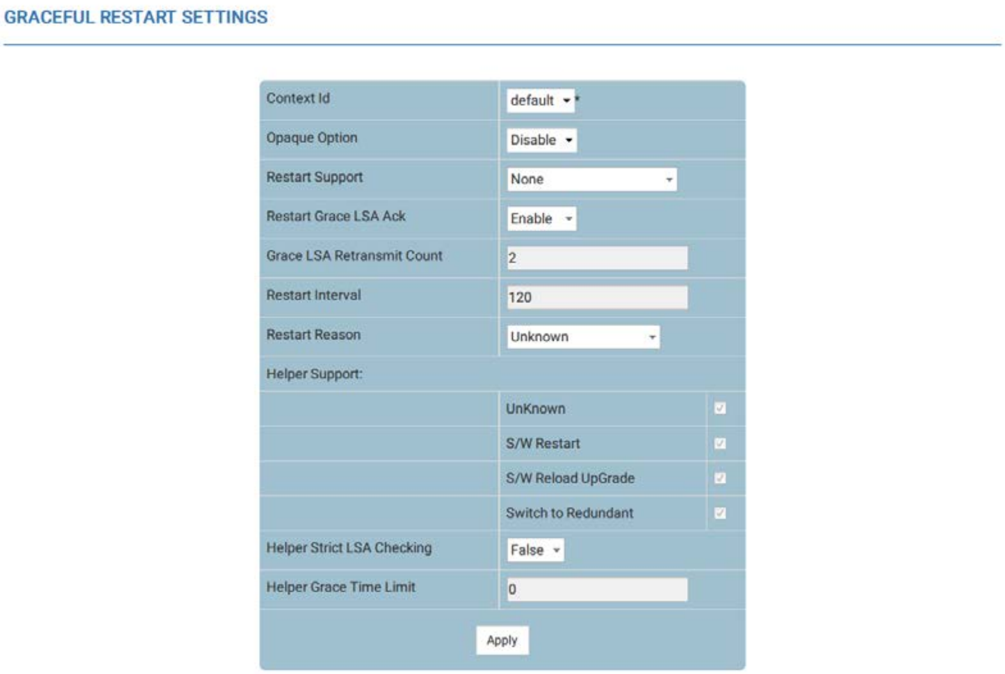
Translation - Enables/disables P Bit setting in the generated Type-7 LSA. The options are:

* enabled - Sets P Bit in the generated Type-7 LSA.

* disabled - Clears the P Bit in the generated Type-7 LSA.

The default value is enabled.

5.7.10 GraceRestart



GRACEFUL RESTART SETTINGS

Context Id	default *
Opaque Option	Disable
Restart Support	None
Restart Grace LSA Ack	Enable
Grace LSA Retransmit Count	2
Restart Interval	120
Restart Reason	Unknown
Helper Support:	
	UnKnown ☑
	S/W Restart ☑
	S/W Reload UpGrade ☑
	Switch to Redundant ☑
Helper Strict LSA Checking	False
Helper Grace Time Limit	0

Fig: Graceful Restart Settings

The *GraceRestart* link opens the **Graceful Restart Settings** Page.
The Graceful Restart Settings page allows the user to configure the
graceful restart settings of the OSPF.

The table below lists the fields present in this page.

Context Id - Select the OSPF virtual context name.

Opaque Option - Enables/disables the opaque-capable option. Options are:

* Enable - Enables the opaque-capable option.

* Disable - Disables the opaque-capable option.

Default option is Disable.

Restart Support - Specifies the router support for the OSPF graceful restart feature. Options are:

* None - No restart support.

* Planned Only - Only planned restarts.

* Planned and Unplanned - Both planned and unplanned restarts.

Default option is None.

Restart Grace LSA Ack - Specifies whether the Grace LSAs sent by the router are expected to be acknowledged by the peers. Options are:

* Enable - Grace LSAs sent by the router are acknowledged by the peers.

* Disable - Grace LSAs sent by the router are not acknowledged.

Default option is Enable.

Grace LSA Retransmit Count - Specifies the number of retransmissions for unacknowledged Grace LSAs. This value ranges between 0 and 180. Default value is 2.

Restart Interval - Configures the OSPF graceful restart timeout interval. This value ranges between 1 and 1800. Default value is 120.

Restart Reason - Specifies the router restart reason code of the OSPF graceful restart feature. Options are:

* UnKnown - System restarts due to unplanned events (such as restarting after a crash).

* S/W Restart - System restarts due to software restart.

* S/W Reload UpGrade - System restarts due to reloading / upgrading of software.

* Switch to Redundant - System restarts due to switchover to a switchover to a redundant support processor.

Default option is Unknown.

Helper Support: - Specifies the router helper support for the OSPF graceful restart feature. Options are:

* UnKnown - Helper support for restarting of system due to unplanned events (such as restarting after a crash).

* S/W Restart - Helper support for restarting of system due to restart of software.

* S/W Reload UpGrade - Helper support for restarting of system due to reload or upgrade of software.

* Switch to Redundant - Helper support for restarting of system due to switchover to a redundant support processor.

By default, all the options are set.

Helper Strict LSA Checking - Indicates whether strict LSA checking is enabled for the graceful restart. Options are:

* True - Strict LSA checking is enabled for the graceful restart.

* False - Strict LSA checking is disabled for the graceful restart.

Default option is False.

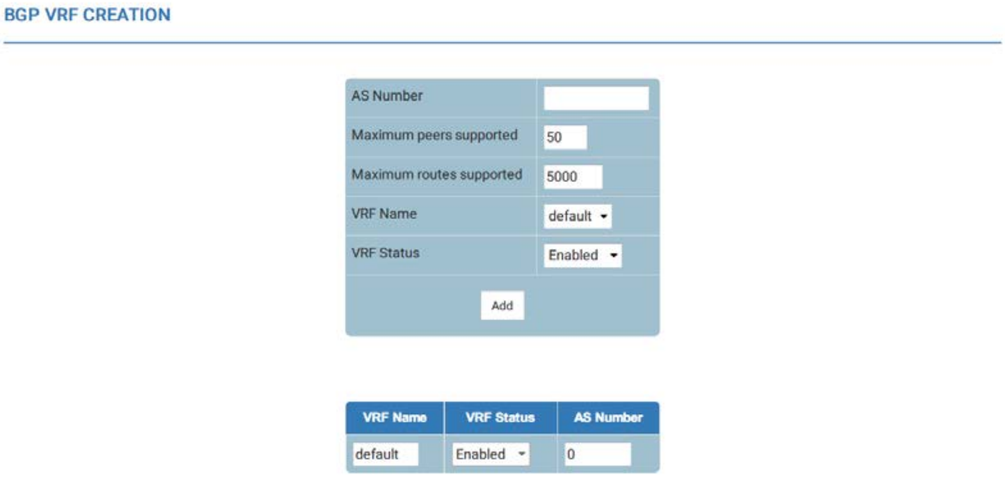
Helper Grace Time Limit - Specifies the OSPF graceful restart interval limit, in seconds, in the helper side. This value ranges between 0 and 1800 seconds. Default value is 0 seconds.

5.8 BGP

The *BGP* link allows you to configure the BGP related parameters for switch. User can configure BGP on the following 18 pages.

- Bgp Context
- Basic Setting
- BGP Scalars
- Neighbors
- Multi-Exit Discriminators
- Local Preferences
- Filters
- Route Aggregation
- Timers
- GR Settings
- TCP-AO Authentication
- Peer-Group
- Peer-Group (Cont..)
- Peer Addition with PeerGroup
- Clear Bgp
- Route Map
- Peer Orf Config
- Orf Filters

5.8.1 BGP Context



BGP VRF CREATION

AS Number	
Maximum peers supported	50
Maximum routes supported	5000
VRF Name	default
VRF Status	Enabled

VRF Name	VRF Status	AS Number
default	Enabled	0

Fig: BGP VRF Creation

The *Bgp Context* link opens the **BGP VRF Creation** Page.

The BGP VRF Creation page allows the user to configure the basic settings of the BGP for the specified VRF instance.

The table below lists the fields present in this page.

AS Number - Enter the local AS number. This value ranges between 1 and 65535. By default the AS number is 0.

> This field can be configured only if the state of the BGP system is set as Disabled in the Basic Settings page.

Maximum peers supported - Enter the maximum number of peers supported in the BGP system. This value ranges between 1 and 50. By default, the value of maximum peers supported is set as 50.

Maximum routes supported - Enter the maximum number of routes supported in the BGP system. This value ranges between 1 and 5000. By default the maximum routes supported is set as 5000.

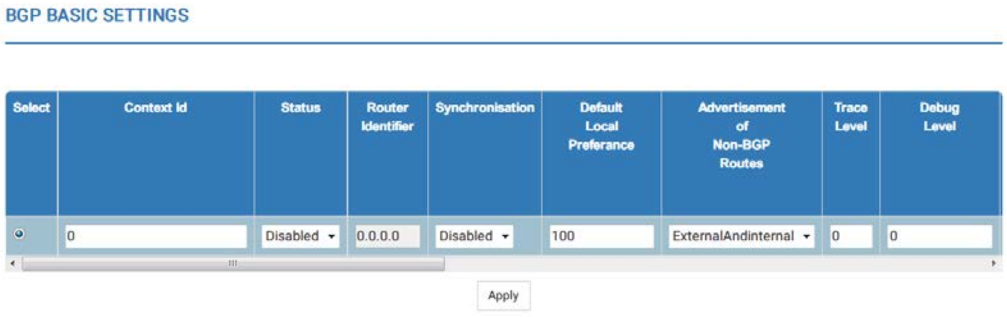
VRF Name - Select the VRF name to configure AS number to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

VRF Status - Select the status of VRF instance in the BGP system.

* Enabled - Enables the created VRF in the BGP system

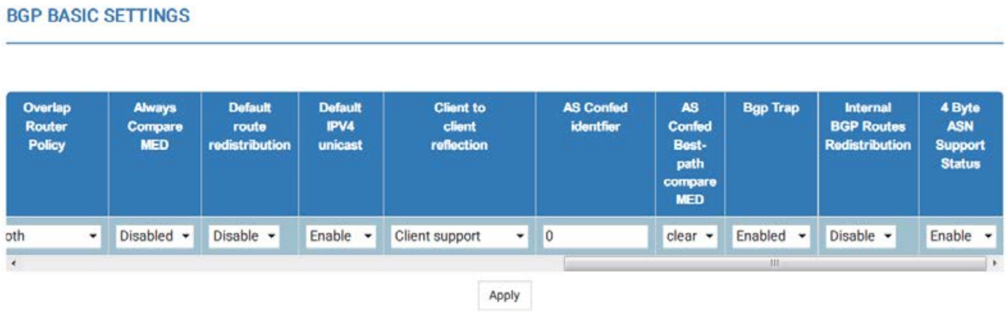
* Disabled - Disables the created VRF in the BGP system

5.8.2 Basic Setting



BGP BASIC SETTINGS

Select	Context Id	Status	Router Identifier	Synchronisation	Default Local Preferance	Advertisement of Non-BGP Routes	Trace Level	Debug Level
●	0	Disabled	0.0.0.0	Disabled	100	ExternalAndinternal	0	0



BGP BASIC SETTINGS

Overlap Router Policy	Always Compare MED	Default route redistribution	Default IPV4 unicast	Client to client reflection	AS Confed identfier	AS Confed Best-path compare MED	Bgp Trap	Internal BGP Routes Redistribution	4 Byte ASN Support Status
oth	Disabled	Disable	Enable	Client support	0	clear	Enabled	Disable	Enable

Fig: BGP Basic Settings

The *Basic Setting* link opens the **BGP Basic Settings** Page.

The BGP Basic Settings page allows the user to configure the basic parameters of the BGP in the system.

The table below lists the fields present in this page.

Select - Select the context id for which the configurations need to be reapplied.

Context Id - Specifies the unique index value that identifies the virtual router for which the configurations need to be applied. This value ranges between 0 and 65535.

Status - Select the status of BGP in the system. By default BGP status is set as Disabled. The list contains:

* Enabled - Enables the BGP system.

* Disabled - Disables the BGP system.

> The BGP system can be enabled only if the local AS number is configured for the context.

Router Identification - Enter the BGP identifier of the local system. This router-id is advertised to other peers and identifies the BGP speaker uniquely.

If loopback interface exists, the router ID is set to the highest address for loopback interface otherwise it is set to the highest IP configured on the IP interfaces

* This field can be configured explicitly only if the BGP speaker is administratively active. The explicitly configured value will be preserved even after the restart of the BGP.

* Peering sessions will be reset if the BGP identifier is changed.

* This field can be set only if the local AS number is configured.

> This field must be configured as 0.0.0.0 to restore the default value for BGP identifier.

Synchronization - Select the synchronization status within an AS. By default Synchronization value is set as Disabled. The list contains:

* Enabled - Enables the synchronization between Border

Gateway Protocol (BGP) and Interior Gateway Protocol (IGP)

This allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems

* Disabled - Disables the synchronization between BGP and IGP.

Default Local Preference - Enter the default local preference value that is to be sent in updates to internal peers. The preference is sent to all routers and access servers in the local Autonomous System .This value ranges between 0 and 2147483647. By default the Default Local Preference value is set to 100.

> This object can be set only if the local AS number is configured.

Advertisement of Non-BGP routes - Select the peer type to which non-BGP routes must be sent. By default the peer type to which non-BGP routes are sent is set as ExternalAndinternal. The list contains:

* External - Sends non-BGP routes only to external peers.

* ExternalAndinternal - Sends non-BGP routes to both external and internal peers.

> This object can be set only if the local AS number is configured.

Trace Level - Enables the traces in BGP module. This value ranges between 0 and 16. This value represents the tracing levels as follows:

* 0 - All Failures

* 1 - All Resource Allocation Failures

* 2 - Init and Shutdown Trace

* 3 - Management Trace

* 4 - Control Path Trace

* 5 - Data Path Trace

* 6 - Peer Connection Trace

* 7 - Update Message Trace

* 8 - FDB Update Trace

* 9 - Keep-Alive Trace

* 10 - All Transmission Trace

* 11 - All Reception Trace

* 12 - Dampening Trace

* 13 - Events Trace

* 14 - High level Packet Dump

* 15 - Low level packet Dump

* 16 - Hex Dump

> Trace Level can be set only if the local AS number is configured.

Debug Level - Enables the debug dynamically in BGP module. This value ranges between 0 and 4294967295. This is a four byte integer value specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debug.

> Debug Level can be set only if the local AS number is configured.

Overlap Policy - Select to set the overlap Policy which configures the BGP speaker's policy for handling the overlapping routes. When an overlapping route is received, depending upon the configured policy either the less-specific routes or more-specific routes or both routes are installed in the RIB tree. By default Overlap Policy value is set as both. This list contains:

* More-Specific - Installs more specific routes to the RIB tree

* Less Specific - Installs more specific routes to the RIB tree

* Both - Installs both more specific and less specific routes to the RIB tree

Overlap Policy can be set only if Local AS number is created and Global Admin Status is down

Always Compare MED - Select the status of comparison of Multi Exit Discriminator (MED) for routes received from different autonomous system. MED is one of the parameters considered for selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. By default Always MED value is set as disable. The list contains:

* Enabled - Enables the comparison of MED for routes received from different autonomous system, This implies that MED is compared irrespective of the autonomous system from which the routes are received.

* Disabled - If set to enable, irrespective of the autonomous system from which the routes are received, MED comparison will be done. Disables the comparison of MED for routes received from different autonomous system. This implies that MED is compared only between routes received from the same autonomous system.

> Always compare MED can be set only if the Local AS number is configured.

Default route redistribution - Select the redistribution and advertisement status of the default route (0.0.0.0/0). By default, the default routes are not redistributed into BGP. The list contains:

* Enable - Enables redistribution and advertisement of default route to BGP Peers. The default route advertisement is possible only if the default route is present in the IP FDB or it is received from any peers

* Disable - Disables redistribution and advertisement of the default route.

Default route redistribution can be set only if the Local AS number is configured

Default IPv4 unicast - Select the status of default routing to IPv4-unicast. The default value is set as enable. The list contains:

* Enable - Enables the negotiation of MP IPv4 Unicast Address Family Capability for that peer, if a neighbor is created.

* Disable - Disables default routing to IPv4 unicast which implies that if a neighbor is created, IPv4 unicast capability will not be negotiated unless IPv4 unicast capability is explicitly configured for that neighbor.

> This affects the negotiation of the MP IPv4 Unicast Address Family Capability for the peers newly created and will not affect the MP IPV4 Unicast negotiation status of the already existing peer

> This field can be set only if the Local AS number is configured

Client to client reflection - Select the desired support of the Route Reflector in the cluster. By default, the Client to client reflection value is set as client support.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. If the clients are fully meshed, route reflection is not required

The list contains:

* None - Sets Route Reflector support in the cluster as none.

This is a read field when set as none

* Client support - Sets Route Reflector support in the cluster as client support.

* Non-client Support - Sets Route Reflector support in the cluster as Non-client support

> This can be set only if BGP Global Admin Status is set to down and Local AS is configured

AS confed Identifier - Enter the Local Confederation Identification number of the AS confederation. This value ranges between 0 and 4294967295. By Default confed identifier is set to zero.

> AS confed Identifier can be set only if the Local AS number is configured. When confed id is set to a non-zero value, this value must be reset to zero before reconfiguring confed id

AS Confed Best-path compare MED - Set the MED comparison status among paths learned from confederation peers. By default compare MED is set as clear. The list contains:

* set - Enables MED comparison among paths learnt from confederation peers. The comparison between MEDs is only made if there are no external autonomous systems in the path. If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made

* clear - Disables MED comparison among paths learnt from confed peers and prevent the software from considering the MED attribute in comparing paths.

Bgp Trap - Select the trap status to be set for BGP. This status is used to control the sending of BGP notification messages to SNMP manager. The BGP notification messages are sent when any error is detected in input BGP messages received from peer or in the BGP state event machine. These notification messages are used to close an active session and to provide information about the closure of the session. By default, the trap status is set as Enabled. The list contains:

* Enabled - Enables the trap notification for the BGP system

* Disabled - Disables the trap notification for the BGP system

Internal BGP Routes Redistribution - Select the status of the IBGP routes redistribution to other IGP protocols. By default Internal BGP route redistribution is set as Disabled. The list contains:

* Enabled - Enables IBGP routes to be redistributed to other IGP protocols.

* Disabled - Disables IBGP routes to be redistributed to other IGP protocols.

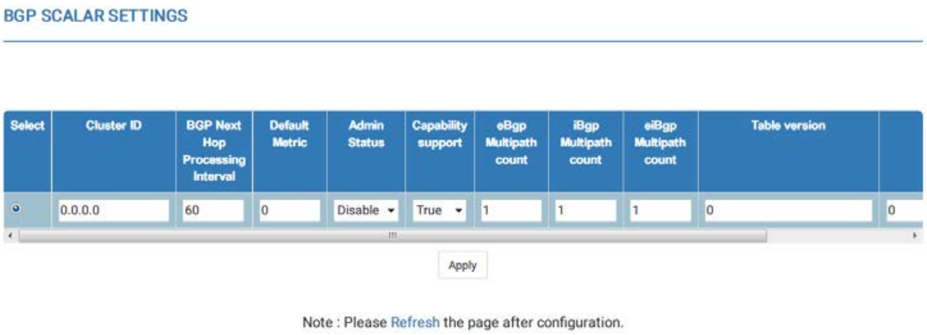
4 Byte ASN Support Status - Select the status of the 4 Byte ASN support in BGP Speaker. By default 4 Byte ASN support is set as Enabled. The list contains:

* Enabled - Enables 4 Byte ASN Support.

* Disabled - Disables 4 Byte ASN Support.

> This can be set only if BGP Global Admin Status is set to down

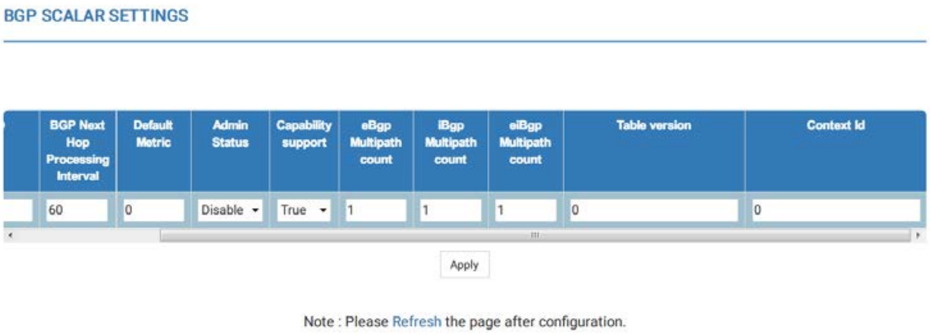
5.8.3 BGP Scalars



BGP SCALAR SETTINGS

Select	Cluster ID	BGP Next Hop Processing Interval	Default Metric	Admin Status	Capability support	eBgp Multipath count	iBgp Multipath count	eiBgp Multipath count	Table version	
●	0.0.0.0	60	0	Disable	True	1	1	1	0	0

Note : Please Refresh the page after configuration.



BGP SCALAR SETTINGS

	BGP Next Hop Processing Interval	Default Metric	Admin Status	Capability support	eBgp Multipath count	iBgp Multipath count	eiBgp Multipath count	Table version	Context Id
	60	0	Disable	True	1	1	1	0	0

Note : Please Refresh the page after configuration.

Fig: BGP Scalar Settings

The *BGP Scalars* link opens the **BGP Scalar Settings** Page.
The BGP Scalar Settings page allows the user to configure the BGP Scalar settings for a given Layer 3 interface.

* This page can be configured only when the BGP status is enabled.
To enable BGP, click Layer-3 > BGP > Basic Settings to access the BGP Basic settings page and set BGP as enabled.

The table below lists the fields present in this page.
Select - Select the Cluster ID for which the configurations needs to be modified
Cluster ID - Enter the cluster-ID of the Router Reflector of the BGP cluster which has more than one route reflector. By default, when the BGP speaker acts as Route Reflector, the BGP Identifier is used as the cluster id.
In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

BGP Next Hop Processing Interval - Enter the interval at which next hops are monitored for reachability. This value ranges between 1 and 120. By default, the BGP next hop processing interval is set as 60.

Default Metric - Enter the default metric value for the IGP routes and static route.

If configured to 0, the metric received from the IGP route will be used. If configured to other value, the MED value of the redistributed routes takes this value. This value has no effect on the Direct routes. This value ranges between 0 and 2147483647.

By default the Default Metric value is set as 0.

Admin Status - Select the admin status of BGP RouteFlap Dampening. By default the admin status is set as Enable. The list contains:

* Enable - Enables BGP RouteFlap Dampening in the system.

* Disable - Disables BGP RouteFlap Dampening in the system.

Capability Support - Select the Capability Advertisement Support status. By default the Capability Support is set as True. The list contains:

* True - Enables Capability Advertisement Support.

* False - Disables Capability Advertisement Support.

When Capability Support is changed, the admin status of BGP RouteFlap Dampening will be enabled.

eBgp Multipath count - Enter the maximum number of external BGP multipath routes to be added per destination network in Routing table. When this object takes the value 1, then only best route is added to Forwarding table.

This value ranges between 1 and 64. By default the eBgp Multipath count value is set as 1.

> This configuration will have effect only after hard/soft reset.

iBgp Multipath count - Enter the maximum number of internal BGP multipath routes to be added per destination network in Routing table. When this object takes the value 1, then only best route is added to Forwarding table.

This value ranges between 1 and 64. By default the iBgp Multipath count value is set as 1.

> This configuration will have effect only after hard/soft reset.

eiBgp Multipath count - Enter the maximum number of external plus internal BGP multipath routes (with same AS PATH) to be added per destination network in Routing table.

When this object takes the value 1, then only best route is added to Forwarding table.

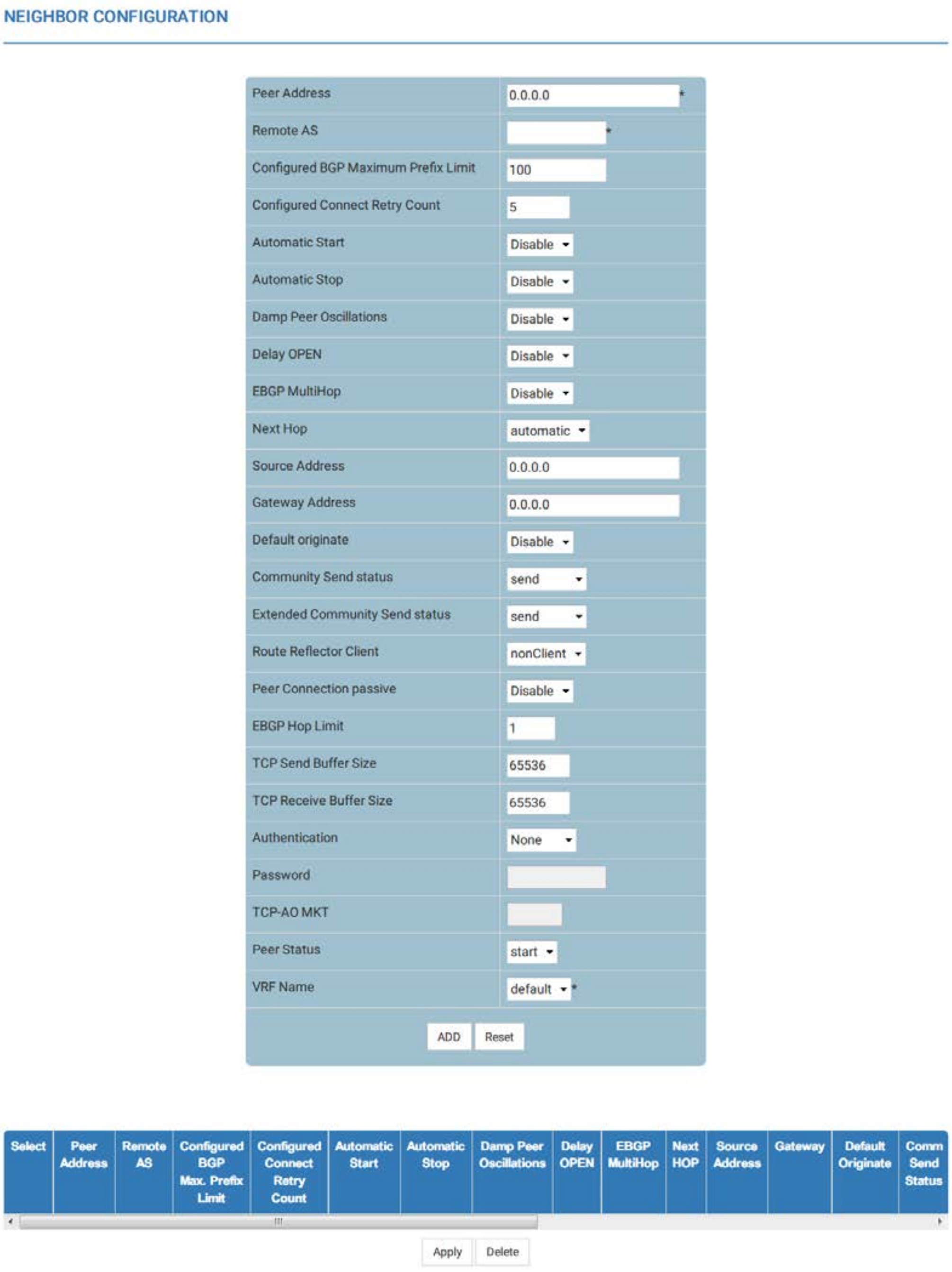
This value ranges between 1 and 64. By default the eiBgp Multipath count value is set as 1.

> This configuration will have effect only after hard/soft reset.

Table version - Displays the Table version which is the total number of valid routes learnt in the system. This is an integer value which increments by 1 whenever a valid route is learnt.

Context Id - Enter the unique index value that identifies the virtual router in which the configuration is done. This value ranges between 0 and 65535.

5.8.4 Neighbors



NEIGHBOR CONFIGURATION

Peer Address	0.0.0.0 *
Remote AS	*
Configured BGP Maximum Prefix Limit	100
Configured Connect Retry Count	5
Automatic Start	Disable
Automatic Stop	Disable
Damp Peer Oscillations	Disable
Delay OPEN	Disable
EBGP MultiHop	Disable
Next Hop	automatic
Source Address	0.0.0.0
Gateway Address	0.0.0.0
Default originate	Disable
Community Send status	send
Extended Community Send status	send
Route Reflector Client	nonClient
Peer Connection passive	Disable
EBGP Hop Limit	1
TCP Send Buffer Size	65536
TCP Receive Buffer Size	65536
Authentication	None
Password	
TCP-AO MKT	
Peer Status	start
VRF Name	default *

Select	Peer Address	Remote AS	Configured BGP Max. Prefix Limit	Configured Connect Retry Count	Automatic Start	Automatic Stop	Damp Peer Oscillations	Delay OPEN	EBGP MultiHop	Next HOP	Source Address	Gateway	Default Originate	Comm Send Status

Fig: Neighbor Configuration

The *Neighbors* link opens the **Neighbor Configuration** Page.

The Neighbor Configuration page allows the user to configure the BGP peer related configurations.

The table below lists the fields present in this page.

Select - Select the neighbor for which the configurations need to be reapplied or deleted.

Peer Address - Enter the remote IP address of the BGP peer.

Remote AS - Enter the remote autonomous system number of the peer. This value ranges between 1 and 65535.

> The admin status of the peer can be made up only if this field is configured for a valid AS number.

Configured BGP Maximum Prefix Limit - Enter the prefix limit value to set upper bound on the number of address prefixes to be accepted by BGP speaker from a neighbor.

The system will not process the prefixes exceeding the upper limit. This value ranges between 1 and 5000. By default, the configured BGP Maximum Prefix Limit value is set as 100.

The default value is calculated based on the following formula:

Maximum number of routes in the routing table / Maximum number of peers supported by BGP.

Configured Connect Retry Count - Enter the retry count to specify the maximum number of times a BGP peer should try for issuing a TCP-Connect with its neighboring peers. This value ranges between 1 and 50. Default value is set as 5.

Automatic Start - Select the automatic start status for the BGP session with the associated peer. By default, the automatic start status is set as Disable. The list contains:

* Disable - The BGP session with the peer should be initiated by manually starting the peer status.

* Enable - The peer session can be automatically started from the idle state after peer idle hold time once the BGP peer session is brought down either by the following

* Automatic stop feature

* Reception of invalid BGP message

The automatic start will not occur, if the IdleHold timer value of the peer exceeds its maximum threshold value.

Automatic Stop - Select the automatic stop status for the BGP connection with the associated peer. By default, the automatic stop status is set as Disable. The list contains:

* Disable - The BGP connection with the associated peer will not be stopped automatically, as the connect retry count will be set as 0.

* Enable - The BGP connection with the associated peer is automatically stopped after the BGP peer attains configured maximum number of TCP connect retry count value. The allocated resources are released and the peer remains in idle state. The peer session initiation is once again started based on the automatic start status, peer idle hold timer and damp peer oscillation status.

Damp Peer Oscillations - Select the damp peer oscillation status that controls the usage of additional logic to damp peer oscillations in states other than established. By default, the damp peer oscillation is set as Disable. The list contains:

* Disable - BGP connection does not use any logic to damp the oscillations of BGP peers.

* Enable - BGP connection uses additional logic to damp the oscillations of BGP peers during a series of automatic start and stop operations in the IDLE state. For each successive damp oscillations, the current idle hold timer value will be increased twice its previous value. It happens through internal logic.

Delay OPEN - Select the delay open status that controls the option to apply delay in sending of open messages. The open message is the initial message sent by the BGP peers after establishing a TCP connection to open a BGP session between them. By default, the delay open status is set as Disable. The list contains:

* Disable - Disables the delay option for sending open messages , which implies that open messages are sent to the remote BGP peer without any delay.

* Enable - Enables delay in sending open messages to the remote BGP peer for a configured open delay time period. This delay allows the remote peer to send the first open message.

EBGP MultiHop - Select the EBGP Multihop option which enables/disables the BGP4 speaker to establish connections to external peers residing on network that are not directly connected. By default EBGP Multihop is Disable. The list contains:

* Disable - Disables BGP to establish connection with external peers residing on networks that are not directly connected. If EBGP-Multihop is disabled and external BGP peers are indirectly connected, then BGP peer session will not be established.

* Enable - Enables BGP to establish connection with external peers residing on networks that are not directly connected. If external BGP peer are not connected directly, then EBGP-Multihop is enabled to initiate the connection with that external peer

This field is applicable only for the directly connected EBGP peers and not applicable for the internal peers.

Next Hop - Select whether the next hop attribute sent in the update message to the peer, has to be generated automatically or self. This is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet By default, Next Hop is set as automatic. The list contains:

* automatic - Generates the next hop based on the IP address of the destination and the present next hop in the route information.

* self - Sets the sender local address as the next hop attribute.

Source Address - Enter the address to be used as the source address for the TCP session initiated with the peer.

> The configured peer address is set as the source address, if no value is configured for the source address

Gateway Address - Enter the gateway router’s address to be used as nexthop in the routes advertised to the peer.

Default originate - Select the status of the advertisement of the default route to the peer or neighbor for use as a default route. By default, the Default Originate value is set as Disable. The list contains:

* Disable - Disables the advertisement of the default route.

* Enable - Enables the advertisement of the default route.

> This field overrides the global default route configuration and always sends a default route to the peer with self next-hop.

This advertisement occurs irrespective of the presence of default route in FDB.

Community Send status / Comm Send Status - Select the status of the send community attribute to a BGP neighbor. By default the Community Send Status is set as send. The list contains:

* none - Sets Community Send status as none.

* send - Sends community attribute to a BGP neighbor and enables advertisement of community attributes (standard/extended) to peer

* dontSend - Disables advertisement of standard community attributes to peer

Extended Community Send status / Ext Comm Send Status - Select the status of extended community send attribute of the BGP peer. The BGP extended community is used to label BGP routing information for controlling the distribution of the information. By default, the Extended Community Send status is set as send. The list contains:

* none - Sets extended community send status as none

* send - Sends extended community attribute to a BGP neighbor and enables advertisement of extended community attributes to peer

* dontSend - Disables advertisement of extended community attributes to peer

Route Reflector Client / RFL - Select the Route Reflector Client status of the peer. This status is used to define client and non-client peers for implementing route reflection. The route reflection mechanism operates as follows:

* A cluster system acting as route reflector sends a route to all client peers within the cluster, if the route is received from a nonclient peer.

* The cluster system acting as route reflector sends a route to all nonclient peers and all client peers except the originator, if the route is received from a client peer.

By default, the route reflector client status is set as nonClient.

The list contains:

* nonClient - Configures the peer as non client peer, which denotes that the peer is outside the cluster

* Client - Configures the peer as client peer, which denotes that the peer is within the cluster.

> The route reflector client can be set as Client only for the peer within the cluster (for the peer entries having the remote AS same as that of the AS number set for RRD in RRD Basic Settings page).

Peer Connection passive / Peer Passive - Select the BGP peer connection status to control the initiation of session from remote peer or speaker. By default Peer Connection Passive is set as Enable. The list contains:

* Enable - Sets the peer connection as passive. BGP speaker waits for the remote peer to initiate the session with the peer.

* Disable - Sets the peer connection as active. BGP speaker initiates the session with the peer.

EBGP Hop Limit - Enter the maximum hop limit value that is used during connection with external peers. This value does not have any effect on connection with internal peers. This value ranges between 1 and 255. By default EBGP Hop Limit value is set as 1.

> BGP speaker accepts or attempts connection to external peers residing on network that are not directly connected but separated by the configured hop limit value.

TCP Send Buffer Size - Enter the TCP send window buffer size. This value ranges between 4096 and 65536. By default TCP Send Buffer Size value is set as 65536.

TCP Receive Buffer Size - Enter the TCP receive window buffer size. This value ranges between 4096 and 65536. By default TCP Receive Buffer Size value is set as 65536.

Password - Enter the TCP MD5 Authentication Password that has to be sent with all TCP packets originated from the peer. This value is a string with the maximum size as 80.

TCP-AO MKT - Enter the Key-ID to associate a TCP-AO MKT to the BGP peer.

Peer Status - Select the desired state of the BGP peer connection. This is used to manually start or stop a BGP peer connection.

By default, the peer status is set as start. The list contains:

* stop **-** Generates BGP stop event to manually stop the BGP session with the peer. The BGP stop event is automatically generated

* once the automatic stop feature is enabled and

* the peer idle hold time exceeds its maximum threshold value.

* start - Generates BGP start event to manually initiate the BGP session with the peer. The BGP start event is generated only after configured peer idle hold time. The manual start is required for the peers damped using damp peer oscillation feature. The BGP start event is automatically generated after peer idle hold time to start BGP session in idle state when

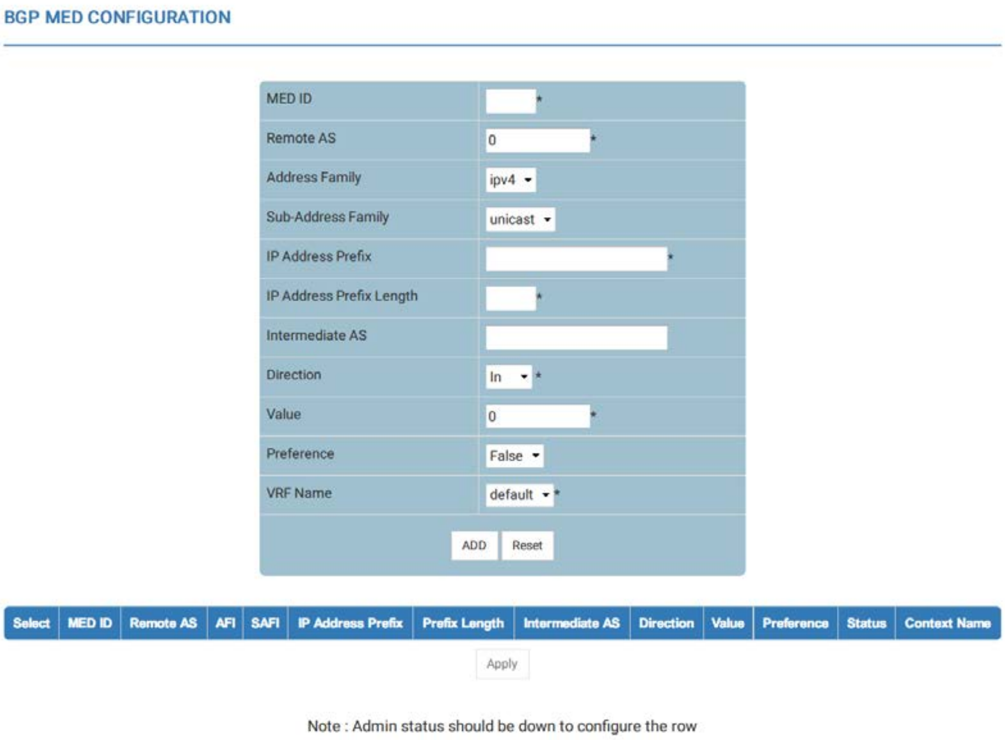
* Automatic start feature is enabled and

* BGP session is brought down either by automatic stop feature or through reception of invalid BGP message

The peer status is internally is set as auto-start when automatic start feature is enabled.

VRF Name / Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.5 Multi-Exit Discriminators



BGP MED CONFIGURATION

MED ID	*
Remote AS	0 *
Address Family	ipv4
Sub-Address Family	unicast
IP Address Prefix	*
IP Address Prefix Length	*
Intermediate AS	
Direction	In *
Value	0 *
Preference	False
VRF Name	default *

Select	MED ID	Remote AS	AFI	SAFI	IP Address Prefix	Prefix Length	Intermediate AS	Direction	Value	Preference	Status	Context Name

Note : Admin status should be down to configure the row

Fig: BGP MED Configuration

The *Multi-Exit Discriminators* link opens the **BGP MED Configuration** Page.
The BGP MED Configuration page allows the user to configure the MED values that are to be assigned to routes learnt from BGP peers.

The table below lists the fields present in this page.
Select - Select the MED entry for which the configurations need to be reapplied.
MED ID - Enter the Multi-Exit Discriminator Index value which is the index value of the BGP MED Table. This value ranges between 1 and 100.
Remote AS - Enter the remote Autonomous System number for which the local preference is associated. This value ranges between 0 and 65535. By default the Remote AS value is set as 0.
Address Family / AFI - Select the type of IP address prefix in the Network Layer Reachability Information field in the update. The options are:
* ipv4 - Sets the type of IP address prefix as IP version 4.
* ipv6 - Sets the type of IP address prefix as IP version 6.
> This field should be configured before configuring the IP address prefix.

Sub-Address Family / SAFI - Select the sub-sequent address family of IP address prefix in the Network Layer Reachability Information field in the update. By default Sub-Address Family is set as unicast. The list contains:

* unicast - Sets the sub-sequent address family of IP address prefix as unicast.

> This field should be configured before configuring the IP address prefix.

IP Address Prefix - Enter the IP address prefix in the Network Layer Reachability Information field on which local-preference policy needs to be applied.

IP Address Prefix Length - Enter the length (in bits) of the IP address prefix in the Network Layer Reachability Information field. This value ranges between 0 and 32 bits. By default IP Address Prefix Length value is set as 0 bits.

Intermediate AS - Enter a list of intermediate Autonomous system numbers through which the route update is expected to travel. This is a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a string with the maximum size as 100.

Direction - Select the direction of application of the MED Policy. By default Direction is set as In. The list contains:

* In - Indicates the updates on the received routes

* Out - Indicates the updates that needs to be advertised to peers on the route

Value - Enter the MED value assigned to the MED Attribute for the route present in NLRI. This value ranges between 0 and 2147483647.

By default MED Value is set as 0.

Preference - Select the preference status which denotes whether the value present in this entry takes precedence when the attribute is already present in the update message that has been received.

By default, the preference is set as False. The list contains:

* True - Indicates that the value present in this entry takes precedence when the attribute is already present in the update message that has been received

* False - Indicates that the value present in this entry does not take precedence

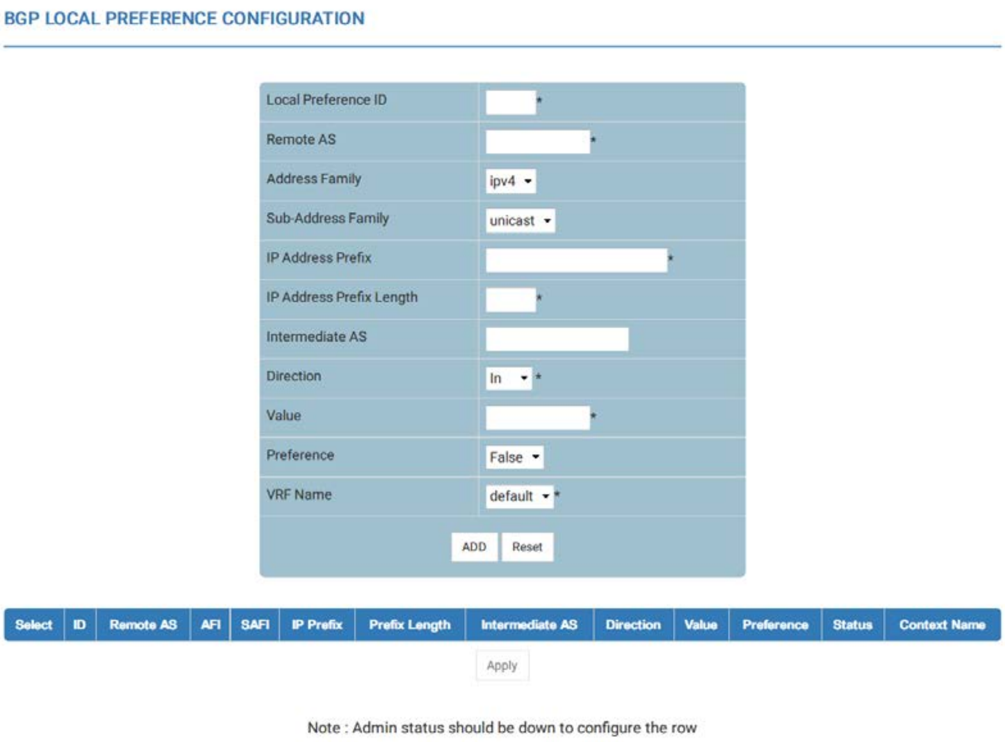
Status - Select the MED Status routes learnt by BGP peers. By default the MED Status is set as Down. The list contains:

* Up - Sets MED Status as UP

* Down - Sets MED Status as Down

VRF Name / Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.6 Local Preferences



BGP LOCAL PREFERENCE CONFIGURATION

Local Preference ID	*
Remote AS	*
Address Family	ipv4
Sub-Address Family	unicast
IP Address Prefix	*
IP Address Prefix Length	*
Intermediate AS	
Direction	In *
Value	*
Preference	False
VRF Name	default *

Select	ID	Remote AS	AFI	SAFI	IP Prefix	Prefix Length	Intermediate AS	Direction	Value	Preference	Status	Context Name

Note : Admin status should be down to configure the row

Fig: BGP Local Preference Configuration

The *Local Preferences* link opens the **BGP Local Preference Configuration** Page.

The BGP Local Preference Configuration page allows the user to configure the Local preference value for the routes.

The table below lists the fields present in this page.

Select - Select the Local Preference Identifier entry for which the configurations need to be modified.

Local preference ID - Enter the Local Preference ID for the route. This value ranges between 1 and 100.

Remote AS - Enter the Remote Autonomous System number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 65535. By default the Remote AS value is set as 0.

Address Family / AFI - Select the type of IP address prefix in the Network Layer Reachability Information field. The list contains:

* ipv4 - Sets the type of IP address prefix as IP version 4.

* ipv6 - Sets the type of IP address prefix as IP version 6.

> This field should be configured before configuring the IP address prefix.

Sub-Address Family / SAFI - Select the sub-sequent address family of IP address prefix in the Network Layer Reachability Information field in the update. The list contains:

* unicast - Sets the sub-sequent address family of IP address prefix as unicast.

> This field should be configured before configuring the IP address prefix.

IP Address Prefix / IP Prefix - Enter the IP Address prefix in the Network Reachability Information field.

IP Address Prefix Length / Prefix Length - Enter the length (in bits) of the IP address prefix in the Network Reachability Information field. The value ranges between 0 and 32. By default IP Address Prefix Length is set as 0.

Intermediate AS - Enter a list of intermediate Autonomous system numbers through which the route update is expected to travel. This is a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a string with the maximum size as 100

Direction - Select the direction of application of the Local Preference Policy with which the entry is to be associated. By default Direction is set as In. The list contains:

* In - Indicates the updates on the received routes

* Out - Indicates the updates that needs to be advertised to peers on the route

Value - Enter the value assigned to the LP (Local Preference) Attribute for the route present in NLRI. The value ranges between 0 and 2147483647. By default Local Preference Value is set as 100.

Preference - Select the preference status which denotes whether the value present in this entry takes precedence when the attribute is already present in the update message that has been received.

The default value is set as false. The list contains:

* True - Indicates that the value present in this entry takes precedence when the attribute is already present in the update message that has been received

* False - Indicates that the value present in this entry does not take precedence

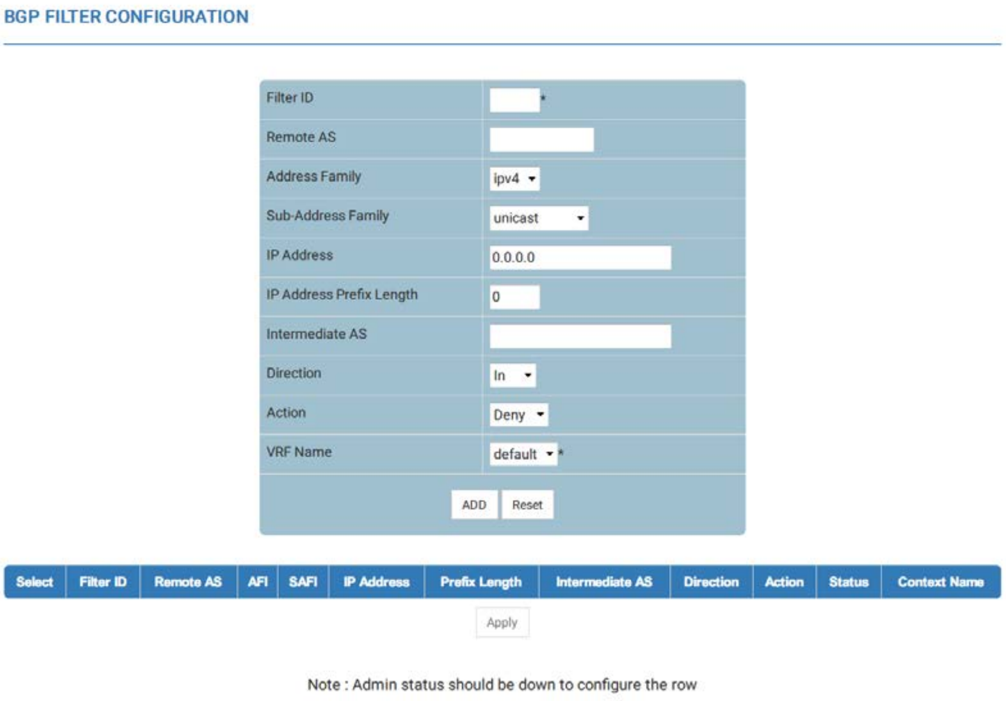
Status - Select the status of the Local Preference routes learnt by BGP peers. By default the Local Preference Status is set as Down. The list contains:

* Up - Sets Local Preference Status as UP

* Down - Sets Local Preference Status as Down

VRF Name / Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.7 Filters



BGP FILTER CONFIGURATION

Filter ID	*
Remote AS	
Address Family	ipv4
Sub-Address Family	unicast
IP Address	0.0.0.0
IP Address Prefix Length	0
Intermediate AS	
Direction	In
Action	Deny
VRF Name	default *

Select	Filter ID	Remote AS	AFI	SAFI	IP Address	Prefix Length	Intermediate AS	Direction	Action	Status	Context Name

Note : Admin status should be down to configure the row

Fig: BGP Filter Configuration

The *Filters* link opens the **BGP Filter Configuration** Page.

The BGP Filter Configuration page allows the user to configure an entry in Update Filter Table which contains rules to filter out updates based on the AS from which it is received, Network Layer Reachability Information (NLRI) and AS through which it had passed.

The table below lists the fields present in this page.

Select - Select the Filter Identifier entry for which the configurations need to be modified.

Filter ID - Enter the filter index. This value ranges between 1 and 100.

Remote AS - Enter the remote AS number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 65535. By default Remote AS value is set as 0.

Address Family / AFI - Select the type of IP address prefix in the Network Layer Reachability Information field. The options are:

* ipv4 - Sets the type of IP address prefix as IP version 4.

* ipv6 - Sets the type of IP address prefix as IP version 6.

> This field should be configured before configuring the IP address prefix.

Sub-Address Family / SAFI - Select the sub-sequent address family of IP address prefix in the Network Layer Reachability Information field in the update. The list contains:

* unknown - Sets the sub-sequent address family of IP address prefix as unknown which implies that any sub-sequent address family can be used for IP address prefix.

* unicast - Sets the sub-sequent address family of IP address prefix as unicast.

* labelledIpv4 - Sets the sub-sequent address family of IP address prefix as labeled IP version 4.

* vpnv4 - Sets the sub-sequent address family of IP address prefix as VPN version 4.

> This field should be configured before configuring the IP address prefix.

IP Address - Enter the IP address prefix in the Network Layer Reachability Information field. The default value is 0.0.0.0.

IP Address Prefix Length / Prefix Length - Enter length (in bits) of the IP address prefix in the Network Layer Reachability Information field. This value ranges between 0 and 32 bits for ipv4 address and 0 to 128 for ipv6 address type. By default IP Address Prefix Length is set as 0 bits.

Intermediate AS - Enter a list of intermediate Autonomous system numbers through which the route update is expected to travel. This is a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a string with the maximum size as 100

Direction - Select the direction of application of filters with which the entry is to be associated. The default value is set as In. The list contains:

* In - Indicates the updates on the received routes

* Out - Indicates the updates that needs to be advertised to peers on the route

Action - Select the status that controls addition or deletion of the non bgp routes. By default the action value is set as Deny. The list contains:

* Allow - Allows addition of non bgp routes.

* Deny- Denies addition of non bgp routes.

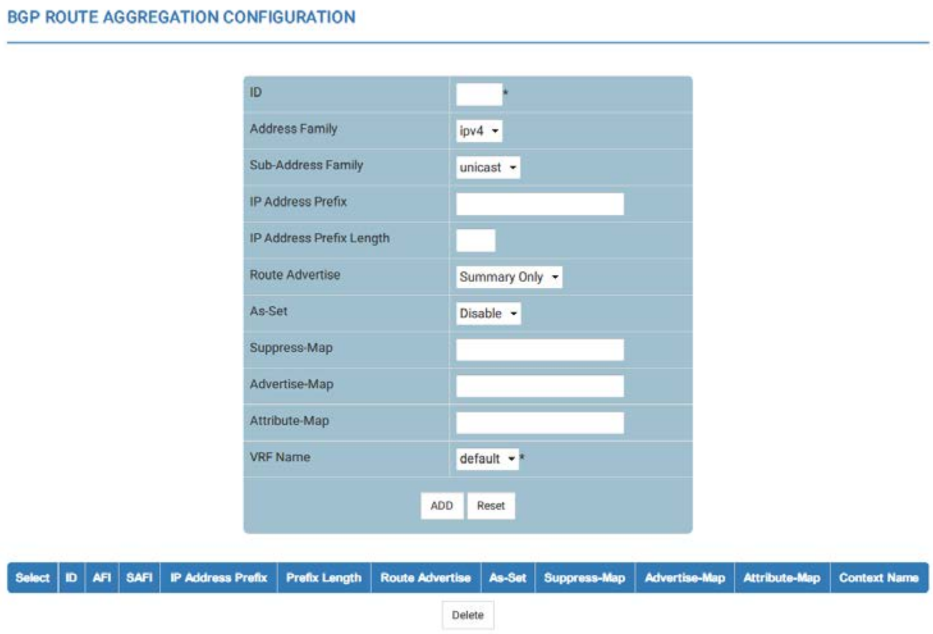
Status - Select the status of the routes learnt by BGP peers. By default the Status is set as Down. The list contains:

* Up - Sets BGP Filter Status as UP

* Down - Sets BGP filter Status as Down

VRF Name / Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.8 Route Aggregation



BGP ROUTE AGGREGATION CONFIGURATION

ID	*
Address Family	ipv4
Sub-Address Family	unicast
IP Address Prefix	
IP Address Prefix Length	
Route Advertise	Summary Only
As-Set	Disable
Suppress-Map	
Advertise-Map	
Attribute-Map	
VRF Name	default *

Select	ID	AFI	SAFI	IP Address Prefix	Prefix Length	Route Advertise	As-Set	Suppress-Map	Advertise-Map	Attribute-Map	Context Name

Fig: BGP Route Aggregation Configuration

The *Route Aggregation* link opens the **BGP Route Aggregation Configuration** Page.

The BGP Route Aggregation Configuration page allows the user to configure the aggregation of the routing information. This creates an aggregate entry in a BGP or multiprotocol BGP routing table if any more-specific BGP or multiprotocol BGP routes are available that fall in the specified range. The entries in the table specify the IP address based on which the routing information has to be aggregated. The aggregate route will be advertised as coming from autonomous system. The atomic aggregate attribute will be set only if some of the information in the AS PATH is missing in the aggregated route, else it will not be set.

The table below lists the fields present in this page.

Select - Select the neighbor for which the configurations need to be reapplied.

ID - Enter the index to BGP Route Aggregation table. This value ranges between 1 and 100.

Address Family/ AFI - Select the type of IP address prefix in the Network Layer Reachability Information field. The options are:

* ipv4 - Sets the type of IP address prefix as IP version 4.

* ipv6 - Sets the type of IP address prefix as IP version 6.

> This field should be configured before configuring the IP address prefix.

Sub-Address Family / SAFI - Select the sub-sequent address family of IP address prefix in the Network Layer Reachability Information field in the update. The options are:

* unicast - Sets the sub-sequent address family of IP address prefix as unicast.

> This field should be configured before configuring the IP address prefix.

IP Address Prefix - Enter the IP address prefix in the Network Layer Reachability Information field.

IP Address Prefix Length/ Prefix Length - Enter the length (in bits) of the IP address prefix in the Network Layer Reachability Information field. This value ranges between 0 and 32 for ipv4 address and 0 to 128 bits for ipv6 address.

Route Advertise - Select the route updates that should be sent to the peers. By default Route Advertise is set as Summary-only. The list contains:

* Summary-only - Indicates that only the summarized route has to be advertised to peers.

* All - Indicates that both the summary and the more-specific routes based on which the summary entry was generated, have to be advertised to the peers.

As-Set - Select the generation status of autonomous system set path information. By default As-Set is set as disable. The list contains:

* enable - Enables the generation of autonomous system set path information

* disable - Disables the generation of autonomous system set path information

Suppress-Map - Enter the name for suppress route-map. The route map contains the rules for suppressing the routes while aggregation.

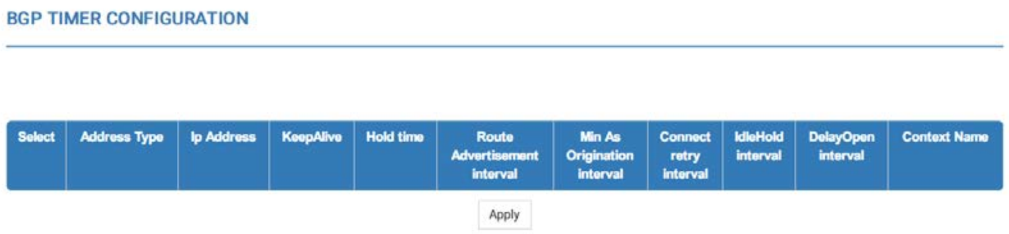
When suppress-map configuration is used along with summary-only option, summary-only configuration does not have any effect. And the more-specific routes that the suppress-map suppresses are not advertised. Other routes are advertised in addition to the aggregated route This value is a string with the maximum size as 20.

Advertise-Map - Enter the name for advertise route-map. The route map contains the rules for advertising the routes while aggregation. When advertise-map is used, only advertise-map influences the creation of aggregate entry. In absence of advertise-map, the aggregate route inherits the attributes of the more specific routes, both suppressed and unsuppressed. This value is a string with the maximum size as 20.

Attribute-Map - Enter the name for attribute route-map. The route map contains the rules for setting the attributes the aggregated route. When attribute-map and advertise-map along with autonomous system set path information are enabled, the attribute-map overrides the attribute that is formed with the routes selected by the advertise-map. This value is a string with the maximum size as 20.

VRF Name / Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.9 Timers



BGP TIMER CONFIGURATION

Select	Address Type	Ip Address	KeepAlive	Hold time	Route Advertisement interval	Min As Origination interval	Connect retry interval	IdleHold interval	DelayOpen interval	Context Name

Fig: BGP Timer configuration

The *Timers* link opens the **BGP Timer configuration** Page.

The BGP Timer configuration page allows the user to configure the timer related parameters for the peer.

The table below lists the fields present in this page.

Address Type - Displays the address type of the remote peer. This is a read-only field. The type can be:

* ipv4 - Denotes the remote peer ip address type as IP version 4.

* ipv6 - Denotes the remote peer ip address type as IP version 6.

Ip Address - Displays the IP address of the BGP peer. This is a read-only field.

KeepAlive - Enter the maximum time interval between successive keepalive messages exchanged between two peers. This value ranges between 0 and 21845 seconds. The optimal value is 30 seconds.

> Periodical KEEPALIVE messages will be sent to the peer after the BGP connection is established.

Hold time - Enter the timer interval that a BGP will wait, before it decides that a connection to the peer is turn down. The system declares a peer dead, after ensuring that keep alive message is not received within this time period from the peer. This value ranges between 3 and 65535 seconds or can be configured as zero. The optimal value is 90 seconds.

Route Advertisement interval - Enter the minimum interval in seconds between router advertisements. This value ranges between 1 and 65535 seconds. The optimal value is 30 seconds.

Min As Origination interval - Enter minimum time in seconds between advertisements of changes within the speaker- s AS. This value ranges between 1 and 65535 seconds. By default the Min As Origination interval is set as 15 seconds.

Connect retry interval - Enter the time (in seconds) to wait before the router attempts to reconnect to the BGP neighbor after failing to connect. This value ranges between 1 and 65535 seconds. By default the optimal value is set as 120 seconds.

IdleHold interval - Enter the time interval till which the BGP peer is held in the idle state prior to the next automatic restart. The value ranges between 1 and 65535 seconds. By Default IdleHoldinterval is set as 60 seconds.

For each successive damp oscillations, the current idle hold timer value will be increased twice its previous value. It happens through internal logic.

The idle hold time interval can be configured if either:

1. Automatic start feature is enabled or
2. Damp peer oscillation feature is enabled

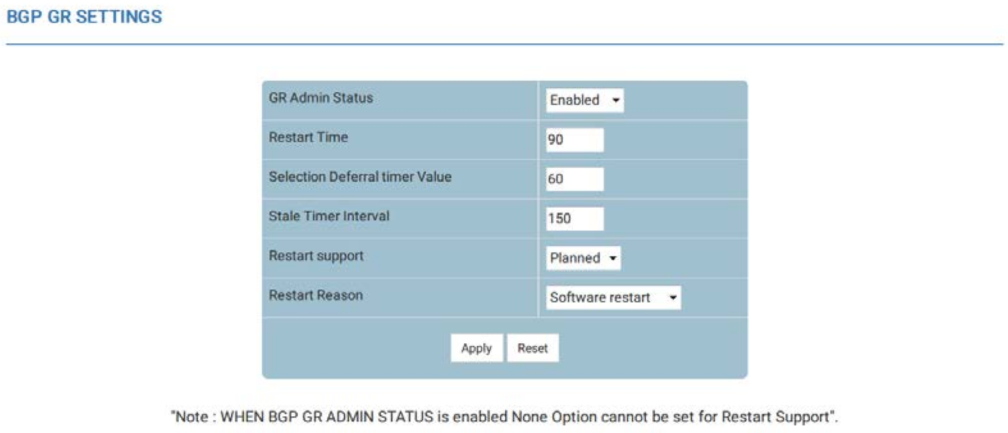
If both damp peer oscillation and automatic start feature are disabled, the existing value is always set instead of the newly configured value.

DelayOpen interval - Enter the amount of time the BGP peer should delay in sending open message to the remote peer. This delay allows the remote peer to send the first open message. The value ranges between 0 and 65535 seconds. By default DelayOpenInterval is set as 0 seconds.

This time can be configured only if the delay open status is set as enabled. Otherwise, the existing value is always set instead of the newly configured value.

Context Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.10 GR Settings



BGP GR SETTINGS

GR Admin Status	Enabled
Restart Time	90
Selection Deferral timer Value	60
Stale Timer Interval	150
Restart support	Planned
Restart Reason	Software restart

"Note : WHEN BGP GR ADMIN STATUS is enabled None Option cannot be set for Restart Support".

Fig: BGP GR Settings

The *GR Settings* link opens the **BGP GR Settings** Page.

The BGP GR Settings page allows the user to configure the graceful restart settings of the BGP.

The table below lists the fields present in this page.

GR Admin Status - Select the GR capability status in the BGP speaker. The default option is Disabled. The list contains:

* Enabled - Enables GR capability in the BGP speaker

* Disabled - Disables capability in the BGP speaker

> To set the GR parameters, the BGP GR admin status should be disabled.

Restart Time - Enter the time, in seconds, for the BGP session to be re-established after a restart. The default value should be less than or equal to Hold Time carried in open message. This value ranges between 1 and 4096 seconds. By default Restart Time is set as 90 seconds.

Selection Deferral timer Value - Enter the upper limit time until which a router defers its route selection. This timer value should be large enough, to provide all the peers of the Restarting Speaker with enough time to send all the routes to the Restarting Speaker. This value ranges between 60 and 1800 seconds. By default Selection Deferral timer Value is set as 60 seconds.

Stale Timer Interval - Enter the upper limit time until which a router retains the stale routes. This value ranges between 90 and 3600 seconds. By default Stale Timer Interval is set as 150 seconds.

Restart support - Select the router support for the BGP graceful restart feature. By default Restart Support option is set to None. The list contains:

* None - Sets restart support as None which implies that no restart support is not provided for the graceful restart feature.

* Planned - Sets restart support as planned restarts.

* Both - Sets restart support as both planned and unplanned restarts.

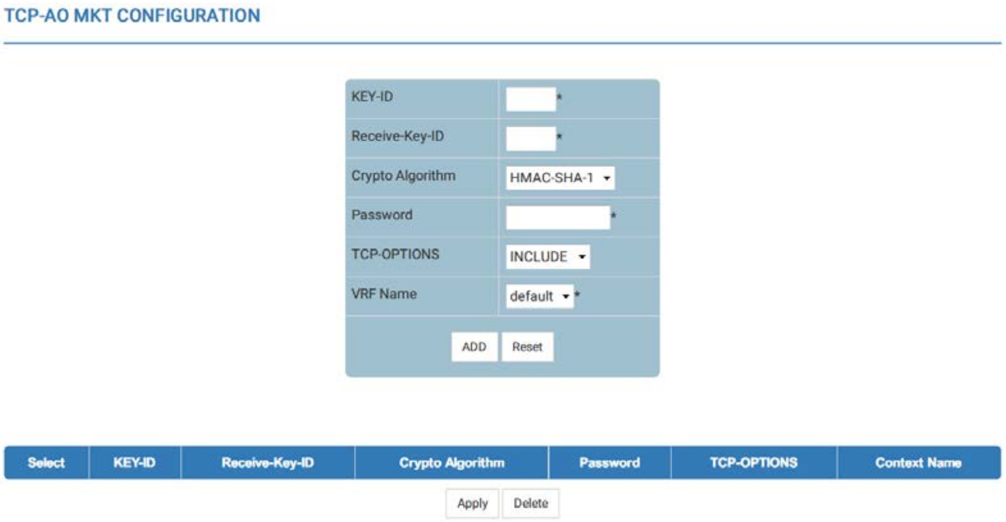
Restart Reason - Select the router restart reason code of the BGP graceful restart feature. By default Restart Reason is set as Software restart. The list contains:

* Unknown - Sets restart reason as unknown where System restarts due to unplanned events (such as restarting after a crash).

* Software restart - Sets restart reason as software restart where System restarts due to software restart.

* Software upgrade - Sets restart reason as software upgrade where System restarts due to reloading / upgrading of software.

5.8.11 TCP-AO Authentication



TCP-AO MKT CONFIGURATION

KEY-ID	*
Receive-Key-ID	*
Crypto Algorithm	HMAC-SHA-1
Password	*
TCP-OPTIONS	INCLUDE
VRF Name	default *

Select	KEY-ID	Receive-Key-ID	Crypto Algorithm	Password	TCP-OPTIONS	Context Name

Fig: TCP-AO MKT Configuration

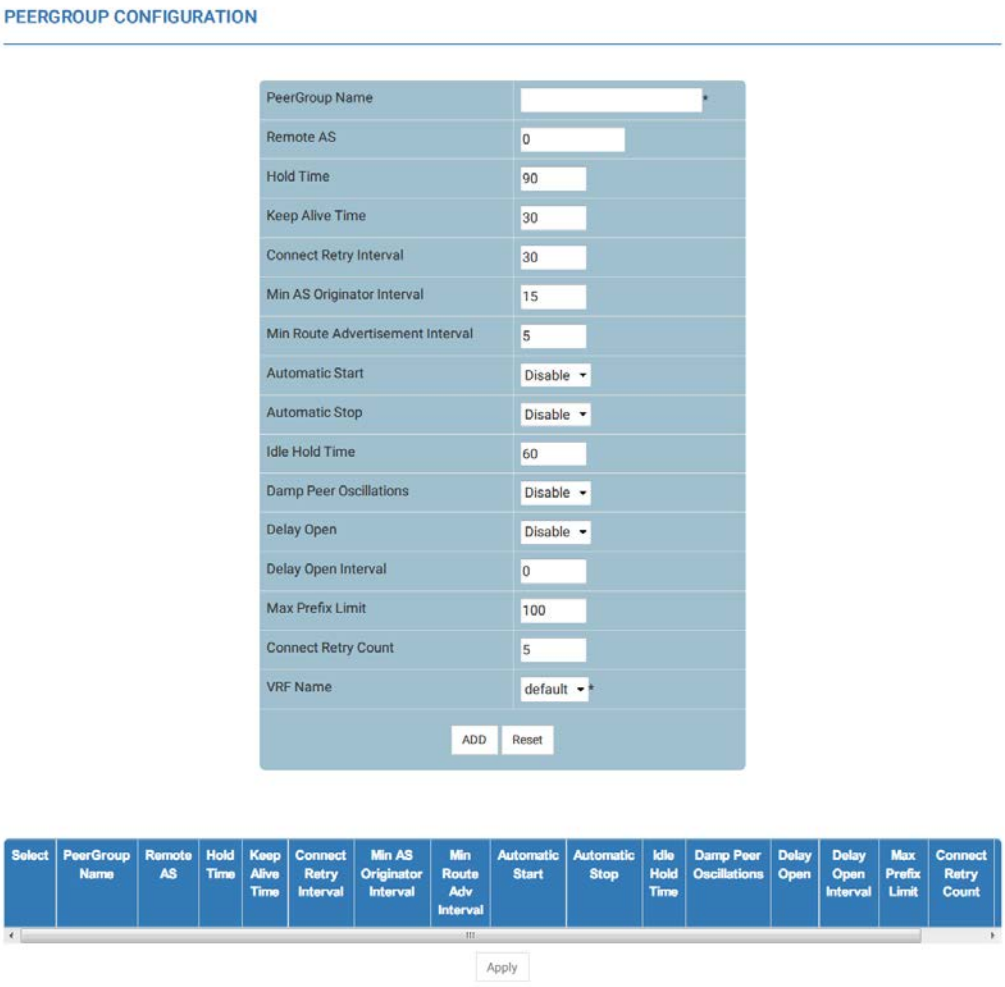
The *TCP-AO Authentication* link opens the **TCP-AO MKT Configuration** Page.
The TCP-AO MKT Configuration page allows the user to configure the TCP-AO MKT settings of the BGP.

The table below lists the fields present in this page.
KEY-ID - Enter the sending KeyID of the MKT. This value is used to fill the key-id field in the TCP-AO option in the TCP header. This value ranges between 0 and 255.
Receive-Key-ID - Enter the receive Key-id of the MKT. The MKT that is ready at the sender to be used to authenticate received segments is indicated to the peer by filling the receive key id of the MKT in the RNExtKeyId field of the TCP-AO option in TCP header. This value ranges between 0 and 255.
Crypto Algorithm - Select the algorithm used for TCP-AO MAC or KDF calculation.
The default value is HMAC-SHA-1. The list contains:
* AES-128 - Indicates usage of hmac-sha-1 for authentication
* HMAC-SHA-1 - Indicates usage of hmac-sha-1 for authentication
Password - Enter the Master Key corresponding to the MKT. This value is a string with the maximum size as 80.
TCP-OPTIONS - Select exclude or include TCP options other than TCP-AO during MAC calculation. If select INCLUDE, TCP-AO MAC will be calculated on tcp segment including all other TCP options. The default value is INCLUDE.
The list contains:
* EXCLUDE - TCP-AO MAC will be calculated on tcp segment excluding all other TCP options

* INCLUDE - TCP-AO MAC will be calculated on tcp segment including all other TCP options

Context Name / VRF Name - Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.12 Peer-Group



PEERGROUP CONFIGURATION

PeerGroup Name	*
Remote AS	0
Hold Time	90
Keep Alive Time	30
Connect Retry Interval	30
Min AS Originator Interval	15
Min Route Advertisement Interval	5
Automatic Start	Disable
Automatic Stop	Disable
Idle Hold Time	60
Damp Peer Oscillations	Disable
Delay Open	Disable
Delay Open Interval	0
Max Prefix Limit	100
Connect Retry Count	5
VRF Name	default *

Select	PeerGroup Name	Remote AS	Hold Time	Keep Alive Time	Connect Retry Interval	Min AS Originator Interval	Min Route Adv Interval	Automatic Start	Automatic Stop	Idle Hold Time	Damp Peer Oscillations	Delay Open	Delay Open Interval	Max Prefix Limit	Connect Retry Count

Fig: PeerGroup Configuration

The *Peer-Group* link opens the **PeerGroup Configuration** Page.

The PeerGroup Configuration page allows the user to create a BGP peer group and configure its parameters. The peer group configurations are applicable to all the peers present in the peer group.

The table below lists the fields present in this page.

Select - Click to select the Peer group name for which the configuration needs to be modified.

Peer Group Name - Enter the peer-group-name for configuring BGP peer group. The members of this peer group will inherit the characteristics configured with this page. This value is a string with the maximum size as 20.

Remote AS - Enter the remote AS associated with the BGP peer group. This value ranges between 0 and 65535. By default the Remote AS value is set as 0.

Hold time - Enter the timer interval for the Hold Time configured for the BGP speaker with all the peers configured for this peer group. This value is placed in an OPEN message sent to the peers by the BGP speaker. This value ranges between 3 and 65535 seconds or can be configured as zero. If it is configured as 0, the Hold Time is not established with the peer.

By default, the Hold time value is set as 90 seconds.

Keep Alive Time - Enter the keep alive interval (in seconds) for the BGP speaker with all the peers configured for this peer group. The value of this object will only determine the KEEPALIVE messages frequency relative to the Hold Time. This value ranges between 1 and 21845.

The keep-alive value must always be less than the configured hold-time value A reasonable maximum value for this timer is one third of that of Hold Time value. If this value is zero (0), no periodical KEEPALIVE messages are sent to the peers after the BGP connection is established.

By default, the keep alive time is set as 30 seconds.

Connect Retry Interval - Enter the connect retry time interval (in seconds) for the peers in this peer group. This is the time interval after which a transport connection with peer is re-initiated. This value ranges between 1 and 65535.

By default the Connect Retry Interval is set as 30 seconds.

Min AS Originator Interval - Enter the AS origination interval for the peers in this peer group. This is the time-interval (in seconds) for spacing successive route-updates originating within the same AS.

By default the Min AS Originator interval is set as 15 seconds.

Min Route Advertisement Interval - Enter the advertisement interval for the peers in this peer group. This is the time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination.

This value ranges between 1 and 65535. By default the Min Route Advertisement Interval is set as 30 seconds for EBGP connections and 5 seconds for IBGP connections.

Automatic Start - Select the Automatic Start status for the BGP session with the associated peers in the peer group. By default, the Automatic Start status is set as Disable The list contains:

* Disable - Disables the BGP session with the associated peer automatically. The BGP session with the peer has to be manually initiated.

* Enable - Starts the BGP session with the associated peer automatically. The peer session is automatically started in the IDLE state, after a BGP Peer session is brought down either by Autostop or through reception of invalid BGP message.

The BGP session is automatically started after an interval specified by idle hold timer.

Automatic Stop - Select the status to enable/disable the auto stop option to stop the BGP peer and BGP connection automatically. By default, the Automatic Stop status is set as Disable. The list contains:

* Disable - Disables the BGP session with the associated peer automatically. When Automatic Stop is disabled, the connect retry count value is set to 0

* Enable - Stops the BGP session with the associated peer automatically. After an automatic stop, the Peer connection needs to be re-intiated manually by the administrator.

IdleHold interval - Enter the time interval till which the BGP peers in this peer group are held in the idle state prior to allow the next automatic restart. This value ranges between 1 and 65535 seconds.

By default the idle hold time interval is set as 60 seconds.

The idle hold time interval can be configured only if either:

* Automatic start feature is enabled or

* Damp peer oscillation feature is enabled

If both damp peer oscillation and automatic start feature are disabled, the existing value is always set instead of the newly configured value.

For each successive damp oscillations, the current idle hold timer value will be increased twice its previous value. It happens through internal logic.

Damp Peer Oscillations - Select the status of the damp peer oscillation option which specifies that specifies that the implementation engages additional logic to damp the oscillations of BGP peers in the face of series of automatic start and automatic stop operations in the IDLE state.

By default the Damp Peer Oscillations is set as Disable. The list contains:

* Disable - Disables the damp peer oscillation option.

* Enable - Enables the damp peer oscillation option.

Delay Open - Select the status of the delay in sending the first OPEN message to the BGP peer for a specific time period. By default the Delay Open is set as Disable. The list contains:

* Disable - Disables the delay option for sending open messages , which implies that open messages are sent to the remote BGP peer without any delay.

* Enable - Enables delay in sending open messages to the remote BGP peer for a configured open delay time period.

This delay allows the remote peer to send the first open message.

Delay Open Interval - Enter the delay open time interval which is the amount of time that the BGP peer should delay in sending the OPEN message to the remote peer. This value ranges between 0 and 65535. By default, the delay open interval is set as 0.

This field can be configured if the Delay Open option is enabled.

Max Prefix Limit - Enter the maximum number of address prefixes that the BGP Peer is willing to accept from the neighbor. This value ranges between 1 and 2147483647. By default the Max Prefix Limit value is set as 100.

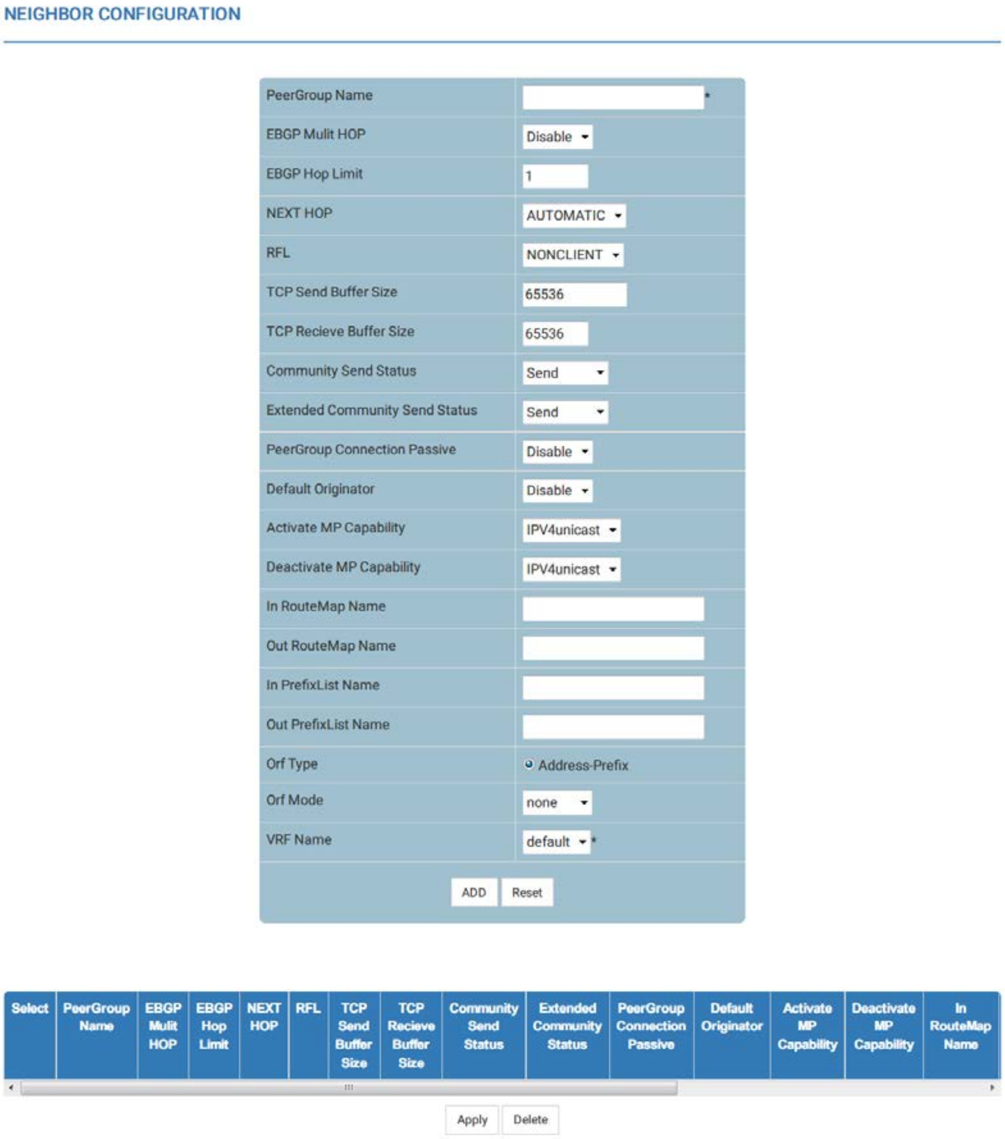
The default value is calculated based on the following formula:

Maximum number of routes in the routing table / Maximum number of peers supported by BGP.

Connect Retry Count - Enter the retry count which specifies the number of times the BGP peer should try to establish a TCP-connect issue with its neighboring peers. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State. This value ranges between 1 and 50. By default the Connect Retry Count value is set as 5.

VRF Name/ Context Name - Select the VRF name from the list to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.13 Peer-Group (Cont..)



NEIGHBOR CONFIGURATION

PeerGroup Name	*
EBGP Mulit HOP	Disable
EBGP Hop Limit	1
NEXT HOP	AUTOMATIC
RFL	NONCLIENT
TCP Send Buffer Size	65536
TCP Recieve Buffer Size	65536
Community Send Status	Send
Extended Community Send Status	Send
PeerGroup Connection Passive	Disable
Default Originator	Disable
Activate MP Capability	IPV4unicast
Deactivate MP Capability	IPV4unicast
In RouteMap Name	
Out RouteMap Name	
In PrefixList Name	
Out PrefixList Name	
Orf Type	● Address-Prefix
Orf Mode	none
VRF Name	default *

Select	PeerGroup Name	EBGP Mulit HOP	EBGP Hop Limit	NEXT HOP	RFL	TCP Send Buffer Size	TCP Recieve Buffer Size	Community Send Status	Extended Community Status	PeerGroup Connection Passive	Default Originator	Activate MP Capability	Deactivate MP Capability	In RouteMap Name

Fig: Neighbor Configuration

The *Peer-Group (Cont..)* link opens the **Neighbor Configuration** Page.

The Neighbor Configuration page allows the user to configure the parameters for BGP peer associated with the peer group.

The table below lists the fields present in this page.

Select - Click to select the Peer group name for which the configuration needs to be modified or the peer group is to be deleted.

PeerGroup Name - Enter the peer-group-name for configuring BGP peer group. The members of this peer group will inherit the characteristics configured with this page. This value is a string with the maximum size as 20.

EBGP Multi HOP - Select the status of the EBGP Multi HOP. By Default EBGP MultiHop is set as Disable. The list contains:

* Disable - Disables BGP to establish connection with external peers residing on networks that are not directly connected .If EBGP-Multihop is disabled and external BGP peers are indirectly connected, then BGP peer session will not be established.

* Enable - Enables BGP to establish connection with external peers residing on networks that are not directly connected. If external BGP peer are not connected directly, then EBGP-Multihop is enabled to initiate the connection with that external peer

This configuration is effective only when EBGP peers added to this peer group

EBGP Hop Limit - Enter the EBGP Hop Limit value that is used during connection with external peers. This value ranges between 1 and 255. By default, the EBGP Hop Limit value is set as 1. BGP speaker accepts or attempts connection to external peers residing on network that are not directly connected but separated by the configured hop limit value.

This configuration is effective only when EBGP peers added to this peer group

NEXT HOP - Select whether the next hop attribute sent in the update message to the peers in this peer group has to be generated automatically or self. This is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet. By default, Next Hop is set as AUTOMATIC. The list contains:

* AUTOMATIC - Generates the next hop based on the IP address of the destination and the present next hop in the route information.

* SELF - Enables BGP to send itself as the next hop for advertised routes.

RFL - Select the Route Reflector Client status of the peer. This status is used to define client and non-client peers for implementing route reflection. The route reflection mechanism operates as follows:

* A cluster system acting as route reflector sends a route to all client peers within the cluster, if the route is received from a nonclient peer.

* The cluster system acting as route reflector sends a route to all nonclient peers and all client peers except the originator, if the route is received from a client peer.

By default, the route reflector client status is set as NONCLIENT.

The list contains:

* NONCLIENT - Configures the peer as non client peer, which denotes that the peer is outside the cluster

* CLIENT - Configures the peer as client peer, which denotes that the peer is within the cluster.

> The route reflector client can be set as Client only for the peer within the cluster (for the peer entries having the remote AS same as that of the AS number set for RRD in RRD Basic Settings page).

TCP Send Buffer Size - Enter the TCP window size on the sender side for all the peers in this peer group. This value ranges between 4096 and 65536. By default, the TCP Send Buffer Size value is set as 65536.

TCP Receive Buffer Size - Enter the TCP window size on the receiver side for all the peers in this peer group. This value ranges between 4096 and 65536. By default, the TCP Receive Buffer Size value is set as 65536.

Community Send Status - Select the status of the send community attribute for the peers in this peer group. By default, Community Send Status is set as Send. The list contains:

* NONE - Sets Community Send status as none.

* SEND - Sends community attribute to a BGP neighbor and enables advertisement of community attributes (standard/extended) to peer

* DONTSEND - Disables advertisement of standard community attributes to peer .

Extended Community Send Status - Select the status of extended community send attribute for the peers in this peer group. The BGP extended community is used to label BGP routing information for controlling the distribution of the information. By default, the Extended Community Send status is set as send. The list contains:

* NONE - Sets extended community send status as none

* SEND - Sends extended community attribute to a BGP neighbor and enables advertisement of extended community attributes to peer

* DONTSEND - Disables advertisement of extended community attributes to peer

PeerGroup Connection Passive - Select the status of the PeerGroup Connection. By default the PeerGroup Connection Passive is set as Disable. The list contains:

* Enable - Sets the peer group connection as passive. BGP speaker waits for the remote peer to initiate the session with the peer.

* Disable - Sets the peer group connection as active. BGP speaker initiates the session with the peer.

Default Originator - Select the status of the advertisement of the default route to all the peers in this peer group. By default the Default Originator is set as Disable. This list contains:

* Disable - Disables the advertisement of the default route to all the peers in this peer group

* Enable - Enables the advertisement of the default route to all the peers in this peer group.

> This field overrides the global default route configuration and always sends a default route to the peer with self next-hop.

This advertisement occurs irrespective of the presence of default route in FDB.

Activate MP Capability - Select the option to activate corresponding MP Capability. If any MP Capability is activated, then this capability should be negotiated while establishing session with the peers in this group.

By default, the Activate MP Capability is set as IPV4unicast. The list contains:

* IPV6unicast - Activates the corresponding MP Capability for IPV6 unicast address.

* IPV4unicast - Activates the corresponding MP Capability for IPV4 unicast address.

Deactivate MP Capability - Select the option to deactivate corresponding MP Capability. If any of MP Capability is activated, then this capability should be negotiated while establishing session with the peers in this group. By default, the Deactivate MP Capability is set as IPV4unicast.

The list contains:

* IPV6unicast - Deactivates the corresponding MP Capability for IPV6 unicast address.

* IPV4unicast - Deactivates the corresponding MP Capability for IPV4 unicast address.

In RouteMap Name - Enter the name to configure the in routemap for this peer group entry. This value is a string with the maximum size as 20.

Out RouteMap Name - Enter the name to configure the out routemap for this peer group entry. This value is a string with the maximum size as 20.

In PrefixList Name - Enter the name to configure the in PrefixList for this peer group entry. This value is a string with the maximum size as 20.

Out PrefixList Name - Enter the name to configure the out PrefixList for this peer group entry. This value is a string with the maximum size as 20.

Orf Type - Select the type of the Outbound Route Filter entry.

It should be configure before enabling the ORF modes.

Currently it supports only Address-Prefix based ORF type.

Orf Mode - Select the ORF Capability mode supported for this peer group entry.

If it is set to none, then the both ORF modes will be disabled.

The list contains:

* none - Disable ORF Capability

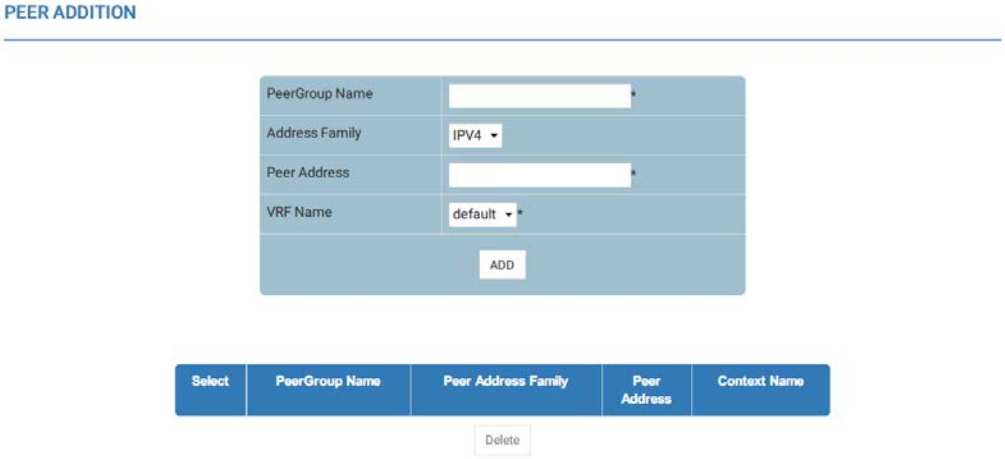
* receive - Enable ORF receive Capability

* send - Enable ORF send capability

* both - Enable both Send and receive Capability

VRF Name / Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.14 Peer Addition with PeerGroup



PEER ADDITION

PeerGroup Name	*
Address Family	IPV4
Peer Address	*
VRF Name	default *

Select	PeerGroup Name	Peer Address Family	Peer Address	Context Name

Fig: Peer Addition

The *Peer Addition with PeerGroup* link opens the **Peer Addition** Page.

The Peer Addition page allows the user to add the configured peer to a peer group.

The table below lists the fields present in this page.

Select - Click to select the Peer Group Name and remove the peer addition to the respective peer group.

Peer Group Name - Enter the name of the peer-group- to which the peer has to be added. This value is a string with the maximum size as 20.

Address Family / Peer Address Family - Select the Address Family of the peer. By default, the Address family is set as IPV4

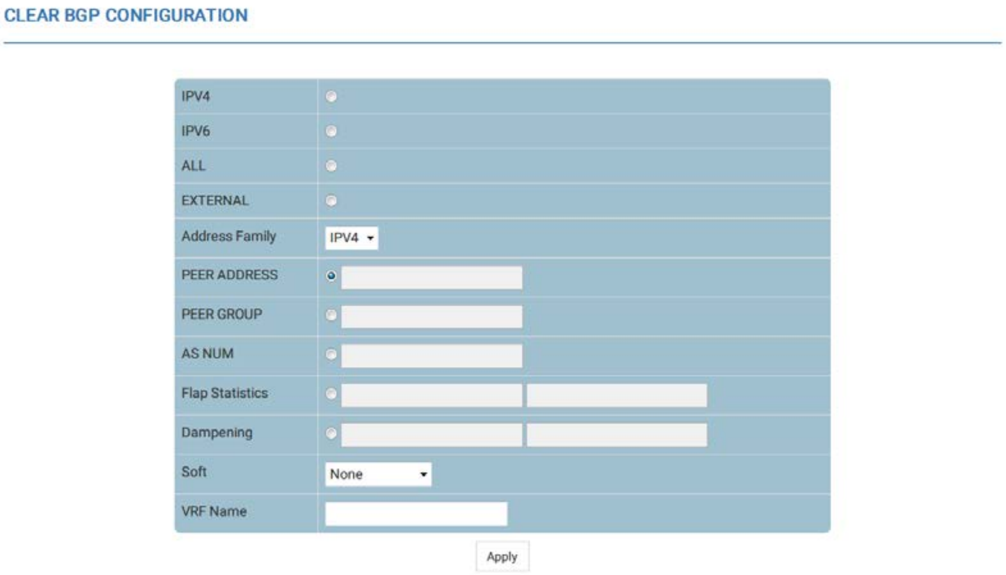
* IPV6 - Specifies that the peer belongs to the IPV6 Address Family

* IPV4 - Specifies that the peer belongs to the IPV4 Address Family.

Peer Address - Enter the remote IP address of the BGP peer.

VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.15 Clear Bgp



CLEAR BGP CONFIGURATION

IPV4	○
IPV6	○
ALL	○
EXTERNAL	○
Address Family	IPV4
PEER ADDRESS	●
PEER GROUP	○
AS NUM	○
Flap Statistics	○
Dampening	○
Soft	None
VRF Name	

Fig: Clear BGP Configuration

The *Clear Bgp* link opens the **Clear BGP Configuration** Page.

The Clear BGP Configuration page allows the user to reset the BGP connection dynamically for inbound and outbound route policy. The inbound routing tables are updated dynamically or by generating new updates using stored update information.

The table below lists the fields present in this page.

IPV4 - Click to reset the bgp connection dynamically for all ipv4 address family peers.

IPV6 - Click to reset the bgp connection dynamically for all ipv6 address family peers

ALL - Click to reset all the BGP peers.

EXTERNAL - Click to reset all the external peers.

Address Family - Select the address family for which the BGP connection needs to be reset.

* IPV6 - Clears all BGP connections which belongs to the IPV6 Address Family.

* IPV4 - Clears all BGP connections which belongs to the IPV4 Address Family.

PEER ADDRESS - Click the option button to select the Peer Address for which the BGP Connection needs to be reset and enter the Peer Address.

PEER GROUP - Click the option button to select the Peer Group for which the BGP Connection needs to be reset and enter the Peer Group name.

This value is a string with the maximum size as 20.

AS NUM - Click the option button to select the AS number for which the BGP Connection needs to be reset and enter the AS number

Flap Statistics - Click to select the option to clears the route flap statistics for the BGP. Enter the required IPv4 / IPv6 address and the Prefix length to clear the route flap statistics.

Dampening - Click to select the option to clear the dampening related configuration for the BGP. Enter the required IPv4 / IPv6 address and the Prefix length to clear the Dampening statistics

Soft - Select the Soft clear which is automatically assumed when the route refresh capability is supported.

* None - Does not initiate inbound soft reconfiguration .

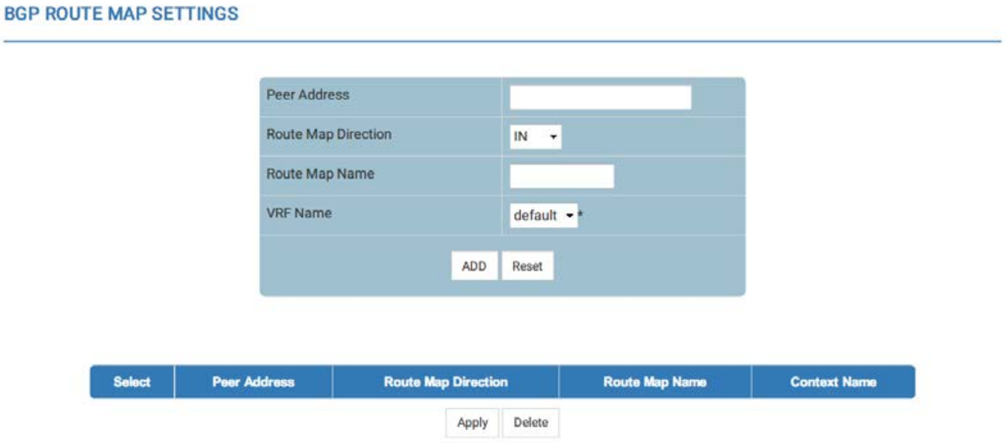
* In - Initiates inbound soft reconfiguration which causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy

* Out - Initiates outbound soft configuration which does not have any memory overhead and does not require any preconfiguration. An outbound reconfiguration can be triggered on the other side of the BGP session to make the new inbound policy take effect.

* Both - Initiates both inbound and outbound soft reconfiguration.

VRF Name - Select the VRF name from the list of instances created to resets the BGP connection for the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.16 Route Map


BGP ROUTE MAP SETTINGS

Peer Address	
Route Map Direction	IN
Route Map Name	
VRF Name	default *

Select	Peer Address	Route Map Direction	Route Map Name	Context Name

Fig: BGP Route Map Settings

The *Route Map* link opens the **BGP Route Map Settings** Page.

The BGP Route Map Settings page allows the user to configure the BGP route map for the neighbor.

The table below lists the fields present in this page.

Select - Click to select the Peer address for which the configuration needs to be modified or the route map is to be deleted.

Peer Address - Enter the remote IP address of the BGP peer.

Route Map Direction - Select the direction of the routemap. By default the Routemap direction is set as IN. The list contains:

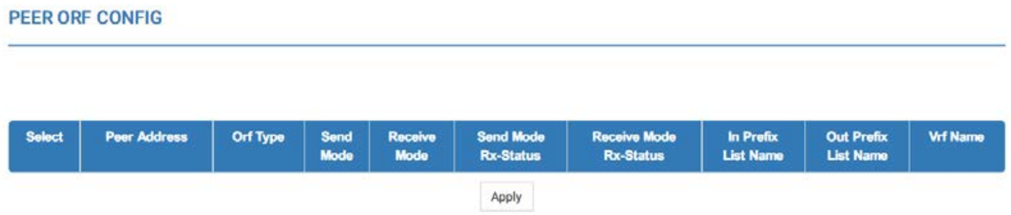
* IN - Enables Routemap for inbound routes. This applies the routemap rules for incoming routes from the peer

* OUT - Enables Routemap for outbound routes. This applies the routemap for the advertising routes to the peer.

Route Map Name - Enter the name of the Route Map to be associated with the peer. This value is a string with the maximum size as 20.

VRF Name / Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.17 Peer Orf Config



PEER ORF CONFIG

Select	Peer Address	Orf Type	Send Mode	Receive Mode	Send Mode Rx-Status	Receive Mode Rx-Status	In Prefix List Name	Out Prefix List Name	Vrf Name

Fig: Peer Orf Config

The *Peer Orf Config* link opens the **Peer Orf Config** Page.

The Peer Orf Config page allows the user to configure the peer ORF parameters of the BGP in the system.

The table below lists the fields present in this page.

Select - Select the Peer Address for which the configurations need to be reapplied.

Peer Address - The remote IP address of the BGP peer.

Orf Type - The type of the Outbound Route Filter entry.

Currently it supports only Address-Prefix based ORF type.

Send Mode - Select the ORF Send Capability supported for this peer group entry.

The list contains:

* enable - Enable ORF Send Capability

* disable - Disable ORF Send Capability

Receive Mode - Select the ORF Receive Capability supported for this peer group entry.

The list contains:

* enable - Enable ORF Receive Capability

* disable - Disable ORF Receive Capability

Send Mode Rx-Status - Displays the status whether the send capability is received from the peer or not. The possible values are:

* Received - The send capability is received

* Not Received - The send capability is not received

Receive Mode Rx-Status - Displays the status whether the receive capability is received from the peer or not. The possible values are:

* Received - The receive capability is received

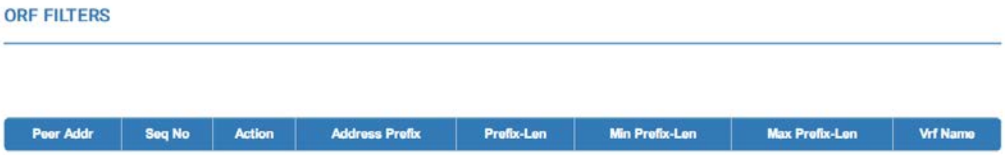
* Not Received - The receive capability is not received

In Prefix List Name - Enter the name to configure the in PrefixList for this peer group entry. This value is a string with the maximum size as 20.

Out Prefix List Name - Enter the name to configure the out PrefixList for this peer group entry. This value is a string with the maximum size as 20.

VRF Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.8.18 Orf Filters



ORF FILTERS

Peer Addr	Seq No	Action	Address Prefix	Prefix-Len	Min Prefix-Len	Max Prefix-Len	Vrf Name

Fig: Orf Filters

The *Orf Filters* link opens the **Orf Filters** Page.

The Orf Filters page shows to the user the ORF filters of the BGP in the system.

The table below lists the fields present in this page.

Peer Address - The remote IP address of the BGP peer.

Seq No - The sequential order in which a route should be matched against an ORF entry.

Action - The action to be taken for a particular route if it matches with the ORF rules defined in this particular ORF entry. The possible values are:

* Permit - the matched route will be advertised to the peer.

* Deny - the matched route will not be advertised to the peer.

Address Prefix - The IP address prefix for which the ORF rule was specified.

Prefix-Len - The length of the IP address prefix length in bits which will be considered when matching a route with the ORF entry.

Min Prefix-Len - The minimum prefix-length in bits for a IP address prefix.

Any route with prefix-length equal to or greater than this length will be considered as a match, if Max Prefix-Len is not specified.

If it is ZERO, it will be considered as unspecified and it will not be considered while applying the rule. If both Min Prefix-Len and Max Prefix-Len are specified, then a route with prefix-length with in the range of Min Prefix-Len and Max Prefix-Len will be considered as a match.

Max Prefix-Len - The maximum prefix-length in bits for a IP address prefix.

Any route with prefix-length equal to or less than this length will be considered as a match, if Min Prefix-Len is not specified. If it is ZERO, then it will be considered as unspecified and it will not be considered while applying the rule. If both Max Prefix-Len and Min Prefix-Len are specified, then a route with prefix-length with in the range of Min Prefix-Len and Max Prefix-Len will be considered as a match.

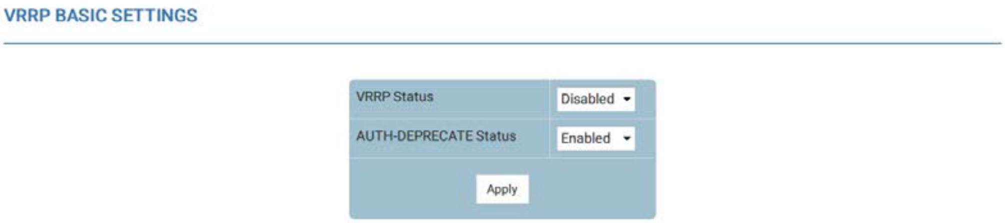
VRF Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.9 VRRP

The *VRRP* link allows you to configure the VRRP related parameters for switch. User can configure VRRP on the following 2 pages.

- Basic Settings
- VRRP Settings

5.9.1 Basic Settings



VRRP BASIC SETTINGS

VRRP Status: Disabled

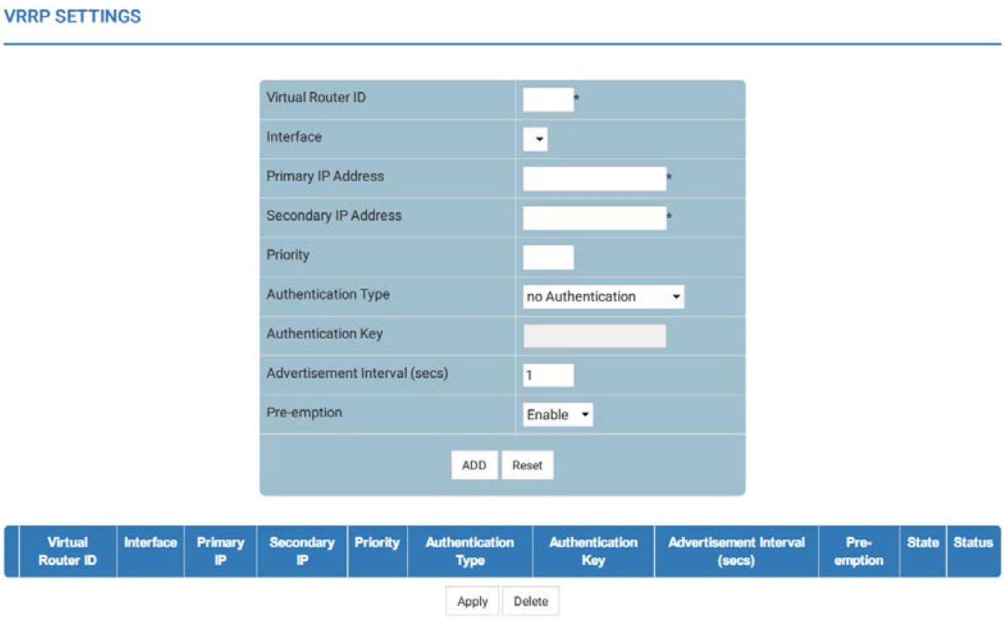
AUTH-DEPRECATE Status: Enabled

Fig: VRRP Basic Settings

The *Basic Settings* link opens the **VRRP Basic Settings** Page.
The VRRP Basic Settings page allows the user to configure the basic settings of the VRRP.

The table below lists the fields present in this page.
VRRP Status - Specifies the global status of the VRRP in the switch. The options are:
* Enabled - Enables the VRRP.
* Disabled - Disables the VRRP.
AUTH-DEPRECATE Status - Specifies the authentication status of the VRRP in the switch. The options are:
* Enabled - Enables the VRRP authentication deprecate.
* Disabled - Disables the VRRP authentication deprecate.

5.9.2 VRRP Settings



VRRP SETTINGS

Virtual Router ID	*
Interface	
Primary IP Address	*
Secondary IP Address	*
Priority	
Authentication Type	no Authentication
Authentication Key	
Advertisement Interval (secs)	1
Pre-emption	Enable

Virtual Router ID	Interface	Primary IP	Secondary IP	Priority	Authentication Type	Authentication Key	Advertisement Interval (secs)	Pre-emption	State	Status

Fig: VRRP Settings

The *VRRP Settings* link opens the **VRRP Settings** Page.

The VRRP Settings page allows the user to configure the VRRP parameters.

Don't allow to modify Authentication Type and Key in bottom form.

Please delete old entry and then create new one with Authentication Type and Key.

The table below lists the fields present in this page.

Virtual Router ID - Specifies the Virtual ID associated with each Virtual Router. This value ranges between 1 and 255.

Interface - Specifies the interface on which the Virtual Router must be configured.

Primary IP Address - Specifies the Primary IP Address for the Virtual Router. The default value is 0.0.0.0.

Secondary IP Address - Specifies the Secondary IP Address for the Virtual Router. The default value is 0.0.0.0.

Priority - Specifies the Priority to be used for the Virtual Router master election process. This value ranges between 1 and 254. The default value is 100.

Authentication Type - Specifies the Authentication Type for the Virtual Router. The options are:

* no Authentication - Does not authenticate the VRRP protocol exchanges.

* Simple Text Password - Authenticates the exchanges by a clear text password.

The default value is no Authentication.

Authentication Key - Specifies the Authentication Key for the Virtual Router. This field is an octet string with size varying between 0 and 8.

Advertisement Interval (Secs) - Specifies the time Interval, in seconds, for sending the advertisement packets. This value ranges between 1 and 255 seconds. The default value is one second.

Pre-emption - Specifies whether a higher priority virtual router will preempt a lower priority master router. The options are:

* Enable

* Disable

The default value is Enable.

State - Indicates the current state of the virtual router. This is a read-only field. The options are:

* Initialize - Indicates that all the virtual router is waiting for a startup event.

* Backup - Indicates that the virtual router is monitoring the availability of the master router.

* Master - Indicates that the virtual router is forwarding packets for IP addresses that are associated with the router.

Status Enables/disables the virtual router function. The option are:

* Up - Transits the state of the virtual router from initialize to backup or master based on the priority value.

* Down - Transits the state of the virtual router from master or backup to initialize.

The default value is Down.

5.10Filtering

The *Filtering* link allows you to configure the Filtering related parameters for switch. User can configure Filtering on the following 3 pages.

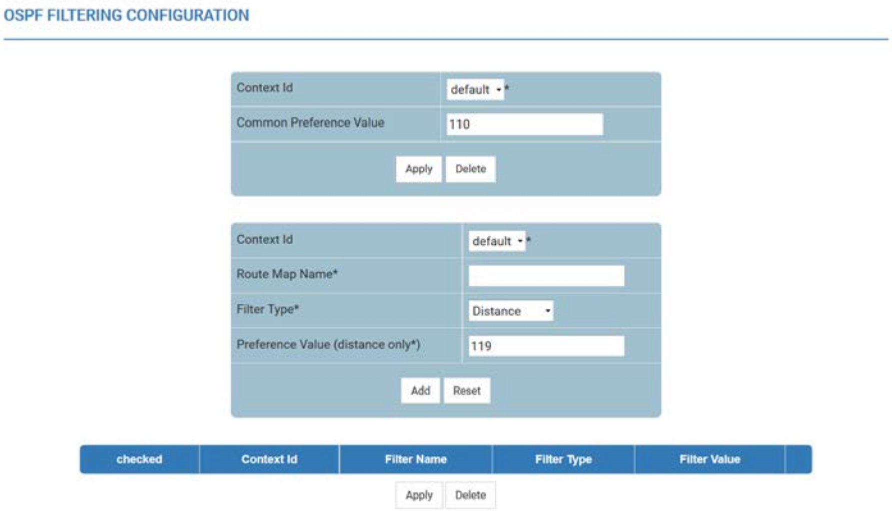
- OSPF
- RIP
- BGP

Route map in filter is used to choose distance value according to route map criteria. If none of the criteria is met then default distance is assigned.

Outgoing filter prevent the other routers from learning one or more routes by suppressing those routes from being advertised in routing updates. Route Map can be used to filter out outgoing routes by specified criteria.

To avoid processing certain routes listed in incoming updates incoming filtering is used. Route map can be used to filter out incoming routes by specified criteria. For OSPF and OSPFv3 this feature has no effect on LSA flooding.

5.10.1 OSPF



OSPF FILTERING CONFIGURATION

Context Id	default *
Common Preference Value	110

Context Id	default *
Route Map Name*	
Filter Type*	Distance
Preference Value (distance only*)	119

checked	Context Id	Filter Name	Filter Type	Filter Value

Fig: OSPF Filtering Configuration

The *OSPF* link opens the **OSPF Filtering Configuration** Page.

The OSPF Filtering Configuration page allows the user to configure the OSPF filtering for route map.

The table below lists the fields present in this page.

Context Id - Select the Context name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

Common Preference Value - Specifies the preference value for OSPF routes. This value ranges between 1 and 255.

Route Map Name* - Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Type* - Specifies the type of the route map. Options are:

* Distance **-** Specifies that the route map is for distance.

* Distribute in - Specifies that the route map is for distribute in.

By default, the route map type is Distance.

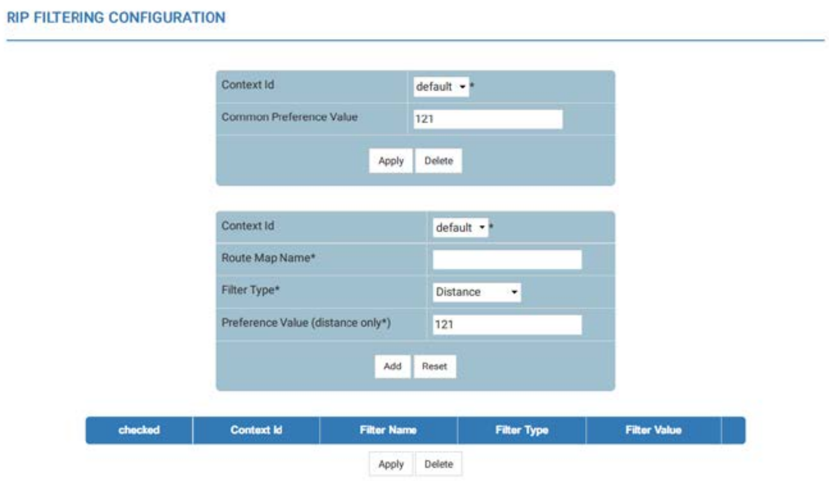
Preference Value (distance only*) - Specifies the distance value that will not be used for distribute list. This value ranges between 1 and 255. Default value is 119.

Filter Name Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Value - Specifies the distance value that will not be used for distribute list.

This value ranges between 1 and 255. Default value is 119.

5.10.2 RIP



RIP FILTERING CONFIGURATION

Context Id	default *
Common Preference Value	121

Context Id	default *
Route Map Name*	
Filter Type*	Distance
Preference Value (distance only*)	121

checked	Context Id	Filter Name	Filter Type	Filter Value

Fig: RIP Filtering Configuration

The *RIP* link opens the **RIP Filtering Configuration** Page.

The RIP Filtering Configuration page allows the user to configure the RIP filtering for route map.

The table below lists the fields present in this page.

Context Id - Select the Context name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

Common Preference Value - Specifies the preference value for RIP routes. This value ranges between 1 and 255.

Route Map Name* - Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Type* - Specifies the type of the route map. Options are:

* Distance - Specifies that the route map is for distance.

* Distribute in - Specifies that the route map is for distribute in

* Distribute out - Specifies that the route map is for distribute out.

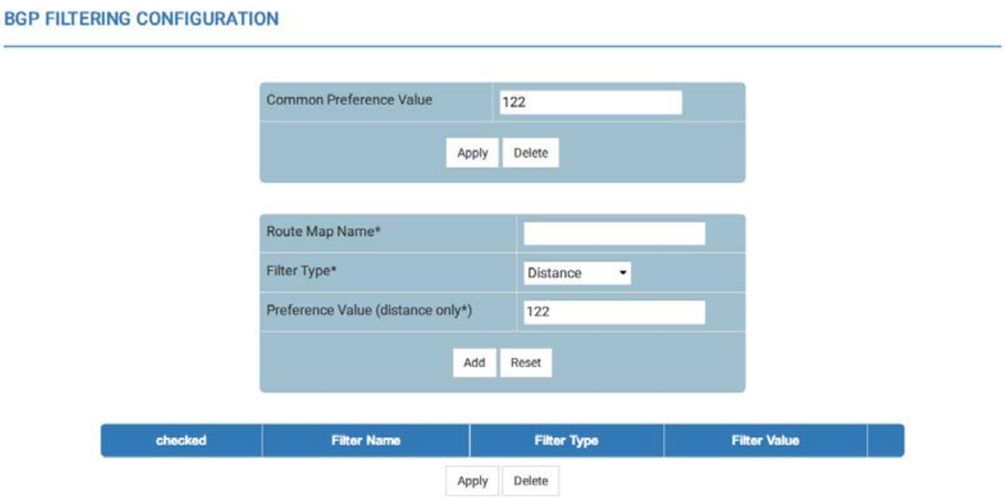
By default, the route map type is Distance.

Preference Value (distance only*) - Specifies the distance value that will not be used for distribute list. This value ranges between 1 and 255. Default value is 121.

Filter Name - Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Value - Specifies the distance value that will not be used for distribute list. This value ranges between 1 and 255. Default value is 121.

5.10.3 BGP


BGP FILTERING CONFIGURATION

Common Preference Value	122

Route Map Name*	
Filter Type*	Distance
Preference Value (distance only*)	122

checked	Filter Name	Filter Type	Filter Value

Fig: BGP Filtering Configuration

The *BGP* link opens the **BGP Filtering Configuration** Page.

The BGP Filtering Configuration page allows the user to configure the BGP filtering for route map.

The table below lists the fields present in this page.

Common Preference Value - Specifies the preference value for BGP routes. This value ranges between 1 and 255.

Route Map Name* - Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Type* - Specifies the type of the route map. Options are:

* Distance **-** Specifies that the route map is for distance.

* Distribute in - Specifies that the route map is for distribute in.

* Distribute out **-** Specifies that the route map is for distribute out.

By default, the route map type is Distance.

Preference Value (distance only*) - Specifies the distance value that will not be used for distribute list.

This value ranges between 1 and 255.

Filter Name - Specifies the name of the route map. This field is a string with size varying between 1 and 20.

Filter Value - Specifies the distance value that will not be used for distribute list.

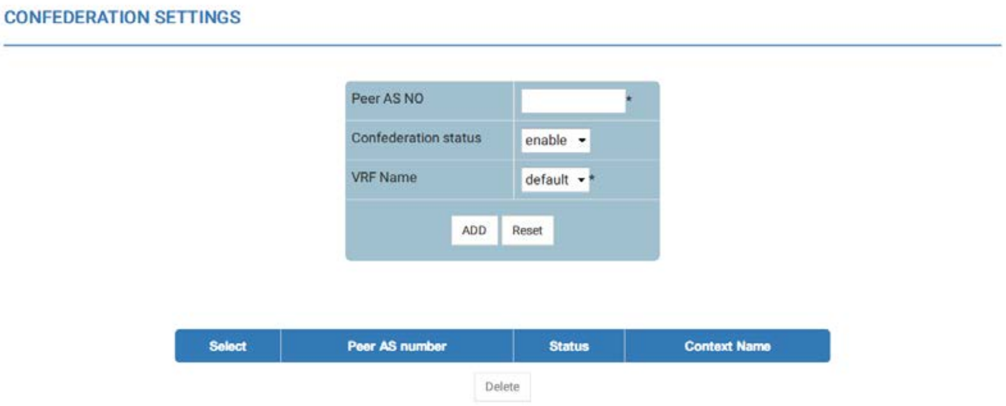
This value ranges between 1 and 255.

5.11BGP4

The *BGP4* link allows you to configure the BGP4 related parameters for switch. User can configure BGP4 on the following 8 pages.

- Confederations
- RFD
- CommFilters
- CommPolicies
- CommRoutes
- ExtCommFilters
- ExtCommPolicies
- ExtCommRoutes

5.11.1 Confederations


CONFEDERATION SETTINGS

Peer AS NO *

Confederation status: enable

VRF Name: default *

Select	Peer AS number	Status	Context Name

Fig: Confederation settings

The *Confederations* link opens the **Confederation settings** Page.

The Confederation settings page allows the user to configure the confederation status of the BGP peer for the specified VRF instance.

The table below lists the fields present in this page.

Select - Click to select the Peer AS number and delete the confederation.

Peer AS NO - Enter the peer AS number for which the confederation status needs to be configured. This value ranges between 1 and 65535.

The AS number identifies the BGP router to other routers and tags the routing information passed along.

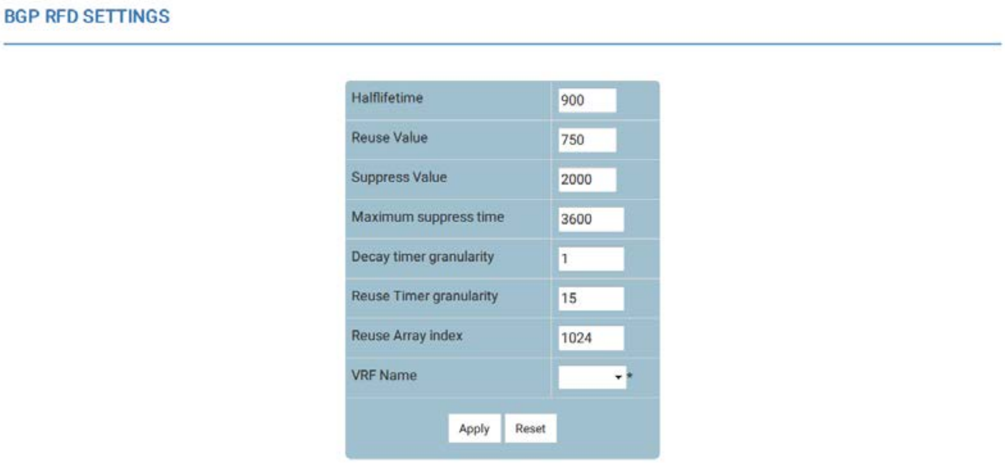
Confederation status / Status - Select the status of the BGP confederation identifier which specifies the confederation to which the autonomous systems belong to. By default Confederation status is set as enable. The list contains:

* enable - Configures the BGP confederation identifier which specifies the confederation to which the autonomous systems belong to

* disable - Deletes the configured the BGP confederation identifier

VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.2 RFD



BGP RFD SETTINGS

Halflifetime	900
Reuse Value	750
Suppress Value	2000
Maximum suppress time	3600
Decay timer granularity	1
Reuse Timer granularity	15
Reuse Array index	1024
VRF Name	*

Fig: BGP RFD Settings

The *RFD* link opens the **BGP RFD Settings** Page.

The BGP RFD Settings page allows the user to configure the RFD (Route Flap Dampening) parameters.

The table below lists the fields present in this page.

Halflifetime - Enter the time duration in seconds after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP- s route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable.. This value ranges between 600 and 2700 seconds. By default, Halflifetime is set as 900 seconds.

Reuse Value - Enter the reuse value below which the suppressed route will be reused. This value ranges between 100 and 1999. If the penalty for a flapping route falls below this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. By default, Reuse value is set as 750.

> Reuse value can be configured only if the HalfLife Time value is configured.

Suppress Value - Enter the suppress value below which the route will be suppressed. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999 seconds. By default, Suppress value is set as 2000.

> Suppress value can be configured only if the HalfLife Time and Reuse value are set.

Maximum suppress time - Enter the maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800 seconds. By default, Maximum suppress time is set as 3600 seconds.

> Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.

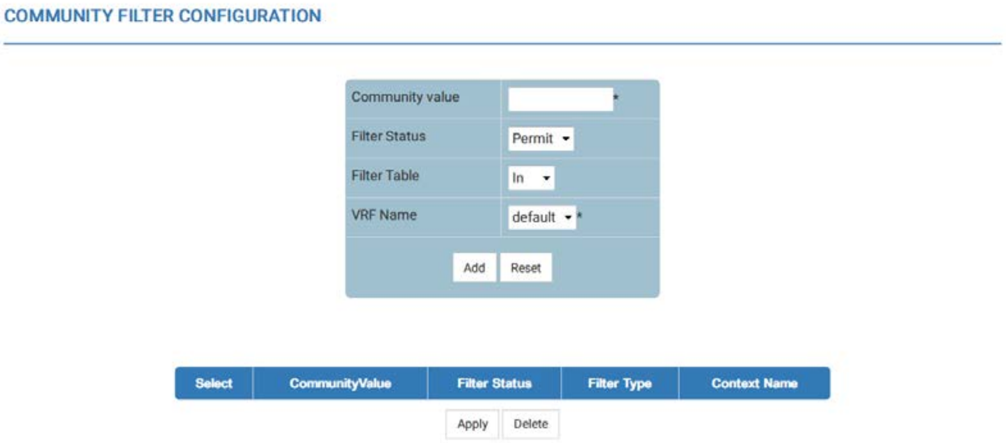
Decay timer granularity - Enter the time granularity (in seconds) to perform all decay calculations. This value ranges between 1 and 10800 seconds. By default Decay timer granularity is set as 1 second.

Reuse Timer granularity - Enter the time interval between evaluations of the reuse lists. This value ranges between 15 and 10800 seconds. By default Reuse Timer granularity is set as 15.

Reuse Array index - Enter the size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time. This value ranges between 256 and 65535. By default Reuse Array index is set as 1024.

VRF Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.3 CommFilters



COMMUNITY FILTER CONFIGURATION

Community value	*
Filter Status	Permit
Filter Table	In
VRF Name	default *

Select	CommunityValue	Filter Status	Filter Type	Context Name

Fig: Community filter configuration

The *CommFilters* link opens the **Community filter configuration** Page.

The Community filter configuration page allows the user to configure the incoming / outgoing filter status for a given community value. This filter status allows/ filters the community attribute while receiving or advertising. The rules to filter out the updates are based on the AS from which it is received, NLRI and AS through which it had passed.

The table below lists the fields present in this page.

Select - Click to select the Community value for which the filter status needs to be modified or deleted.

Community value - Enter the community value for which the incoming / outgoing filtering policy is to be updated. This value ranges between 65536 and 4294901759, or 4294967041 and 4294967043.

Filter Status Select the incoming / outgoing filtering policy for the community.

By default Filter Status is set as Permit. The list contains:

* Permit - Allows a particular community attribute to be received or advertised in updates.

* Deny - Filters the routes containing the community attribute value in received or advertised updates.

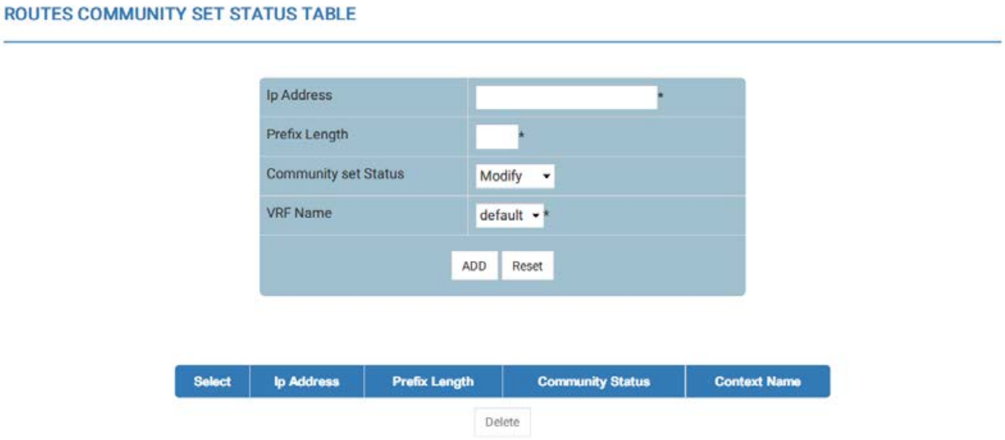
Filter Table/ Filter Type - Select to configure the incoming filter status or outgoing filter status for a given community value. By default Filter Table is set as In. The list contains:

* In - Configures the direction of route-updates on which the community filter policy needs to be applied as in. This indicates that the community filter needs to be applied on received routes

* Out - Configures the direction of route-updates on which the community filter policy needs to be applied as out. This indicates that the community filter needs to be applied on routes advertised to peers.

VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.4 CommPolicies



ROUTES COMMUNITY SET STATUS TABLE

Ip Address	*
Prefix Length	*
Community set Status	Modify
VRF Name	default *

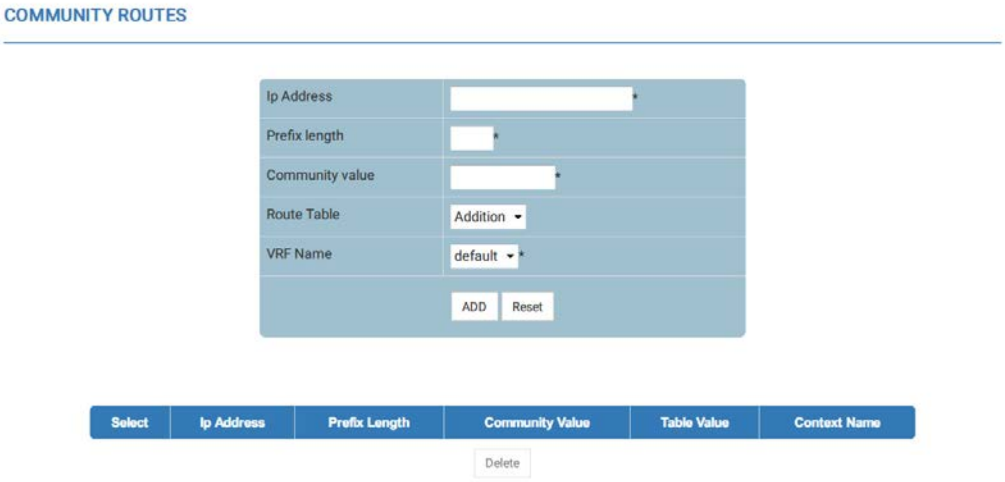
Select	Ip Address	Prefix Length	Community Status	Context Name

Fig: Routes Community Set Status Table

The *CommPolicies* link opens the **Routes Community Set Status Table** Page.
The Routes Community Set Status Table page allows the user to configure the community attribute advertisement policy for a given destination.

The table below lists the fields present in this page.
Select - Click to select the Community value for which the policy needs to be deleted.
Ip Address - Enter the IP address on which the community policy needs to be applied.
Prefix Length - Enter the IP prefix length for the destination. This IP prefix length configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
Community set Status - Select the community set status for the route. By default Community set Status is set as Modify. The list contains:
* Set **-** Sends only the configured additive communities with associated route
* SetNone **-** Sends the associated route without communities.
* Modify **-** Removes the associated route with received delete communities and adds the configured additive communities.
> This field can be set only if the local AS is configured for the BGP4.
VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.5 CommRoutes



COMMUNITY ROUTES

Ip Address	*
Prefix length	*
Community value	*
Route Table	Addition
VRF Name	default *

Select	Ip Address	Prefix Length	Community Value	Table Value	Context Name

Fig: Community Routes

The *CommRoutes* link opens the **Community Routes** Page.

The Community Routes page allows the user to configure additive / delete communities for a given destination.

The table below lists the fields present in this page.

Select - Click to select the Ip Address for which the community route needs to be deleted.

Ip Address - Enter the IP address of the destination.

Prefix length - Enter the IP prefix length for the destination. This field configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.

Community value - Enter the community value for which the additive / delete communities need to be configured. This value ranges between 65536 and 4294901759, and between 4294967041 and 4294967043.

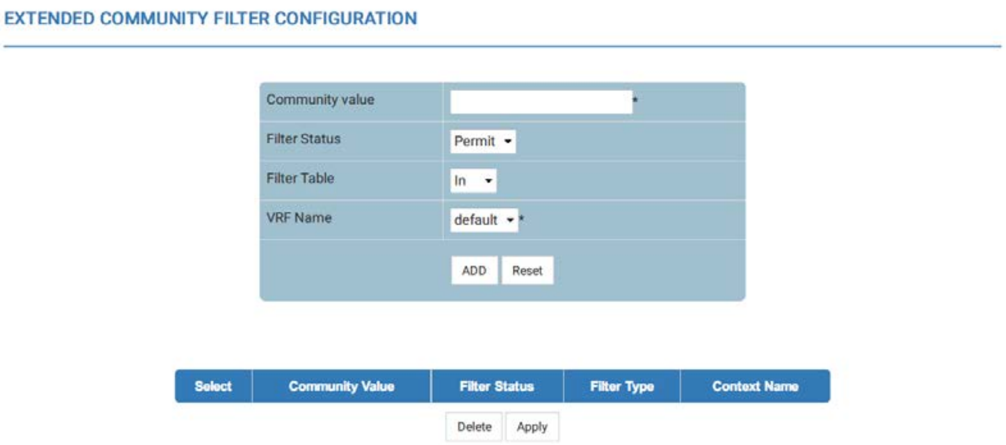
Route Table - Select to configure the additive communities or delete communities for a given destination. By default Route Table is set as Addition. The list contains:

* Addition - Adds associated community value with the already existing communities in the route update

* Deletion - Removes the community attribute from the route-prefix when it passes through the filter process

VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.6 ExtCommFilters



EXTENDED COMMUNITY FILTER CONFIGURATION

Community value	*
Filter Status	Permit
Filter Table	In
VRF Name	default *

Select	Community Value	Filter Status	Filter Type	Context Name

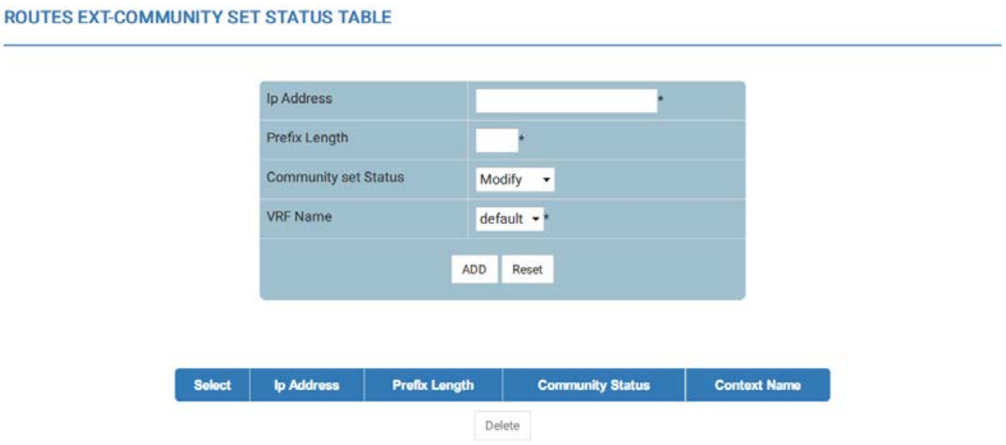
Fig: Extended Community filter configuration

The *ExtCommFilters* link opens the **Extended Community filter configuration** Page.
The Extended Community filter configuration page allows the user to configure the incoming / outgoing filter status for a given extended community value.

The table below lists the fields present in this page.
Select - Click to select the Extended Community value for which the filter status needs to be modified or deleted.
Community value - Enter the extended community value for which the input / outgoing filtering policy is to be updated. This field is an Octet string with a maximum size of 8.
Filter Status - Select the incoming / outgoing filtering policy for the extended community. By default Filter Status is set as Permit. The list contains:
* Permit - Allows a particular extended community attribute to be received or advertised in updates.
* Deny - Filters the routes containing the extended community attribute value in received or advertised updates.
Filter Table - Select to configure the incoming filter status or outgoing filter status for a given extended community value. By default Filter Table is set as In. The list contains:
* In - Configures the direction of route-updates on which the extended community filter policy needs to be applied as in. This indicates that the filter needs to be applied on received routes.
* Out - Configures the direction of route-updates on which the extended community filter policy needs to be applied as out. This indicates that the filter needs to be applied on routes advertised to peers.

VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.7 ExtCommPolicies



ROUTES EXT-COMMUNITY SET STATUS TABLE

Ip Address	*
Prefix Length	*
Community set Status	Modify
VRF Name	default *

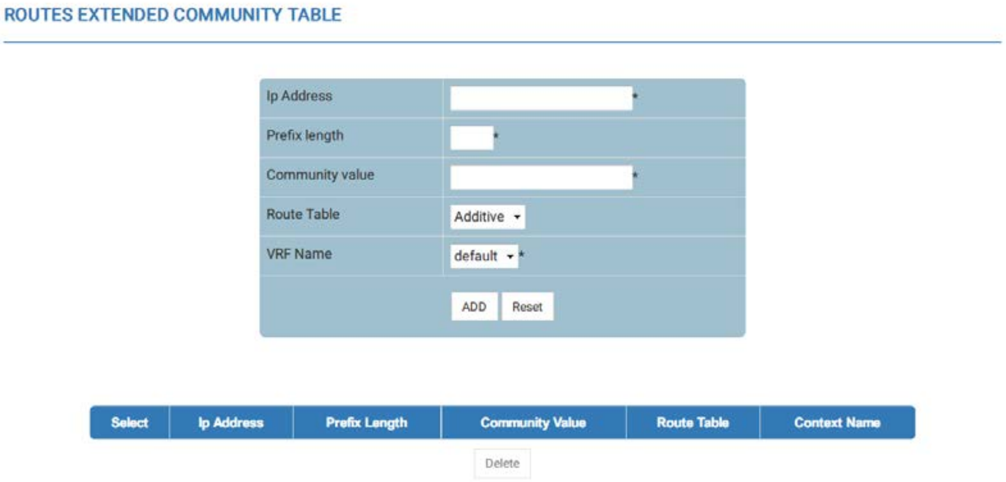
Select	Ip Address	Prefix Length	Community Status	Context Name

Fig: Routes Ext-Community Set Status Table

The *ExtCommPolicies* link opens the **Routes Ext-Community Set Status Table** Page.
The Routes Ext-Community Set Status Table page allows the user to configure the extended community attribute advertisement policy for a given destination.

The table below lists the fields present in this page.
Select - Click to select the Extended Community value for which the policy needs to be deleted.
Ip Address - Enter the destination IPv4 address
Prefix Length - Enter the IP prefix length for the destination. This field configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
Community set Status - Select the extended community set status for the route. By default Community set Status is set as Modify. The list contains:
* Set - Sends only the configured additive communities with associated route
* SetNone - Sends the associated route without communities.
* Modify - Removes the associated route with received delete communities and adds the configured additive communities
> This field can be set only if the local AS is configured for the BGP4.
VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.11.8 ExtCommRoutes



ROUTES EXTENDED COMMUNITY TABLE

Ip Address	*
Prefix length	*
Community value	*
Route Table	Additive
VRF Name	default *

Select	Ip Address	Prefix Length	Community Value	Route Table	Context Name

Fig: Routes Extended Community Table

The *ExtCommRoutes* link opens the **Routes Extended Community Table** Page.
The Routes Extended Community Table page allows the user to configure additive / delete extended communities for a given destination.

The table below lists the fields present in this page.
Select - Click to select the Ip Address for which the extended community route needs to be deleted.
Ip Address - Enter the IP address of the destination.
Prefix length - Enter the IP prefix length for the destination. This field configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
Community value - Enter the extended community value for which the additive / delete communities need to be configured. This field is an Octet string with size of 8.
Route Table - Select to configure the additive / delete extended communities for a given destination. By default Route Table is set as Additive.
The list contains:
* Additive - Adds associated extended community value with the already existing communities in the route update
* Delete - Removes the extended community attribute from the route-prefix when it passes through the filter process

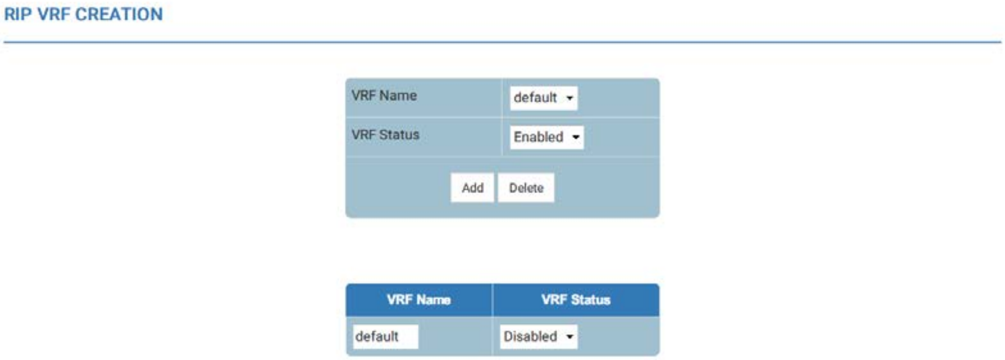
VRF Name/ Context Name - Select the VRF name from the list of instances created to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance. This value is a string with maximum size as 32.

5.12 RIP

The *RIP* link allows you to configure the RIP related parameters for switch. User can configure RIP on the following 6 pages.

- RIP VRF Creation
- Basic Settings
- Interface Configuration
- Neighbors List
- Security Settings
- Address Summary

5.12.1 RIP VRF Creation


RIP VRF CREATION

VRF Name	default
VRF Status	Enabled

VRF Name	VRF Status
default	Disabled

Fig: RIP VRF Creation

The *RIP VRF Creation* link opens the **RIP VRF Creation** Page.

The RIP VRF Creation page allows the user to enable or disable RIP for default VRF instance or a specific VRF instance.

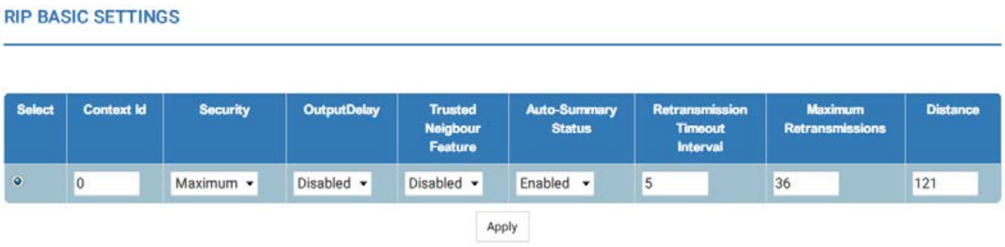
The table below lists the fields present in this page.

VRF Name - Select the VRF context name on which RIP has to be enabled or disabled. Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to co-exist within the same router at the same time.

VRF Status - Select the VRF status in the router. By default the VRF Status is set as Disabled. The list contains:

* Enabled - Enables RIP on the VRF instance to allow multiple instances of a routing table

5.12.2 Basic Settings



RIP BASIC SETTINGS

Select	Context Id	Security	OutputDelay	Trusted Neigbour Feature	Auto-Summary Status	Retransmission Timeout Interval	Maximum Retransmissions	Distance
●	0	Maximum ▾	Disabled ▾	Disabled ▾	Enabled ▾	5	36	121

Fig: RIP Basic Settings

The *Basic Settings* link opens the **RIP Basic Settings** Page.

The RIP Basic Settings page allows the user to configure the basic settings of RIP.

The table below lists the fields present in this page.

Select - Click to select the Context Id for which the RIP configurations need to be modified.

Context Id - Enter a unique value that Identifies the Rip Domain Context

Security - Select the security level of RIP in the system to accept / ignore RIPv1 packets when authentication is in use. By Default Security is set as Maximum. The list contains:

* Minimum - Sets the security status for the RIP domain context as minimum. When minimum security is set that the RIP packets will be accepted even when authentication is in use

* Maximum - Sets the security status for the RIP domain context as maximum. When maximum security is set RIP packets will be ignored when authentication is in use.

OutputDelay - Select the Output Delay status for the RIP Domain Context. By default the Output Delay value is set as Disabled. The list contains:

* Enabled - Sets Output Delay status as Enabled and enables interpacket delay for RIP updates, where the delay is in milliseconds between packets in a multiple-packet RIP update. This interpacket delay feature helps in preventing the routing table from losing information due to flow of RIP update from high speed router to low speed router

* Disabled - Sets Output delay status in the RIP Domain context as Disabled thereby disabling interpacket delay for RIP packets

Trusted Neighbour Feature - Select the Trusted neighbor feature for the RIP domain context. By default the Trusted Neighbor Feature is set as disabled. The list contains:

* Enabled - Sets the Trusted Neighbour Feature status as enabled. When enabled a list of router's IP address can be configured and RIP Packets from those router's will be processed by RIP and packets from other Routers will be dropped.

* Disabled - Sets the Trusted Neighbour Feature status as disabled. When disabled RIP Packet from all the routers will be processed.

Auto-Summary Status - Select the Auto Summary status for the RIP domain context. By default the Auto Summary Status is set as enabled. The list contains:

* Enabled - Sets the Auto Summary Status for the rip domain context as enabled. When enabled, summary routes are sent in regular updates for both rip version 1 and version 2. The summary is sent only if at least one subnet route is learned over an interface which is different from the interface over which the update is sent

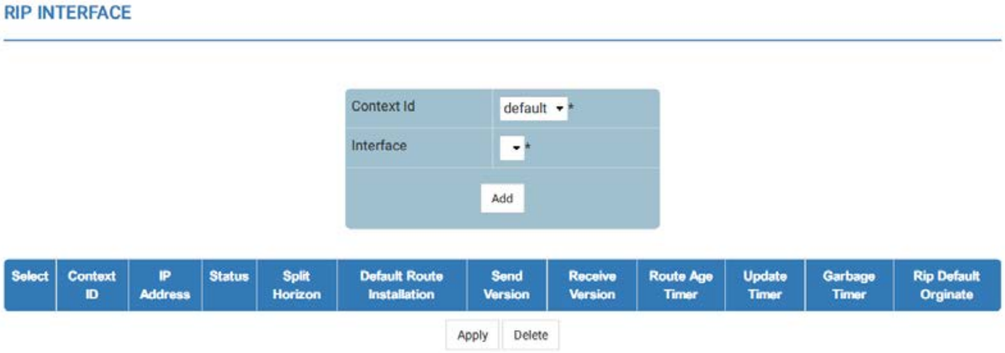
* Disabled - Sets the Auto Summary Status for the rip domain context as disabled. When disabled either individual subnet route are sent or subnet routes are sent based on the specific aggregation configured over the interface

Retransmission Timeout Interval - Enter the timeout interval to be used to retransmit the update request packet or an unacknowledged update response packet. The packets are transmitted at the specified interval till a response is received or the maximum retries. The value ranges between 5 and 10. By default the Retransmission Timeout Interval is set as 5

Maximum Retransmissions - Enter the maximum number of retransmissions of the update request and update response packets. If no response is received then the routes via the next hop router are marked unreachable. This value ranges between 10 and 40 seconds. By default the Maximum Retransmissions is set as 36

Distance - Enter the distance value for the specified context id. This value ranges between 1 and 255. By default the distance value is set as 121.

5.12.3 Interface Configuration


RIP INTERFACE

Context Id: default *

Interface: *

Select	Context ID	IP Address	Status	Split Horizon	Default Route Installation	Send Version	Receive Version	Route Age Timer	Update Timer	Garbage Timer	Rip Default Orginate

Fig: RIP Interface

The *Interface Configuration* link opens the **RIP Interface** Page.

The RIP Interface page allows the user to configure RIP on the specified interface.

The table below lists the fields present in this page.

Select - Click to select the Context Id for which the configuration needs to be modified or deleted.

Context ID - Select the Context Id from the list of VRF instances created in the system.

Interface - Select the Interface ID for which the RIP parameters need to be configured.

IP Address - Displays the IP address of the RIP interface. This is a read-only field.

Status - Select the administrative status of the RIP-2 in the router. By default, the status is set as Enabled. The list contains:

* Enabled - Activates RIP2 process throughout the system.

* Disabled - Disables RIP2 process in the system.

* Passive - Runs RIP2 process as a passive one.

Split Horizon - Select the operational status of Split Horizon in the system. By default the Split horizon value is set as Poisson Reverse. The options are:

* Split Horizon - Enables the split horizon updates for the RIP which prevents the routing loops in distance routing protocol, by prohibiting the router from advertising a route back onto the interface. The split horizon updates are applied in the response packets sent.

* Poisson Reverse - Enables the poisson updates for the RIP which sends route with the metric value 16 on an interface from which route is learnt.

* Disabled - Disables Split horizon updates for the RIP which sends route on all the interfaces with the metric same as that in the RIP Routing Table.

Default Route Installation - Select the Default Route Installation status in the RIP Interface. By default the Default Route Installation is set as No. The list contains:

* Yes - Enables Default Route Installation which installs the default route received in updates to the RIP database.

* No - Disables Default Route Installation which blocks the installation of default route received in updates to the RIP database.

Send Version - Select the version of RIP packets that will be sent by the router. By default Send version value is set as RIP1 Compatible. The list contains:

* Do not send - Stops the IP RIP transmitting advertisements to be sent on a VLAN interface / router port

* RIP Version1 - Sends only RIP updates compliant with RFC 1058, on the interface.

* RIP1 Compatible - Sends both multicasting RIP updates and RIP updates compliant with RFC 1058, on the interface.

* RIP Version2 - Sends only multicasting RIP updates on the interface.

Receive Version - Select the version of RIP updates to be received. By default Receive version value is set as RIP1 or RIP2. The list contains:

* RIP1 - Receives only RIP updates compliant with RFC 1058, on the interface.

* RIP2 - Receives only multicasting RIP updates on the interface.

* RIP1 or RIP2 - Receives both multicasting RIP updates and RIP updates compliant with RFC 1058, on the interface.

* Do not receive - Sets that no IP RIP transmitting advertisements are received on a VLAN interface / router port

Route Age Timer - Enter the time (in seconds) after which the route entry is put into garbage collect (marked as invalid). The value ranges between 30 and 500 seconds.

By default, Route Age Timer is set as 180 seconds.

Update Timer - Enter the time interval (in seconds) at which the RIP updates should be sent. This is the fundamental timing parameter of the routing protocol. The value ranges between 10 and 3600 seconds.

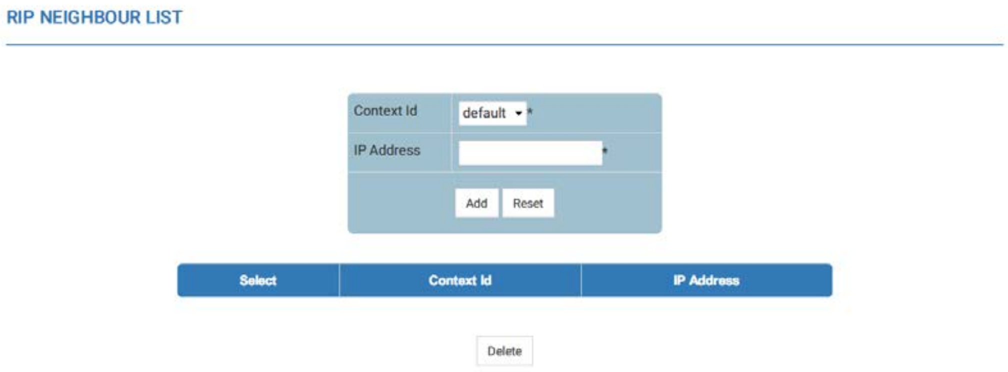
By Default Update Timer is set as 30 seconds.

Garbage Timer - Enter the time (in seconds) after which the route entry marked as invalid is deleted. The advertisement of this entry is set to INFINITY while sending to others. The value ranges between 120 and 180 seconds

By default Garbage timer is set as 120 seconds.

Rip Default Originate - Enter the metric to be used for default route propagated over the VLAN interface / router port in a RIP update message and generates a default route into RIP. This value ranges between 0 and 15. By Default, the RIP Default Originate value is set as 0 which implies that origination of default route over the interface is disabled.

5.12.4 Neighbors List


RIP NEIGHBOUR LIST

Context Id: default *

IP Address: *

Select	Context Id	IP Address

Fig: RIP Neighbour List

The *Neighbors List* link opens the **RIP Neighbour List** Page.

The RIP Neighbour List page allows the user to add a trusted neighbor router with which routing information can be exchanged and from which RIP packets can be accepted. This permits the point-to-point (nonbroadcast) exchange of routing information. When used in combination with the passive-interface vlan, routing information can be exchanged between a subset of routers and access servers. On a LAN multiple neighbor ip addresses can be used to specify additional neighbors or peers.

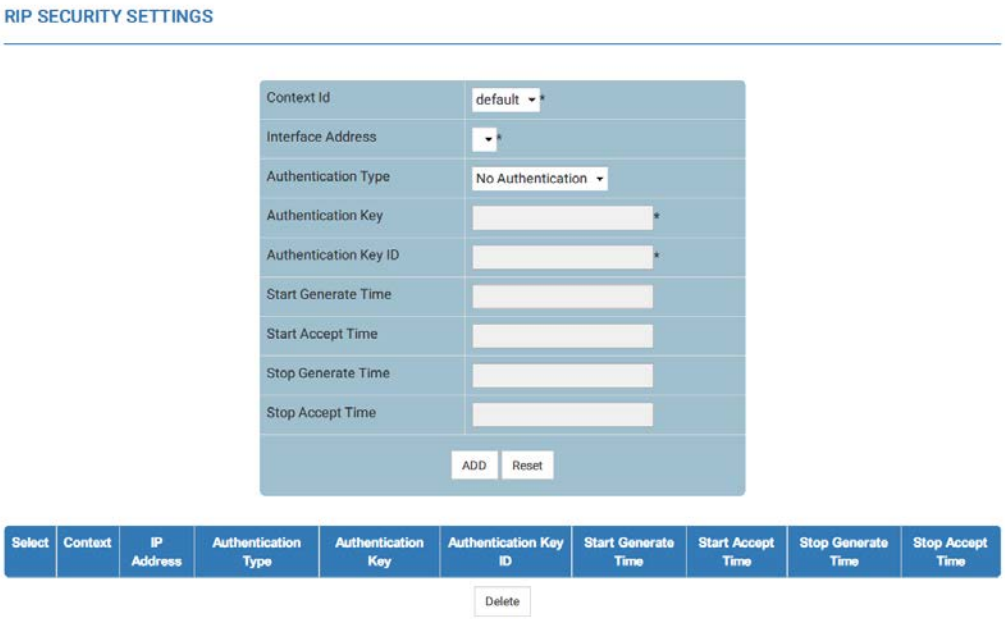
The table below lists the fields present in this page.

Select - Click to select the Context Id for which the neighbor router needs to be deleted.

Context ID - Select the Context ID from the list of VRF instances created in the system to add a trusted neighbor.

IP Address - Enter the IP Address of the neighbor router from which this router can accept RIP packets.

5.12.5 Security Settings



RIP SECURITY SETTINGS

Context Id	default *
Interface Address	*
Authentication Type	No Authentication
Authentication Key	*
Authentication Key ID	*
Start Generate Time	
Start Accept Time	
Stop Generate Time	
Stop Accept Time	

Select	Context	IP Address	Authentication Type	Authentication Key	Authentication Key ID	Start Generate Time	Start Accept Time	Stop Generate Time	Stop Accept Time

Fig: RIP Security Settings

The *Security Settings* link opens the **RIP Security Settings** Page.

The RIP Security Settings page allows the user to configure the type of authentication that is used on the interface.

The table below lists the fields present in this page.

Select - Click to select the IP Address for which the configuration needs to be modified or deleted.

Context ID - Select the Context ID from the list of VRF instances created in the system to configure the security settings.

Interface Address - Select the required Interface from the list of interfaces for which crypto authentication parameters are to be configured.

Authentication Type - Select the type of authentication used on the interface. The list contains:

* No Authentication - Disables authentication when No Authentication is set.

* Simple Password - Sets the authentication type as simple text.

* MD5 - Sets the authentication type as keyed MD5 (Message Digest 5) authentication.

* SHA -1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.

* SHA-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA 256) authentication. SHA 256 generates Authentication digest of length 32 bytes.

* SHA-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.

* SHA- 512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.

By default, Authentication Type is set as No Authentication.

Authentication Key - Enter the key - value to be used as the authentication key. If a string shorter than 16 octets is supplied, it will be left- justified and padded to 16 octets, on the right, with nulls (0x00).

> This field is greyed out if the Authentication type is selected as No Authentication.

Authentication Key ID - Enter the active authentication KeyID currently used in the particular interface for sending RIP updates. This value ranges between 0 and 255.

> This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

Start Generate Time   Enter the time that the router will start using this key for packet generation. If the value is not set, then it will be taken as infinite and displayed as 2136-02-06,06:28:15.

> For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as, 1992-5-26,13:30:15.0

> This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

Start Accept Time - Enter the time that the router will start accepting packets that have been created with this key. If the value is not set, then it will be taken as infinite and displayed as 2136-02-06,06:28:15For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992-5-26,13:30:15

> This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

Stop Generate Time - Enter the time that the router will stop using this key for packets generation. If the value is not set, then it will be taken as infinite and displayed as 2136-02-06,06:28:15.

> For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as, 1992-5-26,13:30:15.0

> Stop Generate time should be later than the Start Generate time.

> This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

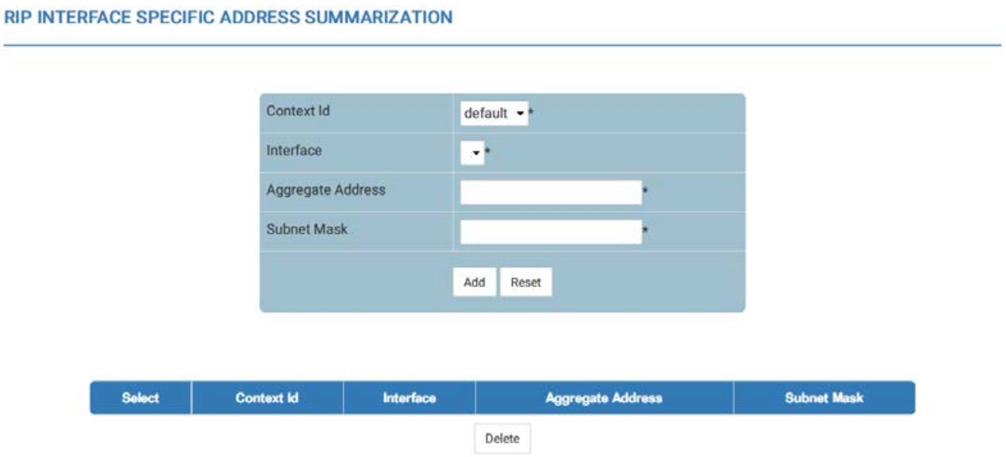
Stop Accept Time - Enter the time that the router will stop accepting packets that have been created with this key. If the value is not set, then it will be taken as infinite and displayed as 2136-02-06,06:28:15.

> For example, Tuesday May 26, 1992 at 1:30:15 PM should be configured as, 1992-5-26,13:30:15.0

> Stop Accept time should be later than the Start Accept time.

> This field is greyed out if the Authentication type is selected as No Authentication or Simple Password.

5.12.6 Address Summary


RIP INTERFACE SPECIFIC ADDRESS SUMMARIZATION

Context Id: default *

Fig: RIP Interface Specific Address Summarization

The *Address Summary* link opens the **RIP Interface Specific Address Summarization** Page. The RIP Interface Specific Address Summarization page allows the user to set route aggregation over a VLAN interface / router port for all subnet routes that falls under the specified IP address and mask.

The table below lists the fields present in this page.

Select - Click to select the Context Id for which the summary address is to be deleted.

Context Id - Select the Context ID from the list of VRF instances created in the system to configure the summary address.

Interface - Select the Interface ID from the list of VLAN interfaces created in the system to configure the summary address.

Aggregate Address - Enter the IP address that is to be combined with the subnet mask to set route aggregation for all subnet routes that fall under the specified IP address and mask of the interface specific aggregation

Subnet Mask - Enter the subnet mask that is to be combined with the IP address to set route aggregation for all subnet routes that fall under the specified mask and IP address of the interface specific aggregation

6 Multicast

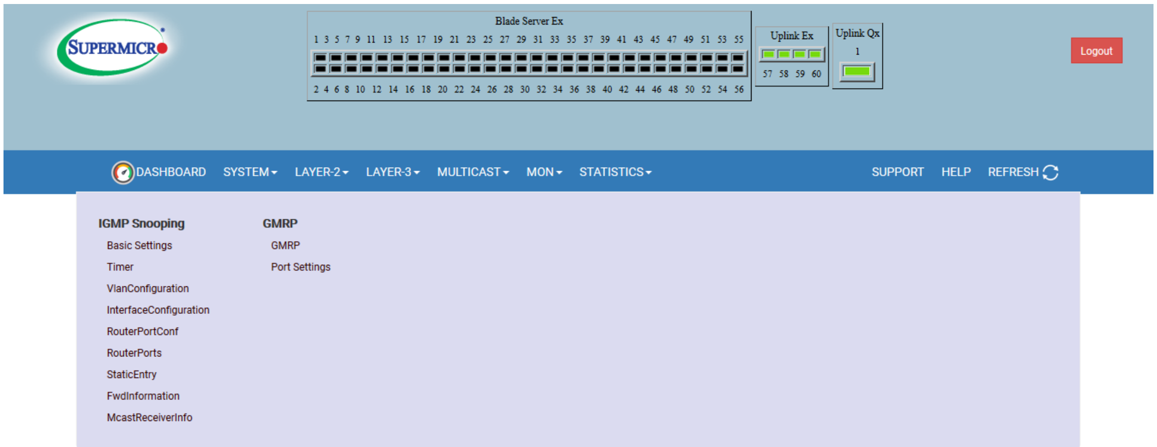


Fig: System Management

Multicast covers the following features of the switch.

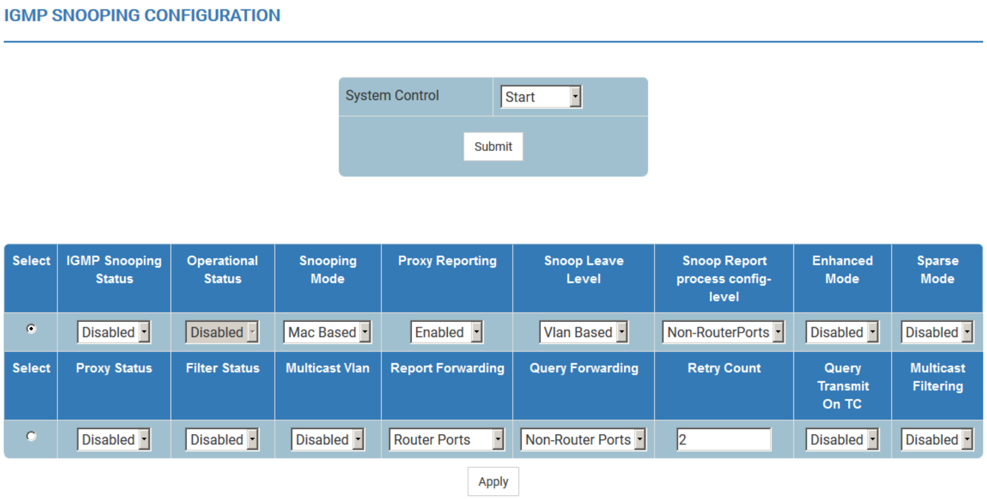
- IGMP Snooping
- GMRP

6.1 IGMP Snooping

The *IGMP Snooping* link allows you to configure the IGMP Snooping for switch. User can configure IGMP Snooping on the following 9 pages.

- Basic Settings
- Timer
- vlanConfiguration
- InterfaceConfiguration
- RouterPortConf
- RouterPorts
- StaticEntry
- FwdInformation
- McastReceiverInfo

6.1.1 Basic Settings



IGMP SNOOPING CONFIGURATION

System Control	Start

Submit

Select	IGMP Snooping Status	Operational Status	Snooping Mode	Proxy Reporting	Snoop Leave Level	Snoop Report process config-level	Enhanced Mode	Sparse Mode
●	Disabled	Disabled	Mac Based	Enabled	Vlan Based	Non-RouterPorts	Disabled	Disabled
Select	Proxy Status	Filter Status	Multicast Vlan	Report Forwarding	Query Forwarding	Retry Count	Query Transmit On TC	Multicast Filtering
○	Disabled	Disabled	Disabled	Router Ports	Non-Router Ports	2	Disabled	Disabled

Apply

Fig: IGMP Snooping Configuration

This page allows the user to configure basic settings such as IGMP snooping status, operational status, Snooping Mode, Proxy Reporting and Snoop Leave level.

The fields in second row of the form at the bottom can be modified by clicking on the select option in the second row. To configure IGS, GMRP status must be disabled.

Select - Select the option button to configure the selected parameters

System Control - Select the System Control status of IGS in the switch.

By default, the System Control status is Start. The list contains:

* Start - Starts the IGMP snooping protocol and allocates the resources required by the IGS module. During protocol start-up, it creates semaphore, RBTree, hash table and also initializes the timer task.

* Shutdown - All the resources are released back to the system and the module stops running. All the timers are stopped. The RBTree and hash Table and the allocated memory pools are deleted.

Click Submit to configure system control.

IGMP Snooping Status - Select the Global status of IGS in the switch.

By default, IGS global status is Disabled. The list contains:

* Enabled - Starts the IGMP snooping protocol operations.

* Disabled - Stops performing the IGMP snooping protocol operations.

Operational Status - Displays the Operational status of the IGS in the switch.

By default, IGS is disabled globally. The list contains:

* Enabled - Indicates that IGS protocol is currently enabled in the system.

* Disabled - Indicates that IGS protocol is currently disabled in the system.

Snooping Mode - Select the IGMP snooping mode. Modes are provided with redundancy support.

By default, snooping mode is set as MAC Based. The list contains:

* IP based - IGS protocol operation is based on the IP address and group address. This mode is chosen if the hardware supports programming of S, G and *, and G entries

* MAC based - Hardware supports only MAC based multicast tables and the snooping protocol operation is based only on the group address.

Proxy Reporting - Select the Proxy Reporting status in the switch. IGS network traffic gets reduced.

By default, Proxy-reporting status is Enabled in the system. The list contains:

* Enabled - Switch generates reports and forwards them to the router, based on the available host information.

* Disabled - Switch acts as transparent snooping bridge. The switch forwards all v3 reports and a single v2 report to the router.

Snoop Leave Level - Select the leave processing mechanism to be implemented at the VLAN level or at port level. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group.

By default, Snoop leave level is Vlan Based. The list contains:

* Vlan Based - Configures the leave mechanism at the VLAN level. In Vlan based leave processing mode, the fast leave functionality configurable per VLAN or normal leave configurations are available for processing leave messages.

* Port Based - Configures the leave mechanism at port level. In port based leave processing mode, the explicit host tracking functionality, the fast leave functionality or normal leave configurable on a interface can be used for processing the leave messages.

Snoop report Process Config Level - Select the report processing mechanism to be used for handling the incoming report messages to be processed.

By default, the value is set as Non-RouterPorts. The list contains:

* Non-RouterPorts - The incoming report messages are processed only in the non-router ports. Report message received on the router ports are not processed.

* All-Ports - The incoming report messages are processed in all the ports inclusive of router ports.

Enhanced Mode - Select the operating status of snooping module. By default, Enhanced mode is Disabled. The list contains:

* Enabled - The snooping module operates in enhanced mode. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning

Multicast group entries based on the Port and Inner Vlan. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating Multicast traffic. The module multicasts from an Outer VLAN (SVLAN) to a set of ports & Inner VLANs (CVLAN). In this mode, an S-tagged multicast data or query packet from one port can result in multiple copies of the packet on the same egress port, each with a different C-tag. The Inner VLAN (CVLAN) will typically have a valid value within the designated range.

* Disabled - The snooping module operates in default mode. This mode of operation is applied when downstream device is capable of performing duplication of Multicast traffic. In the this mode, the module multicasts from an Outer VLAN (SVLAN) to a set of ports. The Inner VLAN (CVLAN) will typically have a value of zero. In this mode, an S-tagged multicast data or query packet from one port can result in multiple packets on separate egress ports, but only one packet on any one egress port with an S-tag or with no tag.

> Enhanced mode is in enabled state only when the snooping mode is set as IP Based

Sparse Mode - Select whether the snooping module operates in the sparse mode or non-sparse mode. This option is to select whether the unknown multicast traffic should be dropped or flooded when there is no interested listener. By default, Sparse mode is disabled. The list contains:

* Enabled - The IGS module drops the unknown multicast traffic when there is no listener for the multicast data

* Disabled - The IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of VLAN.

Sparse mode is in enabled state, only when the snooping mode is set as IP Based.

Proxy Status - Select the status of the Proxy in the system. In proxy mode all the reports and queries generated by the switch will be having the switch IP as the source IP. The list contains:

* Enabled - Enables proxy in the system. The switch act as querier for all downstream interfaces and act as host for all upstream interfaces.

* Disabled - Disables proxy in the system.

> Proxy status can be enabled only if Proxy-reporting is disabled

Filter Status - Select the filter status.

By default, Filter Status is Disabled. The list contains:

* Enabled - Enables the IGS filtering feature. The channel registration is restricted from addition to the database if it is to be filtered. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream.

* Disabled - Disbales the IGS filtering feature. All filter related configurations are allowed but the incoming report will not be subjected to the filter process. IGS module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface.

Multicast Vlan - Select the multicast VLAN status.

Multicast VLAN feature can be used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through other/different VLANs. By default, Multicast VLAN Status is Disabled. The list contains:

* Enabled - Enables the mutlicast Vlan feature. Router sends a single copy of the data for the particular MVLAN, instead of forwarding a separate copy of the multicast data to each VLAN. This saves the network bandwidth.

* Disabled - Disables the multicast Vlan feature. A separate copy of the multicast data has to be forwarded from the router in the absence of M-VLAN.

Report Forwarding - Select whether the report must be forwarded on all ports or only on router ports.

The port which receives the query message from the router is the Router port. By default, Router Ports is selected. The list contains:

* Router Ports - Forwards reports only on the router ports

* All Ports - Forwards reports on all ports of the VLAN

* Non-edge - Forwards the reports on non edge ports detected by spanning tree protocol

Query Forwarding - Select whether the query to be forwarded to the entire member ports of the VLAN or to Non-router Ports. By default, the query forwarding is set as Non-Router Ports. The list contains:

* All Ports - The query messages are forwarded to all the member ports of the VLAN.

* Non-Router Ports - The query messages are forwarded only to the non-router ports.

Retry Count - Enter the maximum number of group specific queries sent on a port on reception of an IGMPv2 leave message.

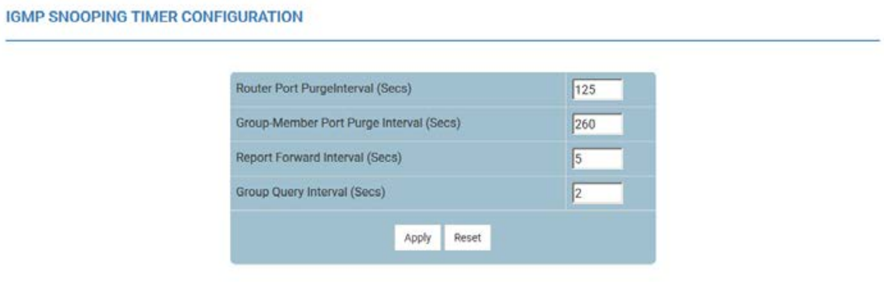
This values ranges between 1 and 5. Default value is 2.

> When the switch receives leave message on a port, it sends group specific query to check if there are any other interested receivers for the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the maximum retry count exceeds the RetryCount, then the port will be deleted from the multicast group membership information in the forwarding database and received leave message will be forwarded onto the router ports if there are no interested receivers for the group.

Query Transmit on TC - Select path redundancy for IGMP Snooping queries transmission to be enabled or disabled whenever topology changes. By default query transmit on TC is disabled. The list contains:

* Enabled- Provides path redundancy while preventing undesirable loops in the network. When enabled allows the path to exchange information so that only one of them will handle a given message that is being sent between two computers within the network.
* Disabled- Path redundancy is disabled and it leads to flooding of data.

6.1.2 Timer



IGMP SNOOPING TIMER CONFIGURATION

Router Port PurgeInterval (Secs)	125
Group-Member Port Purge Interval (Secs)	260
Report Forward Interval (Secs)	5
Group Query Interval (Secs)	2

Fig: IGMP Snooping Timer Configuration

This page allows the user to set Router port purge interval, Group-Member Port Purge Interval, Report Forward Interval and Group Query Interval.

Router Port Purge Interval(Secs) - Enter the time interval after which the learnt router port will be purged. This option is to determine the aliveness of router ports

This value ranges between 60 and 600 seconds. Default value is 125 seconds.

> For each router port learnt, the timer runs for the configured port purge time interval. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted.

Group-Member Port Purge Interval(Secs) - Enter the time interval after which a learnt port entry is purged, if IGMP reports are not received on a port.

This value ranges between 130 and 1225 seconds. Default value is 260 seconds.

> For each port on which report has been received, this timer runs for the configured time. This timer will be restarted whenever a report message is received from a host on the specific port. If the timer expires, then, the learnt port entry will be purged from the multicast group.

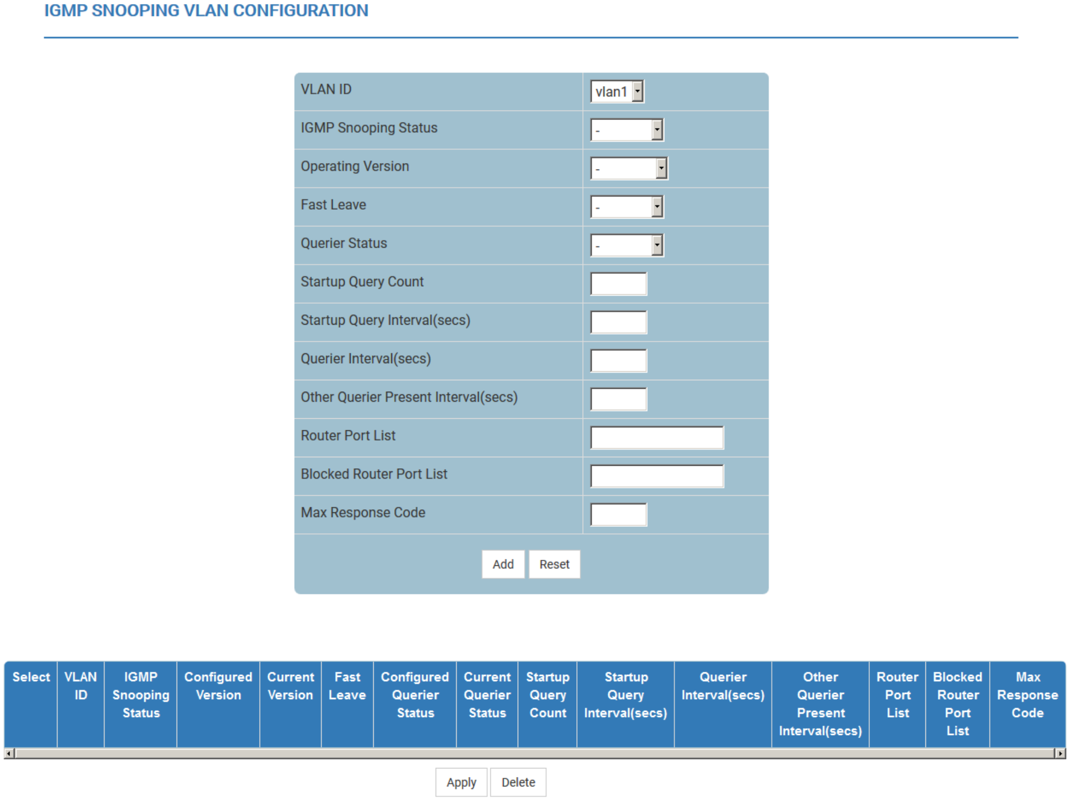
Report Forward Interval(Secs) - Enter the time interval within which the next report messages for the same multicast group will not be forwarded. This timer is used when both proxy and proxy-reporting is disabled. This option is to perform Join Aggregation of IGMP membership report. This value ranges between 1 and 25 seconds. Default value is 5 seconds.

> This is the interval (in seconds) within which report messages for the same multicast group will not be forwarded. The Report Forward Timer is per multicast group. This timer is started as soon as a report message for that group is forwarded out. Within this ReportForwardInterval if another report for the same group arrives, then that report will not be forwarded

Group Query Interval(Secs) - Enter the interval value in which the snooping switch waits for the membership reports from the interested receivers for the given multicast group after sending out query messages.

This value ranges between two and five seconds. Default value is 2 seconds.

6.1.3 VlanConfiguration



IGMP SNOOPING VLAN CONFIGURATION

VLAN ID	vlan1
IGMP Snooping Status	-
Operating Version	-
Fast Leave	-
Querier Status	-
Startup Query Count	
Startup Query Interval(secs)	
Querier Interval(secs)	
Other Querier Present Interval(secs)	
Router Port List	
Blocked Router Port List	
Max Response Code	

Select	VLAN ID	IGMP Snooping Status	Configured Version	Current Version	Fast Leave	Configured Querier Status	Current Querier Status	Startup Query Count	Startup Query Interval(secs)	Querier Interval(secs)	Other Querier Present Interval(secs)	Router Port List	Blocked Router Port List	Max Response Code

Fig: VlanConfiguration

This page allows the user to configure IGMP Snooping on specific VLANs.

VLAN ID - Select the VLAN Identifier that uniquely identifies a specific VLAN. The IGMP snooping configuration is performed for this specific VLAN ID.

IGMP Snooping Status - Select the status of IGMP snooping on the specified VLAN. By default, IGS is enabled after adding the IGMP snooping VLAN. The list contains:

* Enabled - IGS is enabled on the specified VLAN. A switch will listen for IGMP messages from the host connected on those interfaces and build the software. This ensures that only the ports that require a given multicast stream actually receive it.

* Disabled - IGS is disabled on the specified VLAN.

Operating Version - Select the Operating Version of IGS for the specified VLAN. Default operating mode on a VLAN is IGMP Version 3. The list contains:

* Version 1 - The port list connected to listeners of Multicast groups is built based on IGMP membership Reports, Query and Leave messages

* Version 2 - The port list connected to listeners of Multicast groups is built based on IGMP membership Reports, Query and Leave messages, added support for low leave latency, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any member of a particular group present on an attached network.

* Version 3 - The port list is based on source filtering information sent by IGMPv3 hosts in their membership reports to build Source specific Multicast groups. Support for source filtering, that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from other than specific source addresses, sent to a particular multicast address.

Fast Leave - Select the Fast Leave status of IGS. By default, Fast Leave status is disabled. The list contains:

* Enabled - On receipt of a single leave message, the port information is immediately removed from the multicast group entry. The switch immediately removes the port from the forwarding table without sending a group specific query. The fast leave functionality does not verify if other interested receivers are still present for the multicast group on the same port.

* Disabled - Normal leave functionality gets enabled The switch checks if there are any interested receivers for the group by sending a group specific query before removing the port from the forwarding table.

Querier Status - Select whether the switch is configured as a querier in a VLAN. By default, VLAN querier is Disabled. The list contains:

* Enabled - The switch starts acting as a querier and sends query messages until it receives best querier information. The switch sends general queries at regular time intervals. This querier message takes part in querier election.

* Disabled - The switch is configured as non-querier, does not propagate any general query messages and does not take part in querier election.

Startup Query Count - Enter the number of queries to be sent during startup of querier election process at the interval of startup query interval.

This value ranges between two and five. Default value is 2.

Startup Query Interval(secs) - Enter the interval (in seconds) between the startup general query messages sent by the switch (querier) during the startup of querier election process. This value ranges between 15 to 150 seconds. Default value is 31 seconds. This value should be less than or equal to one fourth of query interval value configured for the VLAN.

Querier Interval (secs) - Enter the time period between which the general queries are sent by IGMP snooping, when the switch is configured as querier on a VLAN. The switch waits for the configured time period after sending a general query message. On the expiry of this query interval, the switch again sends the general query message and restarts the timer. This value range between 60 and 600 seconds. Default value is 125 seconds.

Other Querier Present Interval(secs) - Enter the time period (in seconds) that must pass before a multicast router decides that there is no longer another multicast router which should be the querier. This value ranges between 120 to 1215 seconds. Default value is 255 seconds.

* This value must be ((Robustness Variable * Query Interval) + (QueryResponse Interval/2)).

* The Robustness Variable tunes IGMP to expected losses on a link. IGMPv3 is robust to (Robustness Variable - 1) packet losses.

Router Port List - Enter the static Router port list for VLAN. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port and is added in the router port list. By default, Router Port list is set to None.

Blocked Router Port List - Enter the list of ports which are configured statically as blocked router ports. On a blocked router port the software discards queries, PIM/DVMRP and Data Messages and prevents the port from ever becoming a router port. The blocked router port feature does not involve any hardware programming. Multicast data is dropped on a blocked router port. Reports are not forwarded to a blocked router port. Reports coming from blocked router port are not processed. By default, Blocked Router Port list is set to None. A port cannot be configured as blocked router port, if it is already configured as static router port

Max Response Code - Enter the maximum response code advertised in queries which are sent over this VLAN. The value ranges between 0 and 255 tenths of a second. Default value is 100.

Configured Version - Displays the configured IGMP version on the given VLAN. Options are version 1, version 2 and version 3.

Current Version - Displays the working IGMP Version on the given VLAN. The value can be version 1, version 2 or version 3.

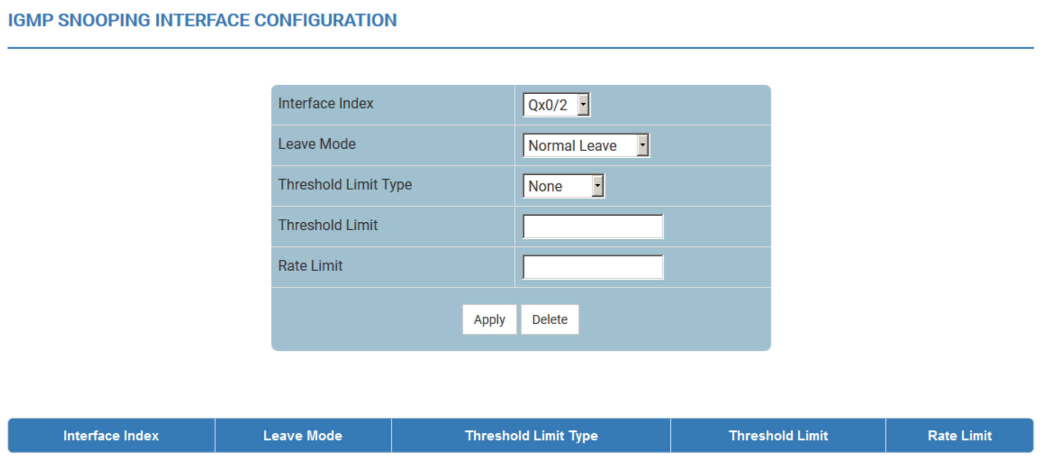
Configured Querier Status - Select the configured querier status in the VLAN. By default the configured querier status is disabled. The list contains:

* Enabled - The switch is acting as a querier and sending query messages until it receives best querier information. The switch sends general queries at regular time intervals. This querier message takes part in querier election.

* Disabled - The switch is configured as non-querier, does not propagate any general query messages and does not take part in querier election.

Current Querier Status - Displays the current querier status in the VLAN. The value can be enabled or disabled.

6.1.4 InterfaceConfiguration



IGMP SNOOPING INTERFACE CONFIGURATION

Interface Index	Qx0/2
Leave Mode	Normal Leave
Threshold Limit Type	None
Threshold Limit	
Rate Limit	

Interface Index	Leave Mode	Threshold Limit Type	Threshold Limit	Rate Limit

Fig: IGMP Snooping Interface Configuration

This page allows the user to configure IGMP Snooping on specific interface.

Interface Index - Select the interface index of the port.

Leave Mode - Select the mechanism to be used for processing leave messages in the downstream interface. Options are:

* Explicit Tracking **-** Leave messages are processed using the explicit tracking mechanism. On receipt of the leave message, the switch uses its learnt database to determine whether the specified multicast group has a single receiver or multiple receivers attached to the port. The switch removes the port from the multicast group entry only when no other receivers are present in the same group.

* Fast Leave **-** Leave messages are processed using the fast leave mechanism. On receipt of a single leave message the port is immediately removed from the group entry. The fast leave functionality does not verify if other interested receivers are still present in the multicast group on the same port. Hence the feature can be used effectively only in a point-to-point connection

* Normal Leave - A group or group specific query is sent on the interface when a leave message is received. Once snooping switch sends the leave message for a multicast group, the snooping switch sends out query messages and waits for a specified time for the membership reports from the interested receivers for the given multicast group.

By default, Leave Mode is Normal Leave This field can be configured only when the Snoop Leave Level is set to Port Based.

Threshold Limit Type - Select the type of limit to be applied for the interface. The threshold limit will be applied when reports are received from the downstream interface. Options are:

* None - No limiting is done.
* Groups - Limits the IGMP report message based on the group registration that are allowed per downstream interface.
* Channels - Limit is applied only for IGMPv3 Include and Allow reports based on the S,G registration that are allowed per downstream interface. By default, Threshold limit type is set to none. The channel limit is applied only for IGMPv3 include and allow reports. The group limit is applied for all IGMP reports.

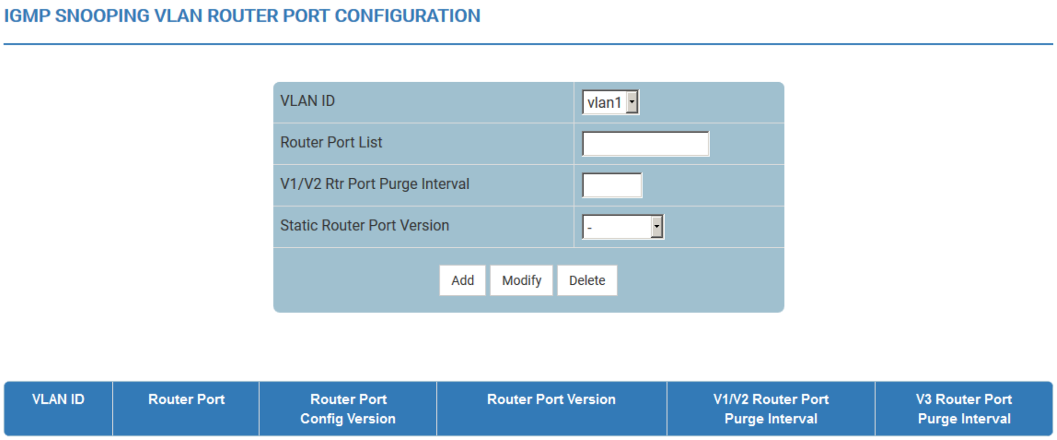
Threshold Limit - Enter the maximum number of unique entries (channel or group) which can be learned simultaneously on the interface. The software allows the configuration of threshold limit per downstream interface. Downstream interface refers to a physical port in the default mode of operation or to a combination of inner VLAN and physical port in the enhanced mode of operation of the switch.

* If the limit type is None - Limit should be less than the maximum of maximum groups and maximum channels.
* If the limit type is Groups - Limit should be less than maximum groups (255).
* If the limit type is Channels - Limit should be less than maximum channels (65025).

By default the threshold limit is 0.

Rate Limit - Enter the rate limit for a downstream interface in the units of the number of IGMP packets per second. The software calls an NPAPI to configure this limit into the data path/hardware. The MDL rate limit per port will eliminate bursts or attacks coming from the specific physical port and thereby eliminates the case of exhausting the system resources. The value ranges between 0 and 4294967295. By default the rate limit is set to 4294967295.

6.1.5 RouterPortConf



IGMP SNOOPING VLAN ROUTER PORT CONFIGURATION

VLAN ID	vlan1
Router Port List	
V1/V2 Rtr Port Purge Interval	
Static Router Port Version	-

VLAN ID	Router Port	Router Port Config Version	Router Port Version	V1/V2 Router Port Purge Interval	V3 Router Port Purge Interval

Fig: IGMP Snooping VLAN Router Port Configuration

This page allows the user to configure the details of the router port.

VLAN ID - Select the VLAN Identifier that uniquely identifies a specific VLAN. The IGMP snooping configuration is performed for the entered VLAN ID.

Router Port List - Enter the router port / port list for the VLAN specified in VLAN ID field. When the snooping switch receives a router advertisement message through a port, the port is learnt as router port. These ports are part of this router port list. User can enter the router port / port-list on which he wants to configure the purge interval / version.

V1/V2 Rtr Port Purge Interval - Enter the time interval after which the switch assumes that there are no v1/v2 routers present on the upstream port. For each router port learnt, this timer runs for 'RouterPortPurgeInterval' seconds. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. The value ranges between 60 and 600. By default, V1/V2 Rtr Port Purge Interval is set to 125

Static Router Port Version - Select the operating version of the IGMP proxy on the upstream router port. By default, Static Router Port Version is Version 3. The list contains:

* Version1 - Indicates that the operating version of IGMP proxy is version 1

* Version2 - Indicates that the operating version of IGMP proxy is version 2

* Version3 - Indicates that the operating version of IGMP proxy is version 3

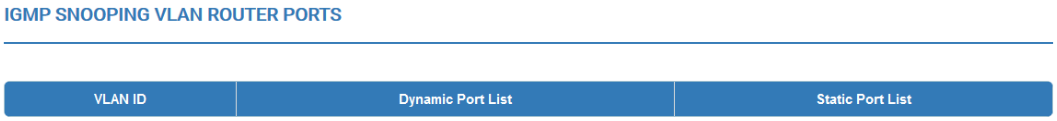
Router Port - Displays the interface index of the port which is defined as an upstream router port. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port.

Router Port Config Version - Displays the configured version of the IGMP Proxy on the upstream router port. By default, Router Port Config Version is set to Version 3

Router Port Version - Displays the operating version of the IGMP proxy on the upstream router port. By default, Router Port Version is set to Version 3

V3 Router Port Purge Interval - Displays the time interval after which the switch assumes that there are no IGMP v3 routers present on the upstream port. For each V3 router port learnt, the timer runs for time interval calculated based on the formula - V3 Router port purge Interval = ((V3 Querier Query Interval * Robustness variable) + Max ResponseTime) seconds. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. The value ranges between 60 and 600. By default, V3 Router Port Purge Interval is set to 125.

6.1.6 RouterPorts



IGMP SNOOPING VLAN ROUTER PORTS

VLAN ID	Dynamic Port List	Static Port List

Fig: IGMP Snooping VLAN Router Ports

This page displays the Router Port List table. The dynamic and static ports are listed in the page.

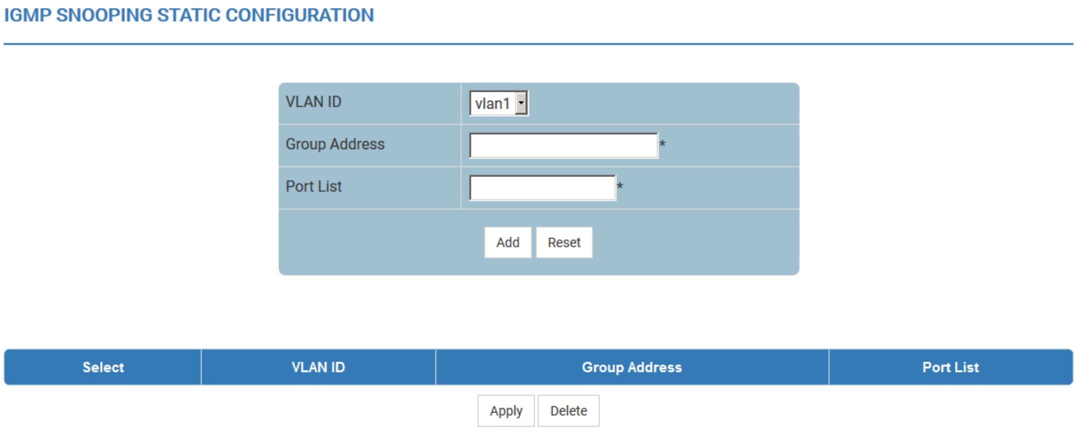
VLAN ID - Displays the VLAN Identifier that uniquely identifies a specific VLAN on which router ports are learnt / configured.

Dynamic Port List - Displays the lists of ports on which routers are present.

> These router ports are learnt through control messages received from routers and can also be configured statically.

Static Port List - Displays the list of ports which are configured statically as router ports. Only static router ports will be restored during save restore. The default operating version for static router ports will be IGMPv3, based on the address type.

6.1.7 StaticEntry



IGMP SNOOPING STATIC CONFIGURATION

VLAN ID	vlan1
Group Address	*
Port List	*

Select	VLAN ID	Group Address	Port List

Fig: IGMP Snooping Static Configuration

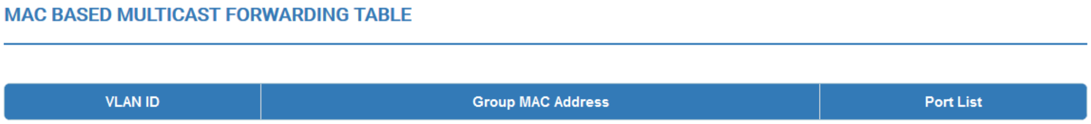
This page allows the user to configure IGMP snooping static multicast in the multicast switch.

VLAN ID - Select the VLAN Identifier that uniquely identifies a specific VLAN. The IGMP snooping configuration is performed for this specific VLAN ID.

Group Address - Enter the specific group MAC multicast address for the VLAN specified in VLAN ID field. This value ranges between 225.0.0.0. and 239.255.255.255

Port List - Enter the port list for specific group MAC multicast address and VLAN ID.

6.1.8 FwdInformation



MAC BASED MULTICAST FORWARDING TABLE

VLAN ID	Group MAC Address	Port List

Fig: MAC Based Multicast Forwarding Table

This page displays the IGMP group information such as MAC based Multicast Forwarding Table and IP based Multicast Forwarding Table. Entries are created in Multicast Forwarding tables based on membership reports from hosts attached to the switch.

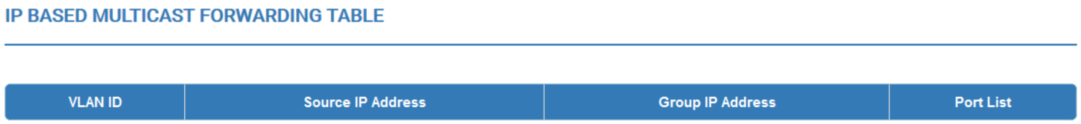
Multicast Forwarding table is populated with list of ports interested in receiving multicast traffic to avoid flooding of multicast data traffic.

When snooping is disabled on the port, all the entries in the group table and forwarding table are deleted for the port.

VLAN ID - Displays the VLAN Identifier that uniquely identifies a specific VLAN. The MAC based multicast forwarding entry is displayed for the requested VLAN ID.

Group MAC Address - Displays the Group MAC Multicast address that is learnt.

Port List - Displays the learnt ports list for which the multicast data packets for the group will be forwarded.



IP BASED MULTICAST FORWARDING TABLE

VLAN ID	Source IP Address	Group IP Address	Port List

Fig: IP Based Multicast Forwarding Table

VLAN ID - Displays the VLAN Identifier that uniquely identifies a specific VLAN. The IP based multicast forwarding entry is displayed for the entered VLAN ID.

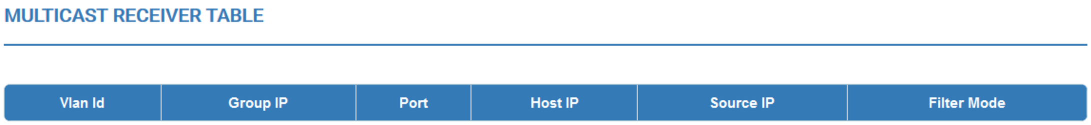
Inner VLAN ID - Displays the Inner VLAN Identifier with the snooping module operates in enhanced mode.

Source IP Address - Displays the unicast source IP address of the data source that sends multicast data to the group.

Group IP Address - Displays the IP address of the group that is registered for receiving the multicast traffic.

Port List - Displays the learnt ports list for which the multicast data packets for group should be forwarded.

6.1.9 McastReceiverInfo



MULTICAST RECEIVER TABLE

Vlan Id	Group IP	Port	Host IP	Source IP	Filter Mode

Fig: Multicast Receiver Table

This page displays multicast report sent by each host in a multicast group requesting data from a specific source.

Vlan ID - Displays the VLAN ID pertaining to the multicast receiver table.

Inner VLAN ID - Displays the Inner VLAN Identifier with the snooping module operates in enhanced mode.

Group IP - Displays the multicast group address for which the receiver has sent a request to join the group.

Port - Displays the port on which the multicast receiver has sent a join request.

Host IP - Displays the IP address of the multicast receiver that has sent a request to join the multicast group.

Source IP - Displays the unicast source IP address of the data source that sends multicast data to the group.

Filter Mode - Displays the mode that has been registered by the multicast receiver, for the unicast source IP address specified.

The list contains:

* Include - Reception of packets sent to the specified multicast address, is requested *only* from those IP source addresses listed in the source-list parameter.

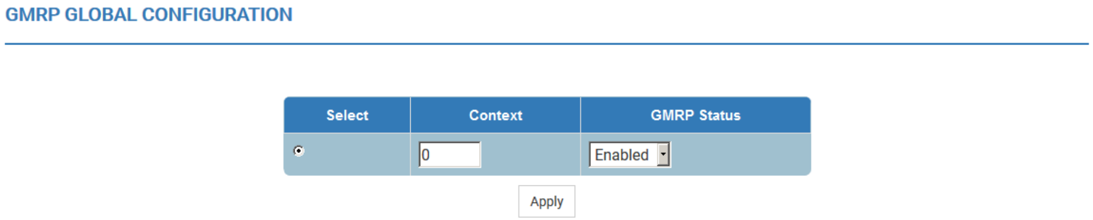
* Exclude - Reception of packets sent to the given multicast address, is requested from all IP source addresses *except* those listed in the source-list parameter.

6.2 GMRP

The *GMRP* link allows you to configure the GMRP for switch. User can configure GMRP on the following two pages.

- ❖ GMRP
- ❖ Port Settings

6.2.1 GMRP



GMRP GLOBAL CONFIGURATION

Select	Context	GMRP Status
●	0	Enabled

Fig: GMRP Global Configuration

This page allows the user to globally configure GMRP.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch

* By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0). The value ranges between 0 and 65535 and the default value is 0.

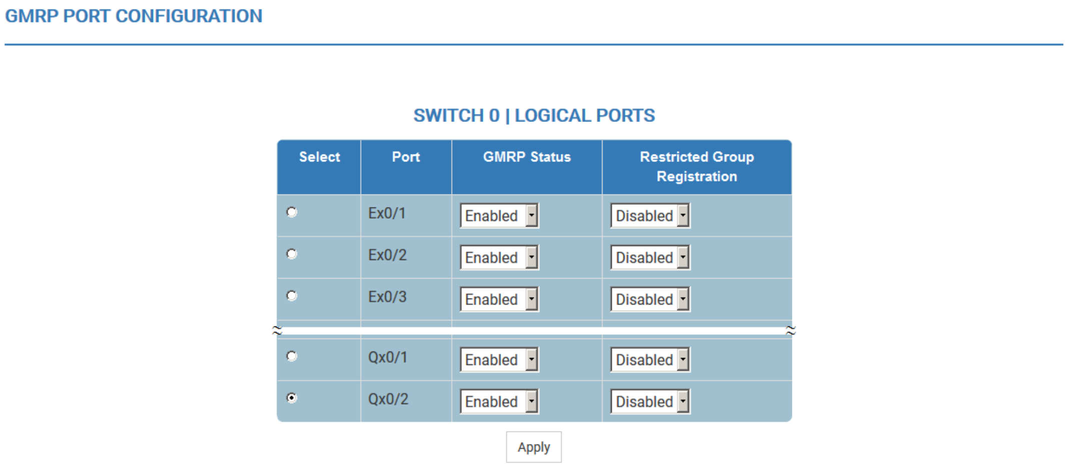
GMRP Status - Select the global status of GMRP protocol in the system. GMRP uses the services of GARP to propagate multicast registration information to the bridges in the LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. By default, the status is enabled. The list contains:

* Enabled - Allows data transmission to multiple recipients using the same stream. GMRP is enabled in all VLANs, on all the ports for which it has not been specifically disabled

* Disabled - Does not allow multicast routing. The previously learnt information is flushed, message received on the port is discarded and messages cannot be sent on the port.

> At the system level, GMRP and snooping (IGS and MLDS) are mutually exclusive. It means that at a point of time either GMRP or Snooping (IGS and MLDS) can only be enabled.

6.2.2 Port Settings



GMRP PORT CONFIGURATION

SWITCH 0 | LOGICAL PORTS

Select	Port	GMRP Status	Restricted Group Registration
○	Ex0/1	Enabled	Disabled
○	Ex0/2	Enabled	Disabled
○	Ex0/3	Enabled	Disabled
○	Qx0/1	Enabled	Disabled
●	Qx0/2	Enabled	Disabled

Fig: GMRP Port Configuration

This page allows the user to configure the GMRP control and restricted group registration details for every bridge port.

Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

GMRP Status - Select the status of GMRP protocol for the selected ports. GMRP uses the services of GARP to propagate multicast registration information to the bridges in the LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. By default the status is enabled. The list contains:

* Enabled - Allows data transmission to multiple recipients using the same stream. GMRP is enabled in all VLANs, on all the ports for which it has not been specifically disabled

* Disabled - Does not allow multicast routing. The previously learnt information is flushed, message received on the port is discarded and messages cannot be sent on the port. When disabled any GMRP packets received will be silently discarded and no GMRP registrations will be propagated from other ports

> At the system level, GMRP and IGMP snooping are mutually exclusive. It means that at a point of time either GMRP or IGMP Snooping can only be enabled.

Restricted Group Registration - Select the Restricted Group Registration status. By default the status is disabled. The list contains:

* Enabled - Enables Restricted Group Registration. Creation of a new dynamic entry is permitted only if there is a Static Filtering Entry for the VLAN concerned, in which the Registrar Administrative Control value is Normal Registration

* Disabled - Disables Restricted Group Registration.

> Restricted Group Registration enables you to restrict the multicast groups learnt through GMRP learning.

7 MON

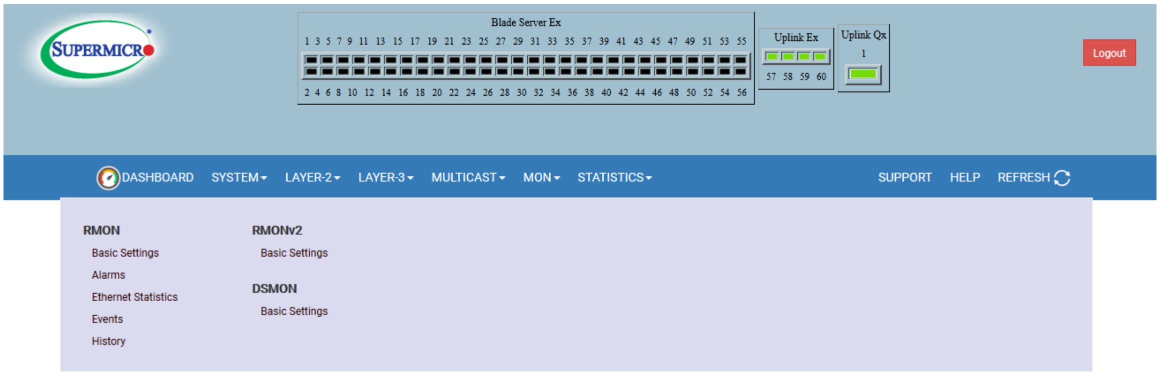


Fig: MON

MON covers the following features of switch:

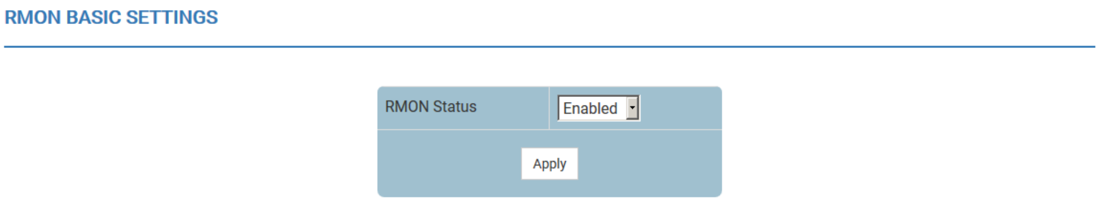
- RMON
- RMONv2
- DSMON

7.1 RMON

The *RMON* link allows you to configure the RMON status. User can configure RMON on the following 5 pages.

- ❖ Basic Settings
- ❖ Alarms
- ❖ Ethernet Statistics
- ❖ Events
- ❖ History

7.1.1 Basic Settings


RMON BASIC SETTINGS

RMON Status: Enabled

Fig: RMON Basic Settings

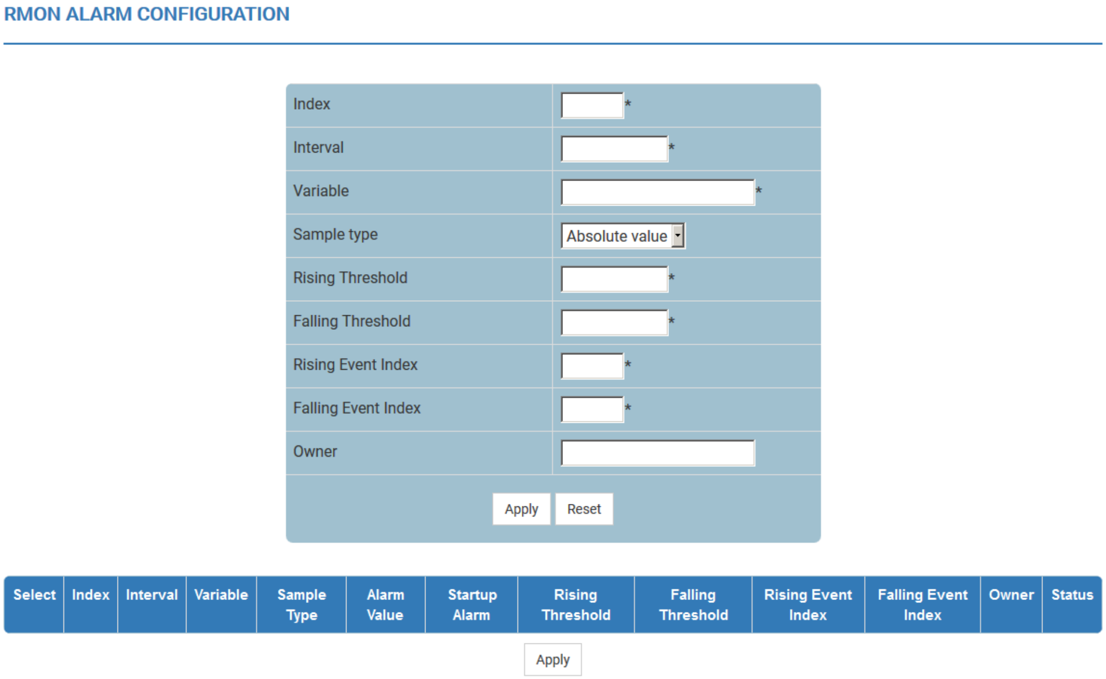
The page allows the user to configure the RMON status. Once the status is enabled the RMON starts monitoring the remote networks and collect data for storage in the table.

RMON Status - Select the status of RMON on the switch. By default, RMON Status is set as Disabled. The list contains:

* Enabled - Enables RMON in the switch. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis.

* Disabled - Disables RMON in the switch. On disabling, the RMON’s network monitoring is called off.

7.1.2 Alarms



RMON ALARM CONFIGURATION

Index	*
Interval	*
Variable	*
Sample type	Absolute value
Rising Threshold	*
Falling Threshold	*
Rising Event Index	*
Falling Event Index	*
Owner	

Select	Index	Interval	Variable	Sample Type	Alarm Value	Startup Alarm	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Status

Fig: RMON Alarm Configuration

This page allows the user to configure RMON alarm settings. This is done to raise an alarm when the condition specified occurs. The various alarm configurations are updated in the table. RMON Events must be configured before Alarms can be configured.

The form at the top is used to create a new RMON alarm entry and the one at the bottom is used to modify the attributes of the alarm table.

Index - Enter the value of RMON alarm table index. The index value uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device.
This value ranges between 1 and 65535.
Interval - Enter the time interval in seconds for which the alarm monitors the MIB object variable. It is during this interval the data is sampled and compared with the rising and falling thresholds.
This value ranges between 1 and 65535.
Variable - Enter the MIB object variable on which the alarm is set. For successful configuration the Variable has to be a valid Object ID.
Sample Type - Select the sample type to be compared against the thresholds. By default the sample type is set as Absolute value. The list contains:

* Absolute value - The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval.

* Delta value - The value of the selected variable at the last sample will be subtracted from the current value, and the difference is compared with the thresholds at the end of the sampling interval.

Rising Threshold - Enter the Rising Threshold value. This value ranges between 0 and 2147483647. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised.

When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated.

Falling Threshold - Enter the Falling Threshold value. This value ranges between 0 and 2147483647. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised.

When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated.

Rising Event Index - Enter the index of the event to be raised when the Rising threshold is reached. This value ranges between 1 and 65535.

The event entry identified by a particular value of this index is the same as identified by the same value of the event index object.

Falling Event Index - Enter the index of the event to be raised when the Falling threshold is reached. This value ranges between 1 and 65535.

The event entry identified by a particular value of this index is the same as identified by the same value of the event index object.

Owner - Enter the entity details that configured this entry.

Alarm Value - Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed.

For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds.

Startup Alarm - Displays the alarm that is sent when the entry is set as valid for the first time. Options are:

* RisingAlarm - Denotes that the first sample after the entry becoming valid is greater than or equal to the rising threshold.

* FallingAlarm - Denotes that the first sample after the entry becoming valid is less than or equal to the falling threshold.

* RisingOrFallingAlarm - Denotes that either Rising or Falling Alarm is sent based on the sample in comparison with the rising and falling threshold.

Status - Select the required status of alarm. The list contains:

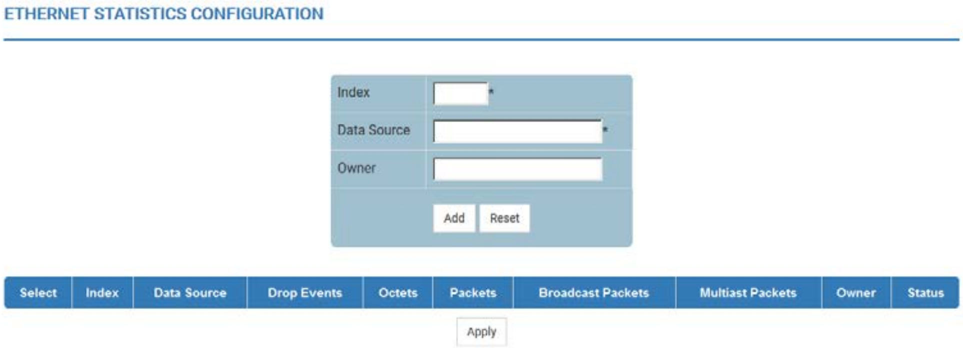
* Valid - Alarm entry is created and completely created.

* Under Creation - Alarm entry is created and not completely configured.

* Invalid - Alarm entry is removed.

> While creating a new RMON alarm entry, for invalid configuration the error message will be displayed and the status is set as Under Creation.

7.1.3 Ethernet Statistics



Select	Index	Data Source	Drop Events	Octets	Packets	Broadcast Packets	Multiast Packets	Owner	Status

Fig: Ethernet Statistics

This page contains statistics measured by the probe for each monitored interface on the device.

The form at the top is used to create new Ethernet statistics entry in the switch and the one at the bottom is used to modify the attributes of the entry.

Index - Enter the Ethernet Statistics index that uniquely identifies an entry in the Ethernet Statistics table.

Data Source - Enter the SNMP object ID of the variable on which the statistics is being collected. This object identifies the instance of the ifIndex object.

For successful configuration the Data Source has to be a valid Object ID

Owner - Enter the details of the entity that configured this entry.

Drop Events - Displays the number of events in which the packets were dropped due to lack of resources.

This number does not specify the number of packets dropped but the number of times the packets were dropped.

Octets - Displays the total number of octets of data received from the network.

This can be used as a reasonable estimate of 10-Megabit Ethernet utilization.

Packets - Displays the total number of packets received from the network.

This includes bad packets, broadcast packets and multicast packets received.

Broadcast Packets - Displays the total number of broadcast packets received from the network.

Multicast Packets - Displays the total number of multicast packets received from the network.

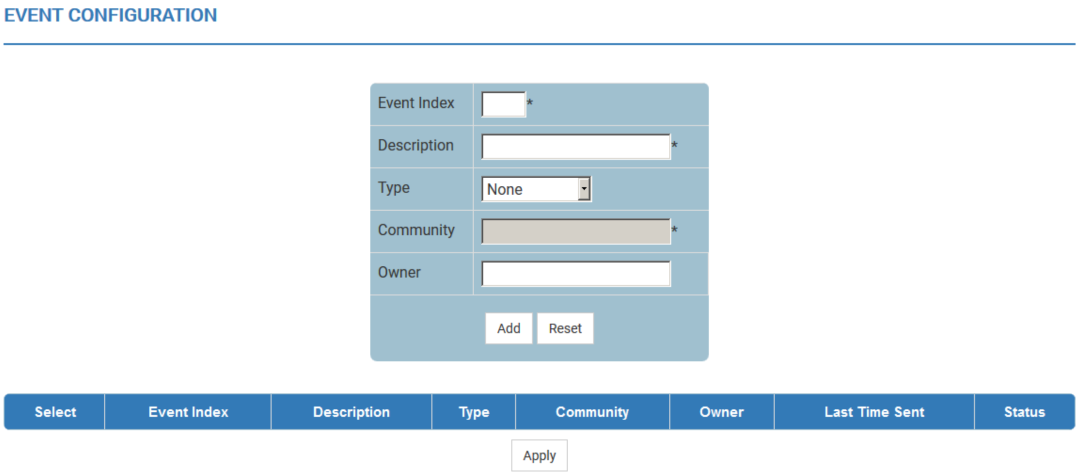
Status - Select the required status of event. The list contains:

* Valid - Ethernet statistics entry is created and completely created.

* Invalid - Ethernet statistics entry is removed.

* Under Creation - Ethernet statistics entry is created and not completely configured.

7.1.4 Events



EVENT CONFIGURATION

Event Index	*
Description	*
Type	None
Community	*
Owner	

Select	Event Index	Description	Type	Community	Owner	Last Time Sent	Status

Fig: Event Configuration

The Event module generates events whenever an associated condition takes place in the device. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module.

This page allows the user to configure RMON event settings.

The form at the top is used to create new RMON Event Configuration entry in the system and one at the bottom is used to delete a RMON Event Configuration entry or modify the attributes of a RMON Event Configuration entry.

Event Index - Enters a number that uniquely identifies an entry in the Events table. This values ranges between 1 and 65535.

Each such entry defines one event that is to be generated when appropriate conditions occur.

Description - Enter a brief description of the event.

The size of the display string varies between 0 and 127 characters.

Type - Select the type of event to be configured. The list contains:

* Log - Creates an entry in the log table for each event.

* SNMP Trap - Sends an SNMP trap to one or more management stations.

* Log and Trap - Creates an entry in the log table and sends an SNMP trap.

* None - No type is set.

> The Community field is disabled, when the event Type is None or Log.

Community - Enter the SNMP community string to which the SNMP trap is to be sent.

> This is relevant when an SNMP trap is requested for an event.

Owner - Displays the entity that configured this entry.

Last Time Sent - Displays the time this event entry last generated an event. If this entry has not generated any events, the value will be zero.

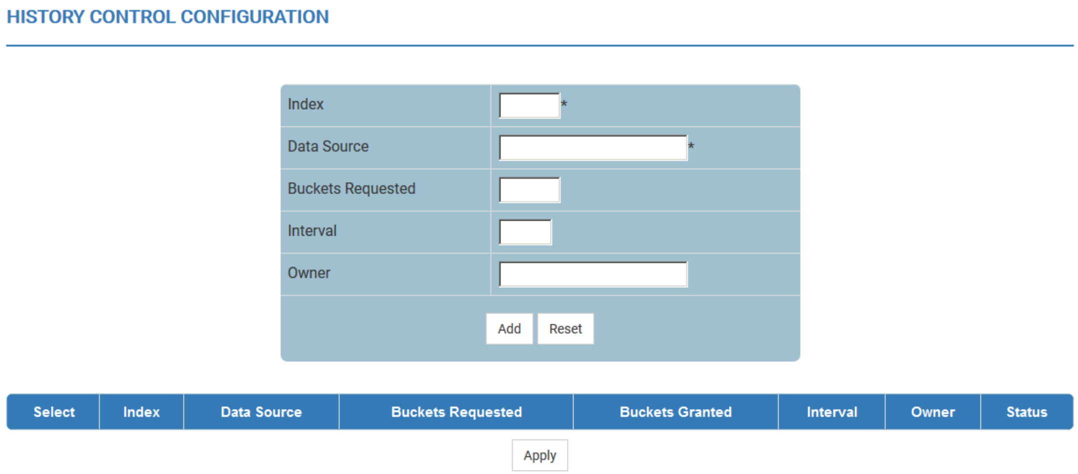
Status - Select the required status of event. The list contains:

* Valid - Event entry is created and completely created.

* Invalid - Event entry and its associated log entries are removed.

* Under Creation - Event entry is created and not completely configured.

7.1.5 History



HISTORY CONTROL CONFIGURATION

Index	*
Data Source	*
Buckets Requested	
Interval	
Owner	

Select	Index	Data Source	Buckets Requested	Buckets Granted	Interval	Owner	Status

Fig: History Control Configuration

This page allows the user to configure RMON history settings. The History module collects periodic statistical sampling of the data collected by statistics module. This module stores the sample collected from the etherstat table to the etherHistory table.

The form at the top is used to create new History Control configuration entry in the system and the one at the bottom is used to modify the attributes of a History Control configuration entry.

Index - Enter an integer value to uniquely identify an entry in the History Control Table.
Each such entry defines a set of samples at a particular interval for an interface on the device.
Data Source - Enter the details of the SNMP object id of the variable on which the history is being collected. This object identifies the instance of the ifIndex object.
For successful configuration the Data source has to be a valid Object ID.
Buckets Requested - Enter the number of buckets to be configured for collecting the RMON statistics, that is, the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
This value ranges between 1 and 65535. Default value is 50.
Interval - Enter the time interval (in seconds) over which the data is sampled for each bucket to collect the statistics.
This value ranges between 1 and 3600 seconds. Default value is 1800 seconds.
Owner - Enter the details of the entity that configured this entry.
Buckets Granted - Displays the number of buckets granted for collecting the RMON statistics.
This value ranges between 1 and 65535. This is a read-only field.
Status - Select the required status of event. The list contains:

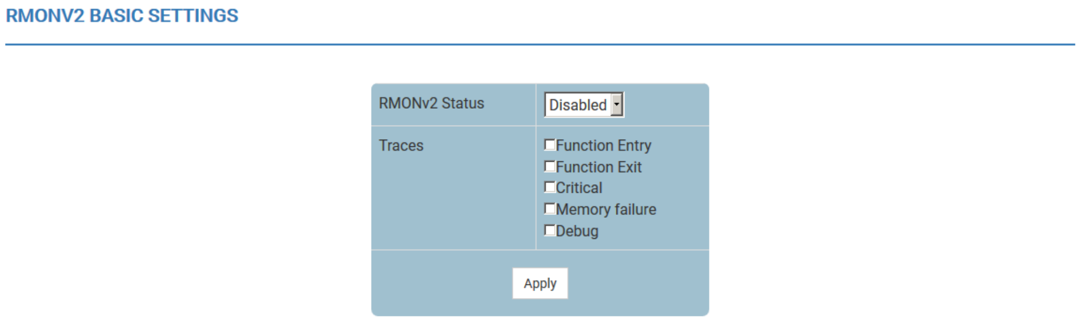
* Valid - History control entry is created and completely created.

* Invalid - History control entry is removed.

* Under Creation - History control entry is created and not completely configured.

7.2 RMONv2

The *RMONv2* link allows you to configure the RMONv2 status. User can configure RMONv2 on the following page.



RMONV2 BASIC SETTINGS

RMONv2 Status	Disabled
Traces	☐Function Entry ☐Function Exit ☐Critical ☐Memory failure ☐Debug

Fig: RMONv2 Basic Settings

The RMONv2 Basic Settings page allows the user to configure RMONv2 related parameters.

RMONv2 Status - Select status for RMONv2.

By default, RMONv2 Status is set as Disabled. The list contains:

* Enabled - Enables RMONv2 in the switch. RMONv2 starts monitoring the network along with the nine groups implemented with it

* Disabled - Disables RMONv2 in the switch.

Traces - Select the traces for which debug statements is to be generated. The options are:

* Function Entry - Generates debug statement for function entry traces.

* Function Exit - Generates debug statements for function exit traces.

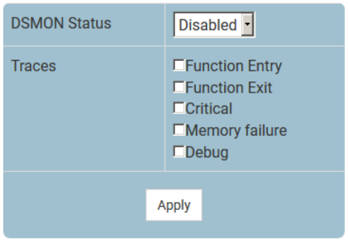
* Critical - Generates debug statements for all Critical occasions.

* Memory failure - Generates debug statements for memory allocation failure traces.

* Debug - Generates debug statements for less severe failures.

7.3 DSMON

DSMON BASIC SETTINGS



DSMON Status	Disabled
Traces	□Function Entry □Function Exit □Critical □Memory failure □Debug

Fig: DSMON Basic Settings

The DSMON Basic Settings page allows the user to configure DSMON related parameters.

DSMON can be enabled, only if the RMONv2 Status is set as Enabled.

DSMON Status - Select status for DSMON.

By default, DSMON Status is set as Disabled. The list contains:

* Enabled - Enables DSMON in the switch. DSMON starts monitoring the network and sends/receive information between Probes and Central managers

* Disabled - Disables DSMON in the switch.

Traces - Select the traces for which debug statements is to be generated. The options are

* Function Entry - Generates debug statement for function entry traces.

* Function Exit - Generates debug statements for function exit traces Critical - This trace captures any failure which can obstruct the operation of DSMON. All critical failures are captured and displayed in the order of occurrence.

* Critical - Generates debug statements for all Critical occasions

* Memory failure - Generates debug statements for memory allocation failure traces.

* Debug - Generates debug statements for less severe failures.

8 Statistics

Statistics menu has links to all statistical information all features.

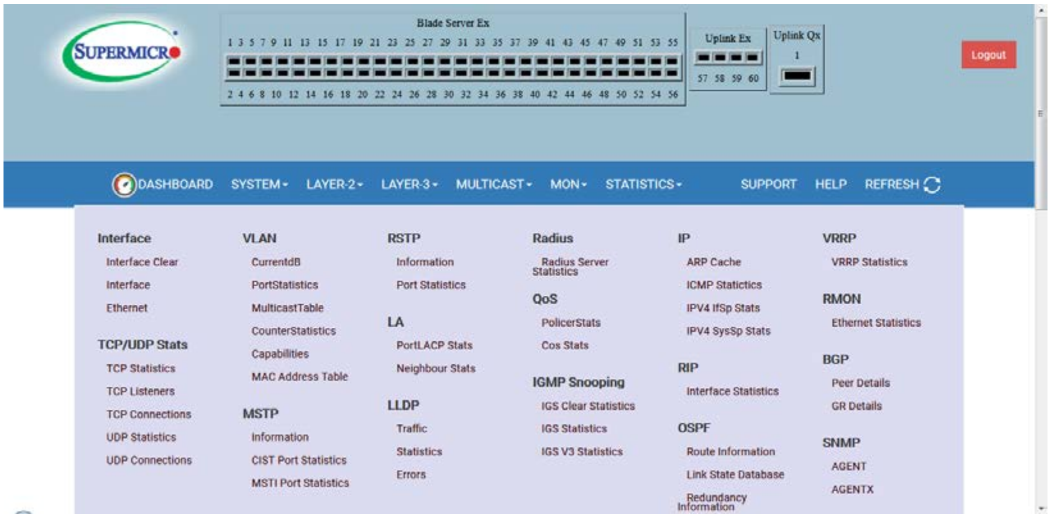


Fig: Statistics

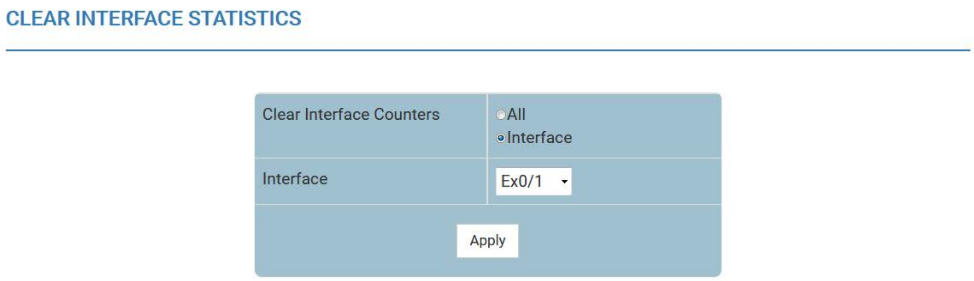
- Interface
- TCP/UDP Stats
- VLAN
- MSTP
- RSTP
- LA
- LLDP
- Radius
- QoS
- IGMP Snooping
- IP
- RIP
- OSPF
- VRRP
- RMON
- BGP
- SNMP

8.1 Interface

The Interface link allows the user to view or reset the interface related statistics screens through the following tabs.

- Interface Clear
- Interface
- Ethernet

8.1.1Interface Clear



CLEAR INTERFACE STATISTICS

Clear Interface Counters	○All ●Interface
Interface	Ex0/1

Fig: Clear Interface Statistics

The *Interface Clear* link opens the **Clear Interface Statistics** Page**.**

Clear Interface Statistics page allows the user to clear the details in the interface counter for a particular interface or for all the interfaces.

The table below lists the fields present in this page.

Clear Interface - Select a particular interface or all the interfaces to clear.

Counters - By default, Clear Interface Counters is set as Interface.

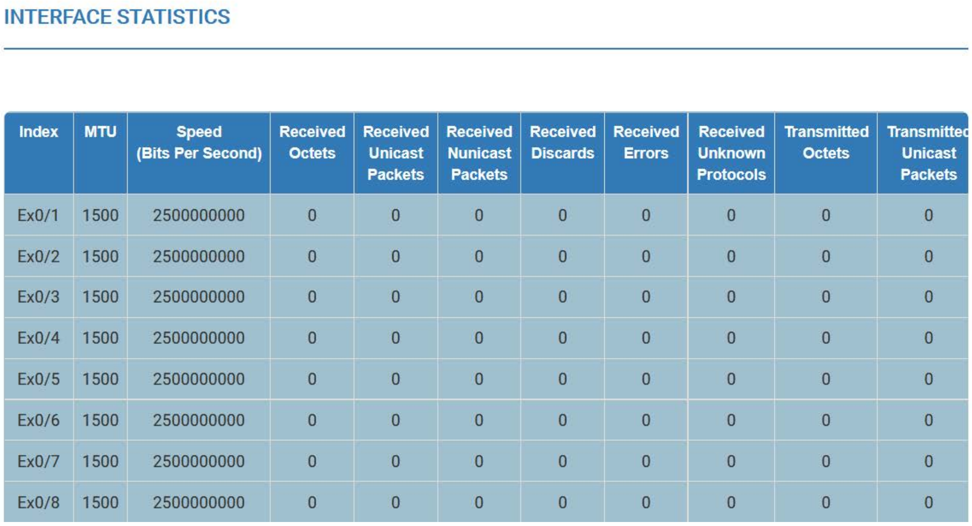
The list contains:

* All - Select all the interfaces.

* Interface - Select a particular interface.

Interface - Select the interface index of the port

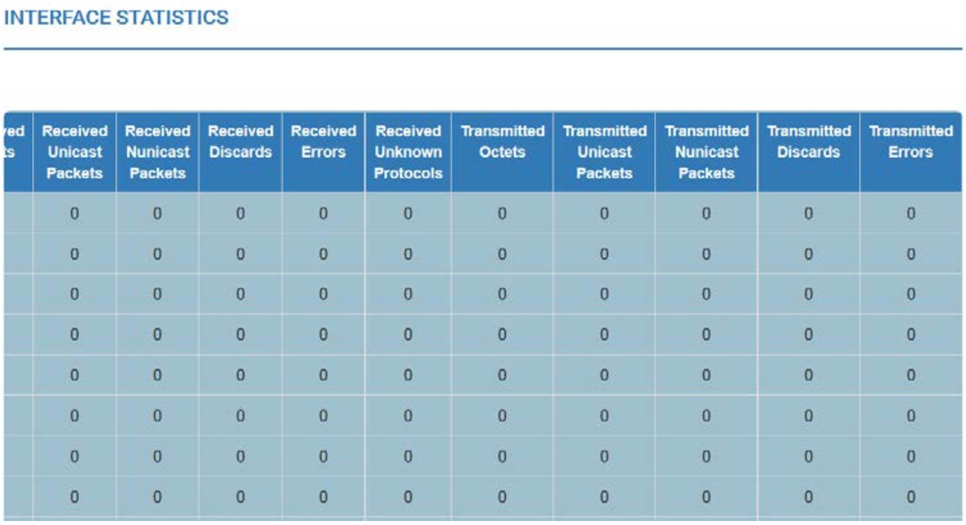
8.1.2Interface



INTERFACE STATISTICS

Index	MTU	Speed (Bits Per Second)	Received Octets	Received Unicast Packets	Received Nunicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets
Ex0/1	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/2	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/3	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/4	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/5	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/6	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/7	1500	2500000000	0	0	0	0	0	0	0	0
Ex0/8	1500	2500000000	0	0	0	0	0	0	0	0

Fig: Interface Statistics – Statistics Group-Part A



INTERFACE STATISTICS

ved ts	Received Unicast Packets	Received Nunicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted Nunicast Packets	Transmitted Discards	Transmitted Errors
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0

Fig: Interface Statistics – Statistics Group-Part B

The *Interface* link opens the **Interface Statistics** Page**.**

Interface Statistics page displays the management information applicable to all the interfaces available in the Switch.

The table below lists the fields present in this page.

Index - Interface name.

MTU - Max Transfer Unit bytes.

Speed (Bits Per Second) - Port speed in bits per second.

Received Octets - Number of bytes received.

Received Unicast Packets - Number of Unicast packets received.

Received Nunicast Packets - Number of Non-unicast packets received.

Received Discards - Number of packets discarded due to errors

Received Errors - Number of packets received with errors.

Received Unknown Protocols - Number of packets received with unknown protocol.

Transmitted Octets - Number of bytes transmitted.

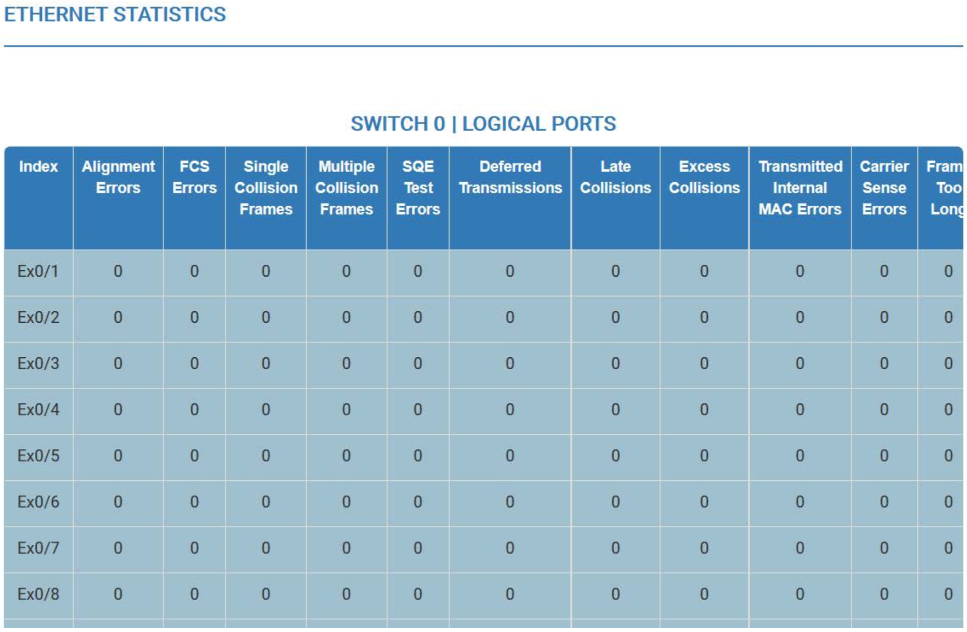
Transmitted Unicast Packets - Number of Unicast packets transmitted.

Transmitted Nunicast Packets - Number of Non-unicast packets transmitted.

Transmitted Discards - Number of packets discarded due to transmit errors.

Transmitted Errors - Number of transmit errors.

8.1.3Ethernet

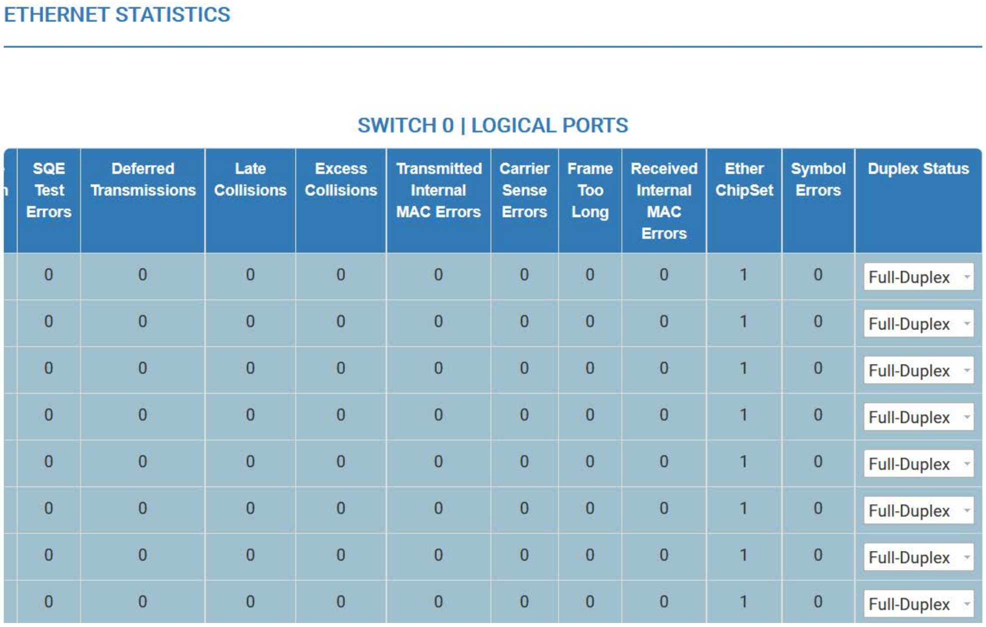


ETHERNET STATISTICS

SWITCH 0 | LOGICAL PORTS

Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Fram Too Long
Ex0/1	0	0	0	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0	0	0	0
Ex0/4	0	0	0	0	0	0	0	0	0	0	0
Ex0/5	0	0	0	0	0	0	0	0	0	0	0
Ex0/6	0	0	0	0	0	0	0	0	0	0	0
Ex0/7	0	0	0	0	0	0	0	0	0	0	0
Ex0/8	0	0	0	0	0	0	0	0	0	0	0

Fig: Ethernet Statistics – Statistics Group-Part A



ETHERNET STATISTICS

SWITCH 0 | LOGICAL PORTS

n	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Frame Too Long	Received Internal MAC Errors	Ether ChipSet	Symbol Errors	Duplex Status
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex
	0	0	0	0	0	0	0	0	1	0	Full-Duplex

Fig: Ethernet Statistics – Statistics Group-Part B

The *Ethernet* link opens the **Ethernet Statistics** Page**.**

Ethernet Statistics page displays the statistics for a collection of Ethernet-like interfaces attached to the Switch.

The table below lists the fields present in this page.

Index - Interface name.

Alignment Errors - Number of alignment errors. Alignment errors generally indicate improper byte-alignment for Ethernet packets.

FCS Errors - Number of packets received with checksum errors.

Received Octets - Number of bytes received.

Single Collision Frames - Number of frames received with a collision.

Multiple Collision Frames - Number of frames received with multiple collisions.

SQE Test Errors - Number of Signal Quality Errors occurred.

Deferred Transmissions - Number of frames deferred for transmissions due to network sense.

Late Collisions - Number of frames faced late collisions.

A collision is considered late if the jam occurs after 512 bit-times, or 64 bytes.

Excess Collisions - Number of excess collisions detected. Excessive Collisions describe the situation where a station has tried 16 times to transmit without success and discards the frame. This means that there is excessive traffic on the network and this must be reduced.

Transmitted Internal MAC Errors - Number of MAC transmit errors.

Carrier Sense Errors - Number of carrier sense errors.

Frame Too Long - Number of too long frames received for transmission.

Received Internal MAC Errors - Number of MAC receive errors.

Ether ChipSet - This object contains an OBJECT IDENTIFIER which identifies the chipset used to realize the interface.

Symbol Errors - Number of symbol errors.

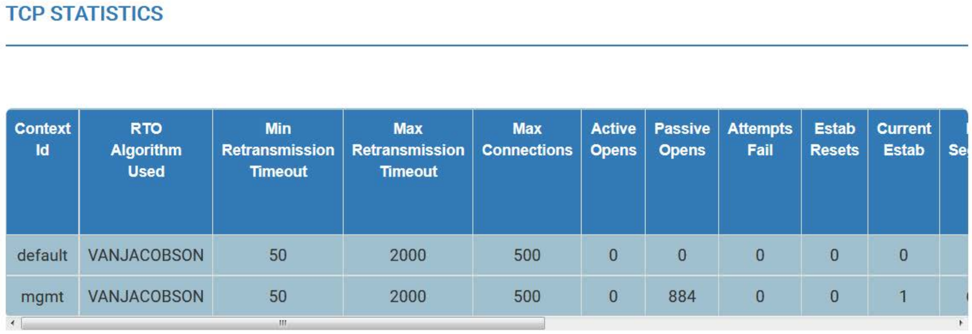
Duplex Status - Current status of duplex

8.2 TCP/UDP Stats

The TCP link allows the user to view the TCP and UDP statistics screens through the following tabs.

- TCP Statistics
- TCP Listeners
- TCP Connections
- UDP Statistics
- UDP Connections

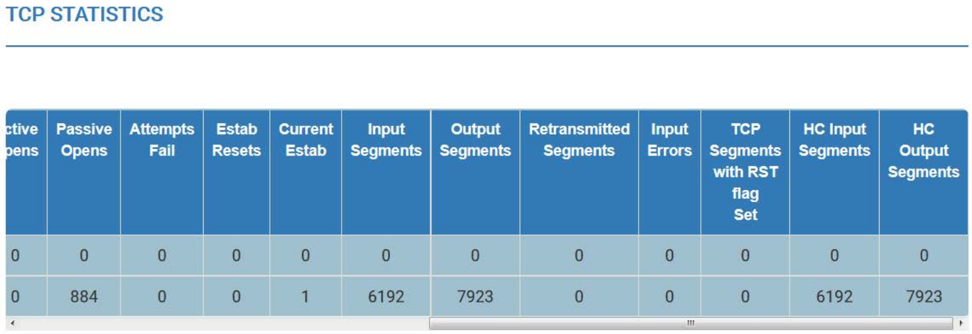
8.2.1TCP Statistics



TCP STATISTICS

Context Id	RTO Algorithm Used	Min Retransmission Timeout	Max Retransmission Timeout	Max Connections	Active Opens	Passive Opens	Attempts Fail	Estab Resets	Current Estab	Se
default	VANJACOBSON	50	2000	500	0	0	0	0	0	
mgmt	VANJACOBSON	50	2000	500	0	884	0	0	1	

Fig: TCP Statistics – Statistics Group-Part A



TCP STATISTICS

ctive pens	Passive Opens	Attempts Fail	Estab Resets	Current Estab	Input Segments	Output Segments	Retransmitted Segments	Input Errors	TCP Segments with RST flag Set	HC Input Segments	HC Output Segments
0	0	0	0	0	0	0	0	0	0	0	0
0	884	0	0	1	6192	7923	0	0	0	6192	7923

Fig: TCP Statistics – Statistics Group-Part B

The *TCP Statistics* link opens the **TCP Statistics** Page.
TCP Statistics page displays the TCP related statistics details such as Min and Maximum Retransmission Timeout, Maximum connections etc, which allows the user to know the status of packets transferred using TCP.

The table below lists the fields present in this page.

Context Id - The Alias name for the Virtual-Context.

RTO Algorithm Used - The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

Min Retransmission Timeout - The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds

Max Retransmission Timeout - The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

Max Connections - The limit on the total number of TCP connections the entity can support.

Active Opens - The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Passive Opens - The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Attempts Fail - The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Estab Resets - The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Current Estab - The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.

Input Segments - The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Output Segments - The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Retransmitted Segments - The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

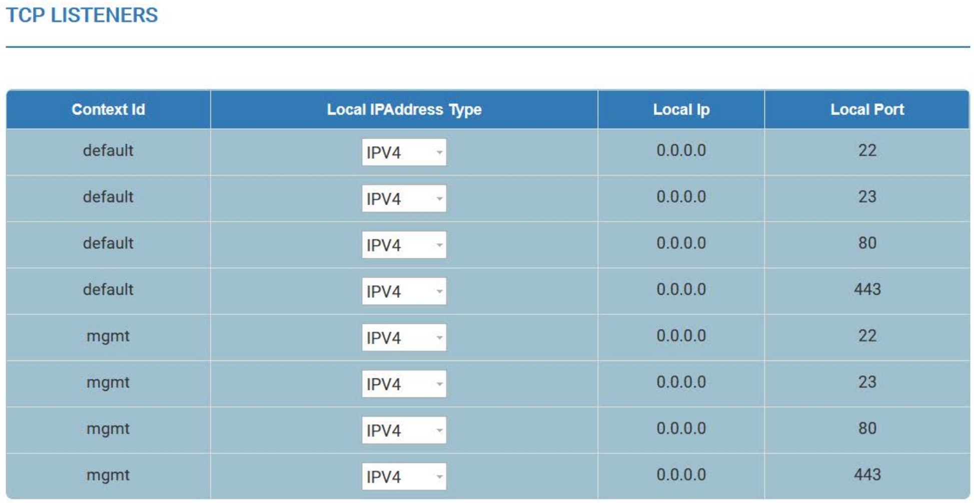
Input Errors - The total number of segments received in error (e.g., bad TCP checksums).

TCP Segments with RST flag Set **-** The number of TCP segments sent containing the RST flag.

HC Input Segments - The total number of segments received, including those received in error. This count includes segments received on currently established connections. This object is the 64-bit equivalent of tcpInSegs.

HC Output Segments - The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. This object is the 64-bitequivalent of tcpOutSegs.

8.2.2TCP Listeners



TCP LISTENERS

Context Id	Local IPAddress Type	Local Ip	Local Port
default	IPV4	0.0.0.0	22
default	IPV4	0.0.0.0	23
default	IPV4	0.0.0.0	80
default	IPV4	0.0.0.0	443
mgmt	IPV4	0.0.0.0	22
mgmt	IPV4	0.0.0.0	23
mgmt	IPV4	0.0.0.0	80
mgmt	IPV4	0.0.0.0	443

Fig: TCP Listeners – Statistics Group

The *TCP Listeners* link opens the **TCP Listeners** Page.

TCP Listeners page displays the information such as Local IP, stored in the TCP listeners table.

The table below lists the fields present in this page.

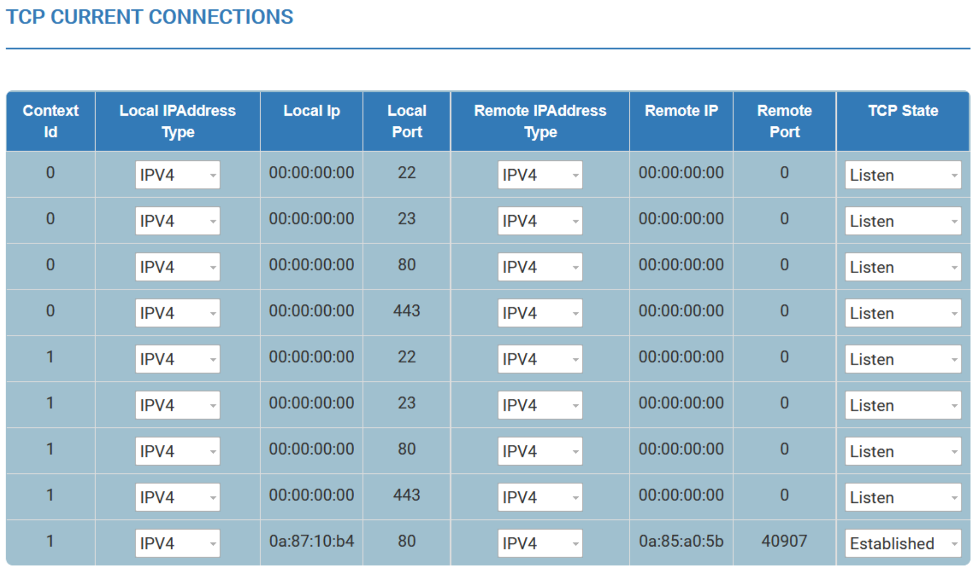
Context Id - The Alias name for the Virtual-Context Local IPAddress

Type - The address type of tcpListenerLocalAddress.

Local Ip - The local IP address for this TCP connection

Local Port - The local port number for this TCP connection.

8.2.3TCP Connections



TCP CURRENT CONNECTIONS

Context Id	Local IPAddress Type	Local Ip	Local Port	Remote IPAddress Type	Remote IP	Remote Port	TCP State
0	IPV4	00:00:00:00	22	IPV4	00:00:00:00	0	Listen
0	IPV4	00:00:00:00	23	IPV4	00:00:00:00	0	Listen
0	IPV4	00:00:00:00	80	IPV4	00:00:00:00	0	Listen
0	IPV4	00:00:00:00	443	IPV4	00:00:00:00	0	Listen
1	IPV4	00:00:00:00	22	IPV4	00:00:00:00	0	Listen
1	IPV4	00:00:00:00	23	IPV4	00:00:00:00	0	Listen
1	IPV4	00:00:00:00	80	IPV4	00:00:00:00	0	Listen
1	IPV4	00:00:00:00	443	IPV4	00:00:00:00	0	Listen
1	IPV4	0a:87:10:b4	80	IPV4	0a:85:a0:5b	40907	Established

Fig: TCP Current Connections – Statistics Group

The *TCP Connections* link opens the **TCP Current Connections** Page.

TCP Current Connections page displays the information such as Remote IP, describing the status of the currently available TCP connections.

The table below lists the fields present in this page.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).This value ranges between 0 and 65535. The default value is 0.

Local IPAddressType - The address type of tcpConnectionLocalAddress

Local Ip - The local IP address for this TCP connection

Local Port - The local port number for this TCP connection Remote IPAddress

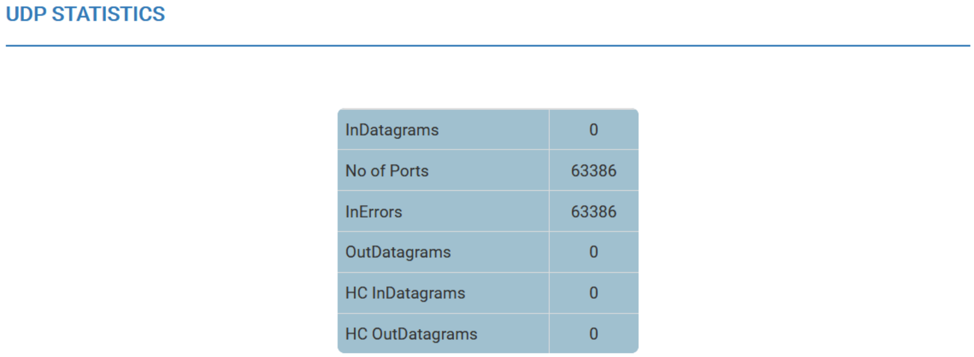
Type - The address type of tcpConnectionRemAddress.

Remote IP - The remote IP address for this TCP connection

Remote Port - The remote port number for this TCP connection.

TCP State - The state of this TCP connection.

8.2.4UDP Statistics



UDP STATISTICS

InDatagrams	0
No of Ports	63386
InErrors	63386
OutDatagrams	0
HC InDatagrams	0
HC OutDatagrams	0

Fig: UDP Statistics – Statistics Group

The *UDP Statistics* link opens the **UDP Statistic**s Page.

UDP Statistics page displays the UDP related statistics details s which allow the user to know the status of packets transferred using UDP.

The table below lists the fields present in this page.

InDatagrams - The total number of UDP delivered to UDP users.

No of Ports - The total number of received UDP datagrams for which there was no application at the destination port.

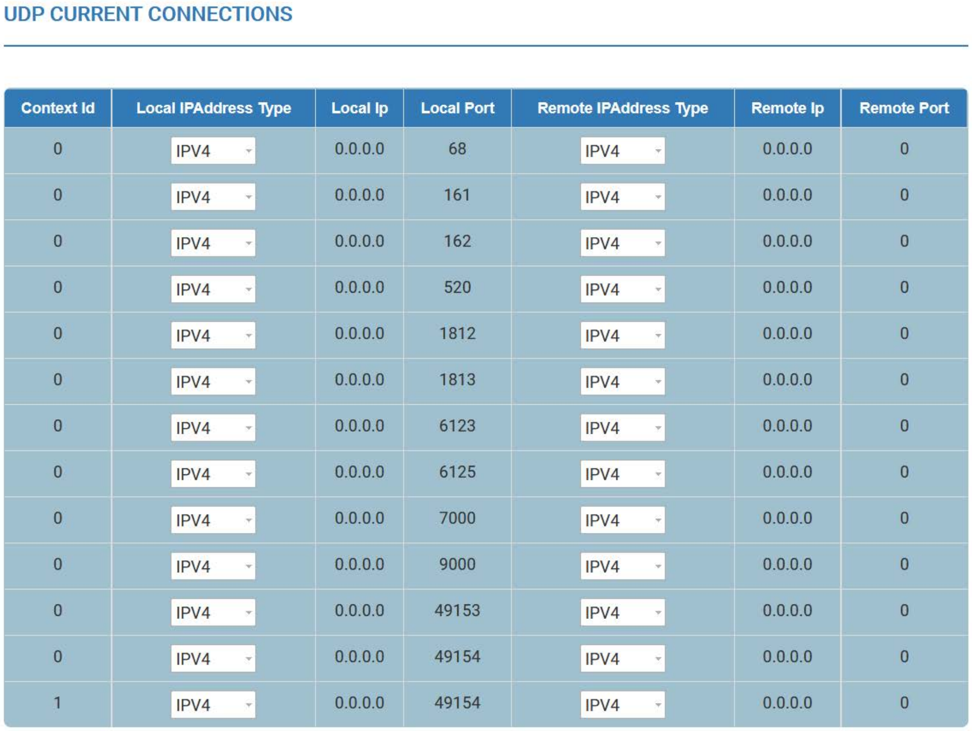
InErrors - The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

OutDatagrams - The total number of UDP datagrams sent from this entity.

HC InDatagrams - The total number of UDP datagrams delivered to UDP users, for devices that can receive more than 1 million UDP datagrams per second.

HC OutDatagrams - The total number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams per second.

8.2.5UDP Connections



UDP CURRENT CONNECTIONS

Context Id	Local IPAddress Type	Local Ip	Local Port	Remote IPAddress Type	Remote Ip	Remote Port
0	IPV4	0.0.0.0	68	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	161	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	162	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	520	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	1812	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	1813	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	6123	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	6125	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	7000	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	9000	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	49153	IPV4	0.0.0.0	0
0	IPV4	0.0.0.0	49154	IPV4	0.0.0.0	0
1	IPV4	0.0.0.0	49154	IPV4	0.0.0.0	0

Fig: UDP Current Connections – Statistics Group

The *UDP Connections* link opens the **UDP Current Connections** Page.

UDP Current Connections page displays the Local and Remote IP Address and Port type information about current available UDP connections.

The table below lists the fields present in this page.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).This value ranges between 0 and 65535. The default value is 0.

Local IPAddressType - The address type of udpEndpointLocalAddress.

Local Ip - The local IP address for this UDP endpoint.

Local Port - The local port number for this UDP endpoint.

Remote IPAddressType - The address type of udpEndpointRemoteAddress.

Remote IP - The remote IP address for this UDP endpoint.

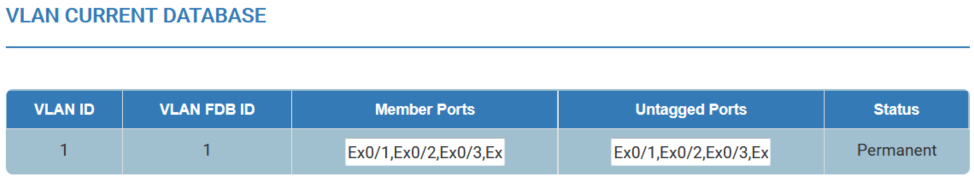
Remote Port - The remote port number for this UDP endpoint.

8.3 VLAN

VLAN link allows the user to view the VLAN statistics screens through the following tabs.

- CurrentdB
- PortStatistics
- MulticastTable
- CounterStatistics
- Capabilities
- MAC Address Table

8.3.1CurrentdB



VLAN CURRENT DATABASE

VLAN ID	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	1	Ex0/1,Ex0/2,Ex0/3,Ex	Ex0/1,Ex0/2,Ex0/3,Ex	Permanent

Fig: VLAN Current Database – Statistics Group

The *CurrentdB* link opens the **VLAN Current Database** Page.

VLAN Current Database page displays the information for a VLAN that is configured in the device or that is dynamically created as a result of GVRP requests received.

The table below lists the fields present in this page.

VLAN ID - VLAN identifer.

VLAN Name - Name string for this VLAN.

Member Ports - Index of member ports.

Tagged Ports - Index of tagged ports.

Untagged Ports - Index of untagged ports.

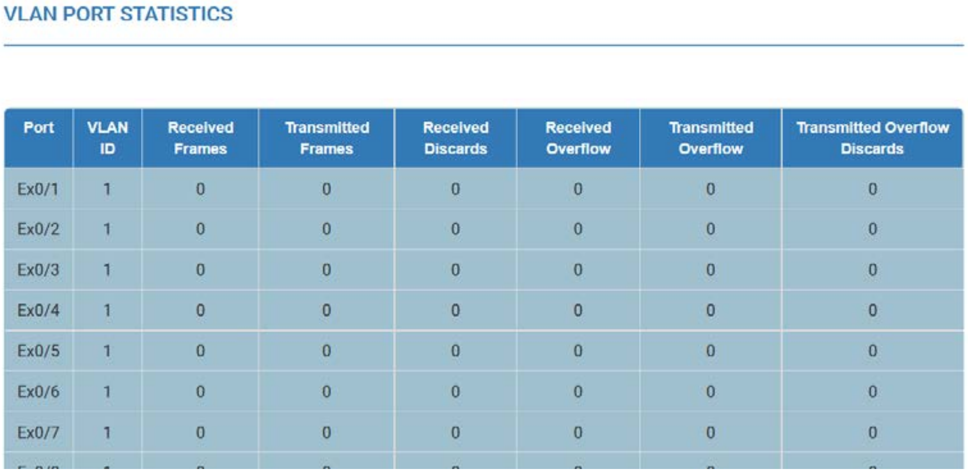
Forbidden Ports - Index of forbidden ports.

Access Ports - Index of access ports.

Trunk Ports - Index of trunk ports.

Status - VLAN status.

8.3.2 PortStatistics



VLAN PORT STATISTICS

Port	VLAN ID	Received Frames	Transmitted Frames	Received Discards	Received Overflow	Transmitted Overflow	Transmitted Overflow Discards
Ex0/1	1	0	0	0	0	0	0
Ex0/2	1	0	0	0	0	0	0
Ex0/3	1	0	0	0	0	0	0
Ex0/4	1	0	0	0	0	0	0
Ex0/5	1	0	0	0	0	0	0
Ex0/6	1	0	0	0	0	0	0
Ex0/7	1	0	0	0	0	0	0

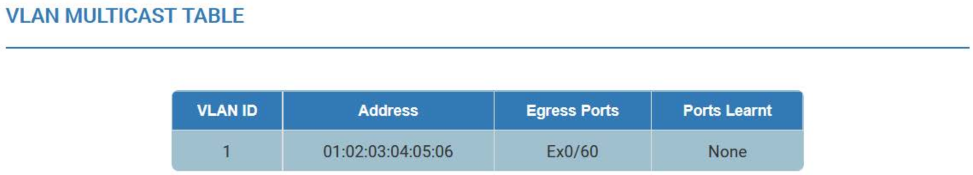
Fig: VLAN Port Statistics – Statistics Group

The *PortStatistics* link opens the **VLAN Port Statistics** Page.
VLAN Port Statistics page displays the VLAN related port specific statistics for all the interfaces.

The table below lists the fields present in this page.

Port - Index of port to the VLAN.
VLAN ID - VLAN identifier.
Received Frames - Number of valid frames received in the interface from the VLAN.
Transmitted Frames - Number of valid frames transmitted through the interface to the VLAN.
Received Discards - Number of discarded frames received in the interface from the VLAN.
Received Overflow - Number of overflowed frames received in the interface from the VLAN.
Transmitted Overflow -Number of overflowed frames transmitted through the interface to the VLAN.
Transmitted Overflow Discards - Number of discarded frames due to transmit overflow through the interface to the VLAN.

8.3.3 MulticastTable



VLAN MULTICAST TABLE

VLAN ID	Address	Egress Ports	Ports Learnt
1	01:02:03:04:05:06	Ex0/60	None

Fig: VLAN Multicast Table – Statistics Group

The *MulticastTable* link opens the **VLAN Multicast Table** Page.

VLAN Multicast Table page displays all static / dynamic unicast and multicast MAC entries created in the MAC address table.

The table below lists the fields present in this page.

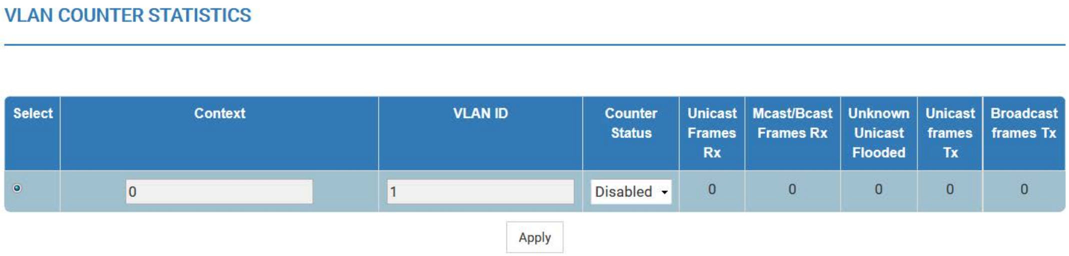
VLAN ID - VLAN identifier.

Address - VLAN address.

Egress Ports - Indexes of egress ports.

Ports Learnt - Indexes of ports on this VLAN is learned.

8.3.4 CounterStatistics



VLAN COUNTER STATISTICS

Select	Context	VLAN ID	Counter Status	Unicast Frames Rx	Mcast/Bcast Frames Rx	Unknown Unicast Flooded	Unicast frames Tx	Broadcast frames Tx
●	0	1	Disabled ▾	0	0	0	0	0

Fig: VLAN Counter Statistics – Statistics Group

The *CounterStatistics* link opens the **VLAN Counter Statistics** Page.

VLAN Counter Statistics page displays the unicast/broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.

Click the option button to select the VLAN ID, modify the counter status as enabled or disabled and click Apply to apply the configuration to the switch.

The table below lists the fields present in this page.

Context - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.

VLAN ID - VLAN identifier.

Unicast Frames Rx - Number of unicast packets received in the VLAN.

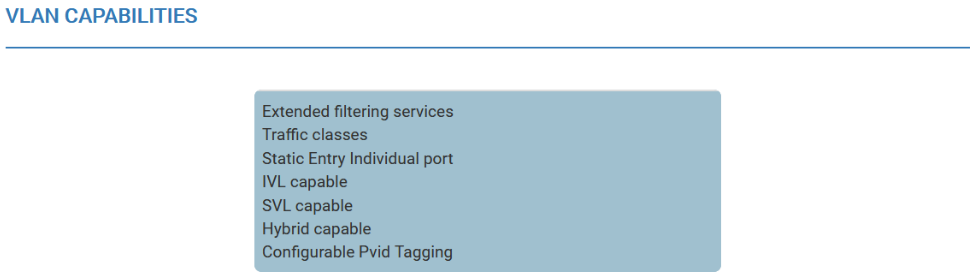
Mcast/Bcast Frames Rx - Number of multicast/broadcast packets received in the VLAN.

Unknown Unicast Flooded - Number of unknown unicast packets flooded in the VLAN.

Unicast frames Tx - Number of known unicast packets forwarded in the VLAN.

Broadcast frames Tx - Number of known broadcast packets forwarded in the VLAN.

8.3.5 Capabilities



VLAN CAPABILITIES

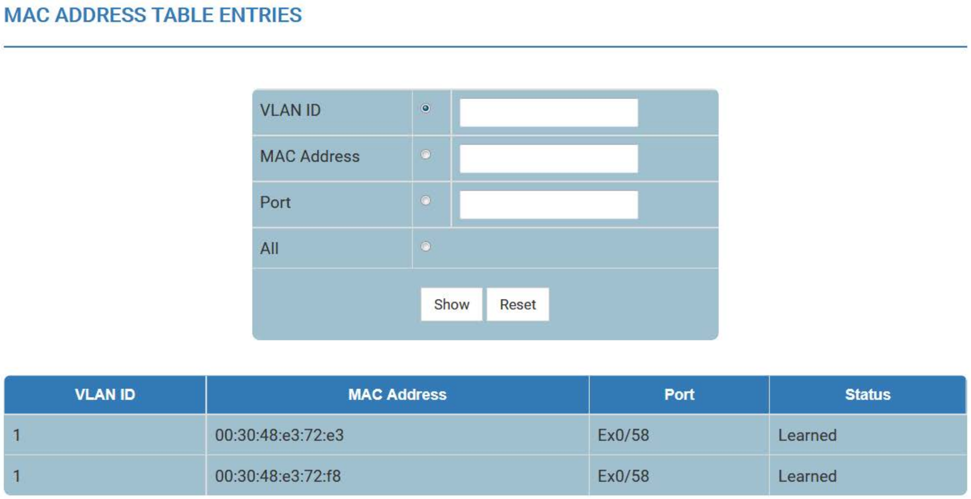
Extended filtering services
Traffic classes
Static Entry Individual port
IVL capable
SVL capable
Hybrid capable
Configurable Pvid Tagging

Fig: VLAN Capabilities – Statistics Group

The *Capabilities* link opens the **VLAN Capabilities** Page.

VLAN Capabilities page displays the list of VLAN features supported in the switch.

8.3.6 MAC Address Table


MAC ADDRESS TABLE ENTRIES

VLAN ID	●	
MAC Address	○	
Port	○	
All	○	

VLAN ID	MAC Address	Port	Status
1	00:30:48:e3:72:e3	Ex0/58	Learned
1	00:30:48:e3:72:f8	Ex0/58	Learned

Fig: Mac Address Table Entries – Statistics Group

The *MAC Address Table* link opens the **MAC Address Table** Page.

MAC Address Table page displays information about a specific about a specific MAC address/ VLAN ID/ Port or all entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

Click Show to display the required FDB entries for the specified VLAN ID, Mac address, port or all entries.

Click Reset to discard the information entered.

The table below lists the fields present in this page.

VLAN ID - VLAN identifier.

MAC Address - MAC address learned.

Port - Index of port where this entry is learned.

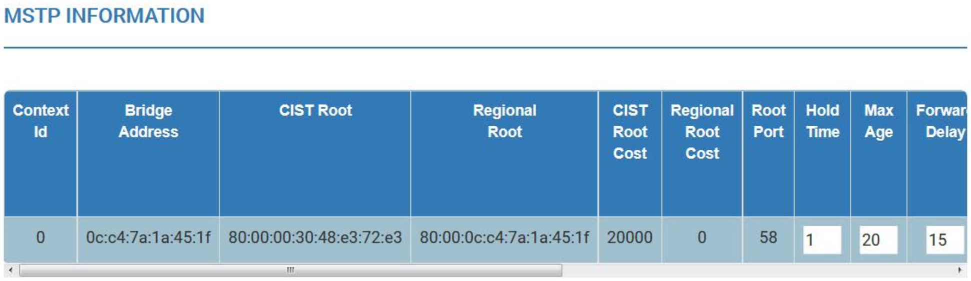
Status - Status of this entry

8.4 MSTP

The MSTP link allows the user to view the MSTP statistics screens through the following tabs.

- Information
- CIST Port Statistics
- MSTI Port Statistics

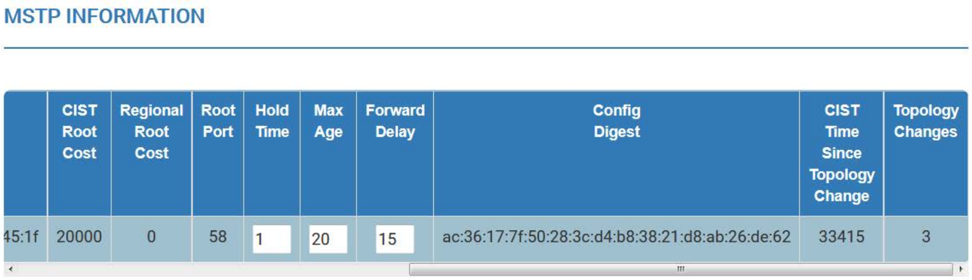
8.4.1Information



MSTP INFORMATION

Context Id	Bridge Address	CIST Root	Regional Root	CIST Root Cost	Regional Root Cost	Root Port	Hold Time	Max Age	Forwar Delay
0	0c:c4:7a:1a:45:1f	80:00:00:30:48:e3:72:e3	80:00:0c:c4:7a:1a:45:1f	20000	0	58	1	20	15

Fig: MSTP Information – Statistics Group-Part A



MSTP INFORMATION

	CIST Root Cost	Regional Root Cost	Root Port	Hold Time	Max Age	Forward Delay	Config Digest	CIST Time Since Topology Change	Topology Changes
45:1f	20000	0	58	1	20	15	ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62	33415	3

Fig: MSTP Information – Statistics Group-Part B

The *Information* link opens the **MSTP Information** Page.
MSTP Information page displays the information corresponding to the Multiple Spanning Tree protocol.

The table below lists the fields present in this page.
Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0).This value ranges between 0 and 65535. The default value is 0.
Bridge Address - The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with Mst Cist Bridge Priority or Mst Msti Bridge Priority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
CIST Root –
The bridge identifier of the Root of the common spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the CIST Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Regional Root Cost - The Cost of the path to the CIST Regional Root as seen from this bridge.

Root Port - The Port Number of the Port which offers the lowest path cost from this bridge to the CIST Root Bridge.

Hold Time - Hold time in seconds.

Max Age - Maximum age in seconds.

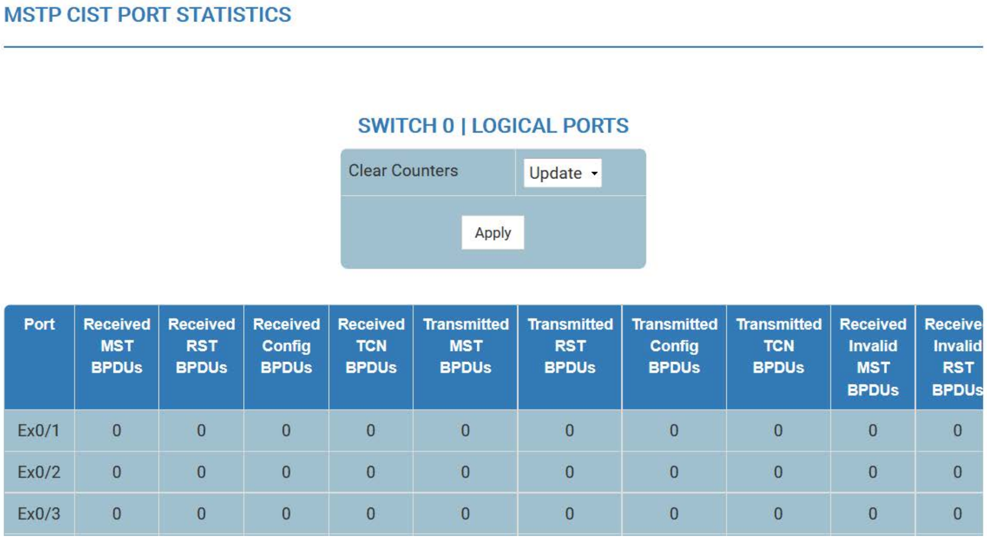
Forward Delay - Forward delay in seconds.

Config Digest   The Configuration Digest value for this Region.

CIST Time Since Topology Change - Time (in hundredths of a second) since topology last changed.

Topology Changes - Number of topology changes.

8.4.2 CIST Port Statistics



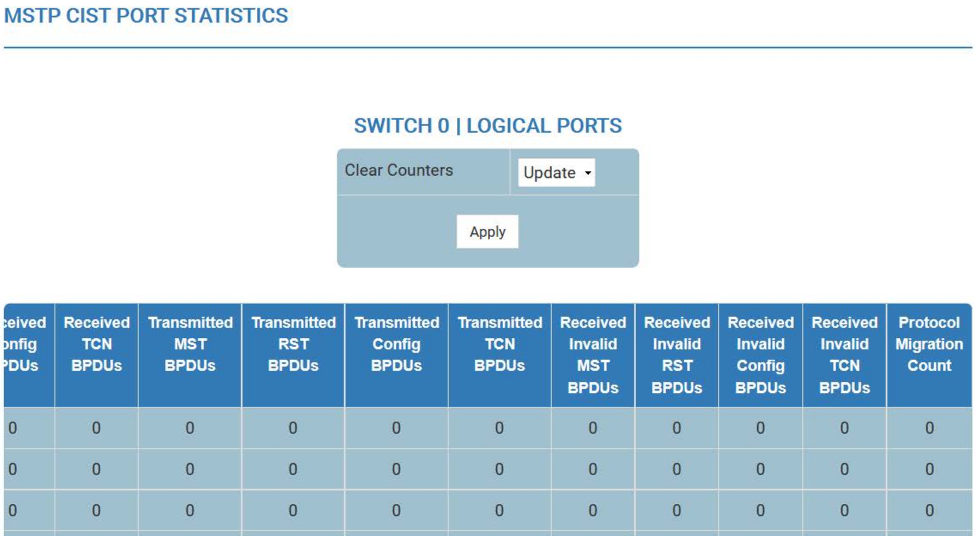
MSTP CIST PORT STATISTICS

SWITCH 0 | LOGICAL PORTS

Clear Counters	Update

Port	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Receive Invalid RST BPDUs
Ex0/1	0	0	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0	0	0

Fig: MSTP CIST Port Statistics – Statistics Group-Part A



MSTP CIST PORT STATISTICS

SWITCH 0 | LOGICAL PORTS

Clear Counters	Update

ceived onfig PDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0

Fig: MSTP CIST Port Statistics – Statistics Group-Part B

The *CIST Port Statistics* link opens the **MSTP CIST Port Statistics** Page.

MSTP CIST Port Statistics page displays a list of information maintained by every port for the Common Spanning Tree.

Click Apply to apply the configuration to the switch.

The table below lists the fields present in this page.

Clear Counters - Select an action to update or clear the statistics.

The list contains:

* Update - Update the statistics.

* Clear - Clear the statistics.

Port - Port index.

Received MST BPDUs - Number of MSTP BPDUs received.

Received RSTBPDUs - Number of RSTP BPDUs received.

Received Config BPDUs - Number of config BPDUs received.

Received TCN BPDUs - Number of topology change notification BPDUs received.

Transmitted MST BPDUs - Number of MSTP BPDUs transmitted.

Transmitted RST BPDUs - Number of RSTP BPDUs transmitted.

Transmitted Config BPDUs - Number of config BPDUs transmitted.

Transmitted TCN BPDUs - Number of topology change notification BPDUs transmitted.

Received Invalid MST BPDUs - Number of invalid MSTP BPDUs received.

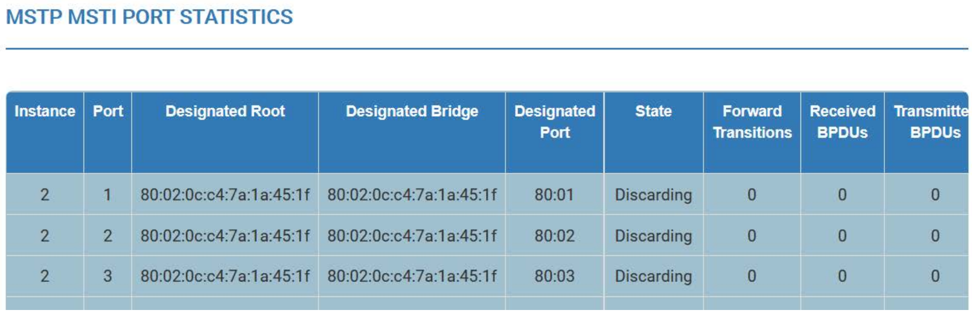
Received Invalid RST BPDUs - Number of invalid RSTP BPDUs received.

Received Invalid Config BPDUs - Number of invalid config BPDUs received.

Received Invalid TCN BPDUs - Number of invalid TCN BPDUs received.

Protocol Migration Count - Number of times protocol migration happened.

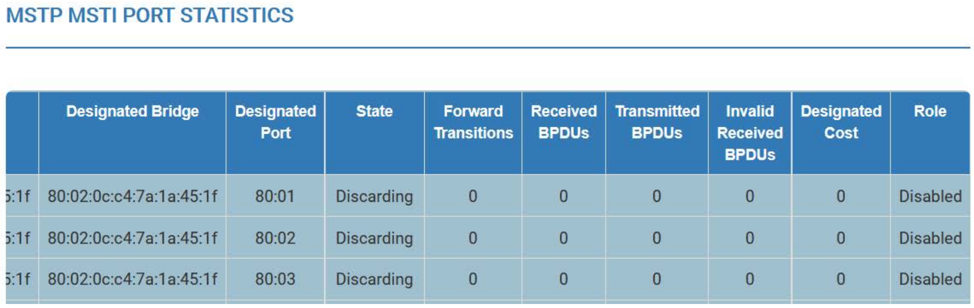
8.4.3 MSTI Port Statistics



MSTP MSTI PORT STATISTICS

Instance	Port	Designated Root	Designated Bridge	Designated Port	State	Forward Transitions	Received BPDUs	Transmitte BPDUs
2	1	80:02:0c:c4:7a:1a:45:1f	80:02:0c:c4:7a:1a:45:1f	80:01	Discarding	0	0	0
2	2	80:02:0c:c4:7a:1a:45:1f	80:02:0c:c4:7a:1a:45:1f	80:02	Discarding	0	0	0
2	3	80:02:0c:c4:7a:1a:45:1f	80:02:0c:c4:7a:1a:45:1f	80:03	Discarding	0	0	0

Fig: MSTP MSTI Port Statistics – Statistics Group-Part A



MSTP MSTI PORT STATISTICS

	Designated Bridge	Designated Port	State	Forward Transitions	Received BPDUs	Transmitted BPDUs	Invalid Received BPDUs	Designated Cost	Role
5:1f	80:02:0c:c4:7a:1a:45:1f	80:01	Discarding	0	0	0	0	0	Disabled
5:1f	80:02:0c:c4:7a:1a:45:1f	80:02	Discarding	0	0	0	0	0	Disabled
5:1f	80:02:0c:c4:7a:1a:45:1f	80:03	Discarding	0	0	0	0	0	Disabled

Fig: MSTP MSTI Port Statistics – Statistics Group-Part B

The *MSTI Port Statistics* link opens the **MSTP MSTI Port Statistics** Page.
MSTP MSTI Port Statistics page displays a list of information maintained by every port for each and every spanning tree instance.

The table below lists the fields present in this page.
Instance - MSTP instance Identifier.
Port - Port index.
Designated Root – Designated root bridge address.
Designated Bridge - Designated Bridge address.
Designated Port - Index of designated port for this MSTP instance.
State - Current state.
Forward Transitions - Number of times this port has transitioned to the Forwarding State for specific instance.
Received BPDUs - Number of BPDUs received.
Transmitted BPDUs - Number of BPDUs transmitted.
Invalid Received BPDUs - Number of invalid BPDUs received.

Designated Cost - The path cost of the Designated Port of the segment connected to this port.

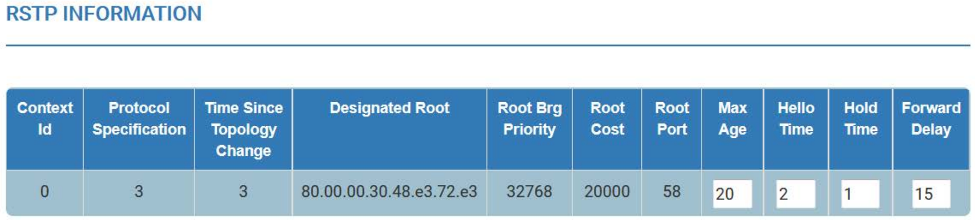
Role - Current role.

8.5 RSTP

The RSTP link allows the user to view the RSTP statistics screens through the following tabs.

- Information
- Port Statistics

8.5.1 Information



RSTP INFORMATION

Context Id	Protocol Specification	Time Since Topology Change	Designated Root	Root Brg Priority	Root Cost	Root Port	Max Age	Hello Time	Hold Time	Forward Delay
0	3	3	80.00.00.30.48.e3.72.e3	32768	20000	58	20	2	1	15

Fig: RSTP Information – Statistics Group

The *Information* link opens **RSTP Information** Page.

RSTP Information page displays the information on the bridges that supports the Spanning Tree protocol.

The table below lists the fields present in this page.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0). This value ranges between 0 and 65535. The default value is 0.

Protocol Specification -

Time Since Topology Change - Number of seconds since topology changed.

Designated Root – Designated Root bridge address.

Root Brg Priority - Priority of Root Bridge.

Root Cost - Cost to root.

Root Port - Index of the root port.

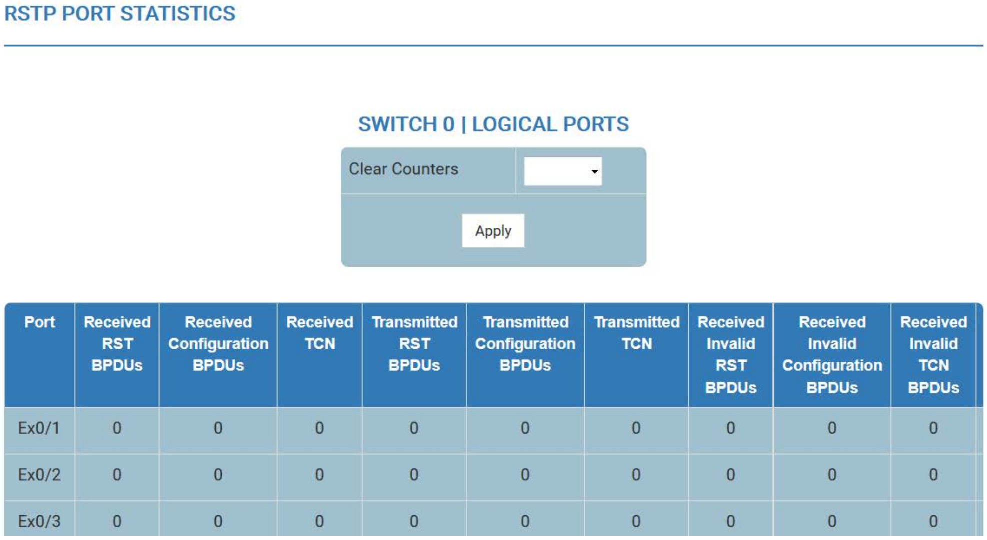
Max Age - Maximum age in seconds.

Hello Time - Hello time in seconds.

Hold Time - Hold time in seconds.

Forward Delay - Forward delay in seconds.

8.5.2 Port Statistics



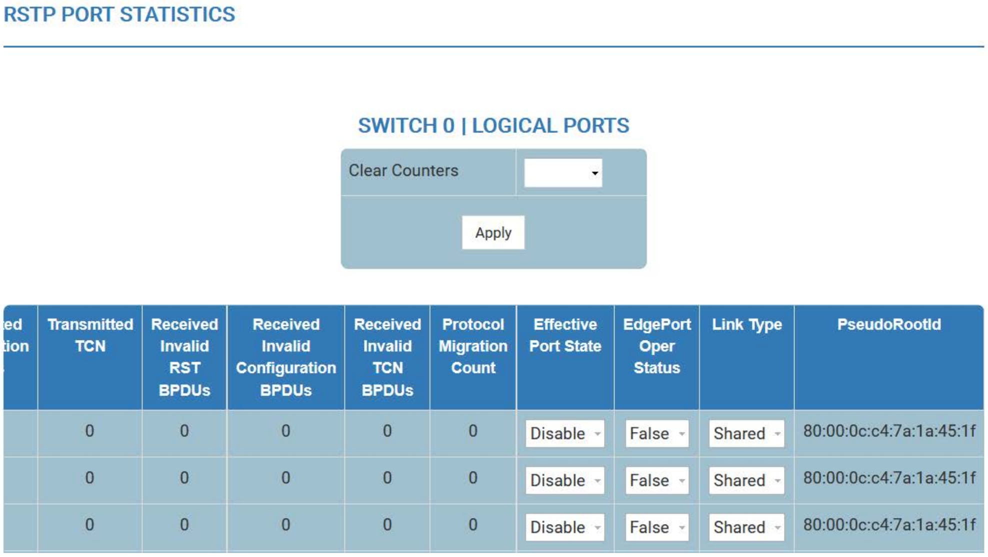
RSTP PORT STATISTICS

SWITCH 0 | LOGICAL PORTS

Clear Counters

Port	Received RST BPDUs	Received Configuration BPDUs	Received TCN	Transmitted RST BPDUs	Transmitted Configuration BPDUs	Transmitted TCN	Received Invalid RST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs
Ex0/1	0	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0	0

Fig: RSTP Port Statistics – Statistics Group-Part A



RSTP PORT STATISTICS

SWITCH 0 | LOGICAL PORTS

Clear Counters

ed tion	Transmitted TCN	Received Invalid RST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count	Effective Port State	EdgePort Oper Status	Link Type	PseudoRootId
	0	0	0	0	0	Disable	False	Shared	80:00:0c:c4:7a:1a:45:1f
	0	0	0	0	0	Disable	False	Shared	80:00:0c:c4:7a:1a:45:1f
	0	0	0	0	0	Disable	False	Shared	80:00:0c:c4:7a:1a:45:1f

Fig: RSTP Port Statistics – Statistics Group-Part B

The Port Statistics link opens RSTP Port Statistics Page.

RSTP Port Statistics page displays the various RSTP statistics involved with each of the port available in the system like the role, state, transition state machine, various packet statistics etc.

Click Apply to apply the configuration to the switch.

The table below lists the fields present in this page.

Clear Counters - Select a action to update or clear the statistics.

The list contains:

* Update - Update the statistics.

* Clear - Clear the statistics..

Port – Port Index.

Received RST BPDUs - Number of RSTP BPDUs received.

Received Configuration BPDUs - Number of config BPDUs received.

Received TCN BPDUs - Number of topology change notification BPDUs received.

Transmitted RST BPDUs - Number of RSTP BPDUs transmitted.

Transmitted RST BPDUs - Number of RSTP BPDUs transmitted.

Transmitted Configuration BPDUs - Number of config BPDUs transmitted.

Transmitted TCN BPDUs - Number of topology change notification BPDUs transmitted.

Received Invalid RST BPDUs - Number of invalid RSTP BPDUs received.

Received Invalid Configuration BPDUs - Number of invalid Configuration BPDUs received.

Received Invalid TCN BPDUs - Number of invalid TCN BPDUs received.

Protocol Migration Count - Number of times protocol migration happened.

Effective Port State -

EdgePort Oper Status – Operational status of Edge port.

Link Type - Broadcast or Point to point.

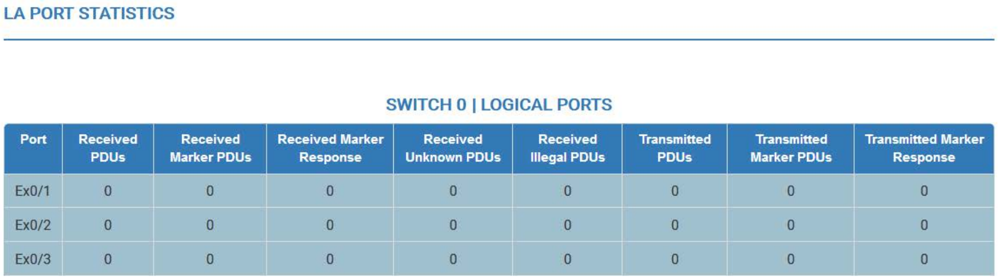
PseudoRootId - Unique identifier of pseudo root.

8.6 LA

The LA link allows the user to view the LA statistics screens through the following tabs.

- PortLACP Stats
- Neighbour Stats

8.6.1 PortLACP Stats



LA PORT STATISTICS

SWITCH 0 | LOGICAL PORTS

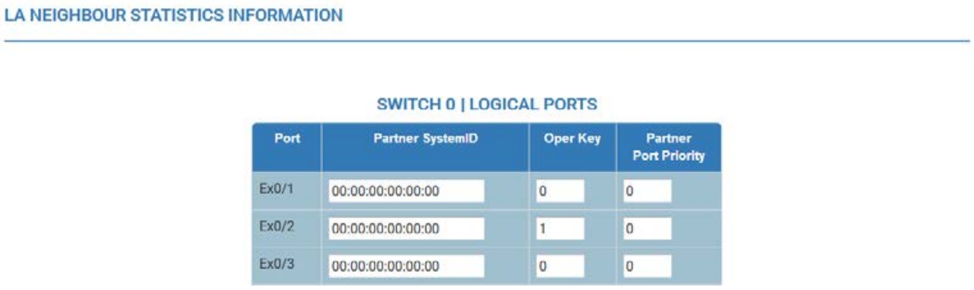
Port	Received PDUs	Received Marker PDUs	Received Marker Response	Received Unknown PDUs	Received Illegal PDUs	Transmitted PDUs	Transmitted Marker PDUs	Transmitted Marker Response
Ex0/1	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0

Fig: LA Port Statistics – Statistics Group

The *PortLACP Stats* link opens **LA Port Statistics** Page.
LA Port Statistics page displays the Link Aggregation Protocol statistics for each port on the device.

The table below lists the fields present in this page.
Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
Received PDUs - Number of LACP PDUs received.
Received Marker PDUs - Number of Marker PDUs received.
Received Marker Response - Number of Marker response PDUs received.
Received Unknown PDUs - Number of unknown PDUs received.
Received Illegal PDUs - Number of invalid PDUs received.
Transmitted PDUs - Number of LACP PDUs transmitted.
Transmitted Marker PDUs - Number of Marker PDUs transmitted.
Transmitted Marker Response - Number of Marker response PDUs transmitted.

8.6.2 Neighbour Stats



LA NEIGHBOUR STATISTICS INFORMATION

SWITCH 0 | LOGICAL PORTS

Port	Partner SystemID	Oper Key	Partner Port Priority
Ex0/1	00:00:00:00:00:00	0	0
Ex0/2	00:00:00:00:00:00	1	0
Ex0/3	00:00:00:00:00:00	0	0

Fig: Neighbor Statistics – Statistics Group

The *Neighbour Stats* link opens **LA Neighbour Statistics Information** Page.
LA Neighbour Statistics Information page displays the Neighbor statistics for each port on the device.

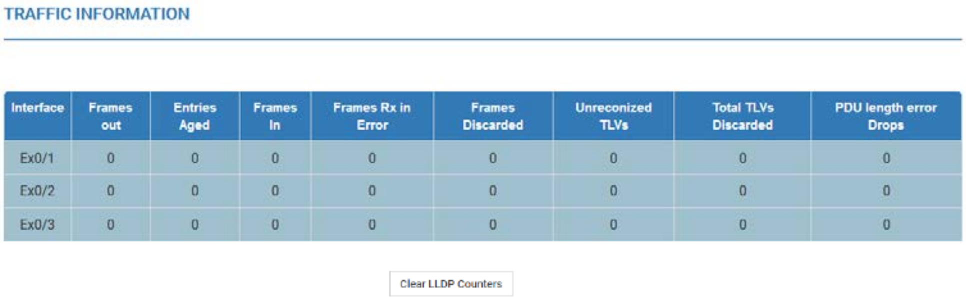
The table below lists the fields present in this page.
Port - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
Partner SystemID - Displays the 6-octet read-only MACAddress value representing the current value of the Aggregation Port's protocol Partner's System ID. A value of zero indicates that there is no known protocol Partner.
Oper Key - Displays the current operational value of the Key for the protocol Partner.
Partner Port Priority - Displays the priority value assigned to this Aggregation Port by the Partner.

8.7 LLDP

The LLDP link allows the user to view the LLDP statistics screens through the following tabs.

- Traffic
- Statistics
- Errors

8.7.1 Traffic



TRAFFIC INFORMATION

Interface	Frames out	Entries Aged	Frames In	Frames Rx in Error	Frames Discarded	Unreconized TLVs	Total TLVs Discarded	PDU length error Drops
Ex0/1	0	0	0	0	0	0	0	0
Ex0/2	0	0	0	0	0	0	0	0
Ex0/3	0	0	0	0	0	0	0	0

Fig: Neighbor Statistics – Statistics Group

The *Traffic* link opens **Traffic Information** Page.

Traffic Information page allows the user to view or clear the LLDP counters on specified interface.

Click Clear LLDP Counters to clear the LLDP counters on all interfaces.

The table below lists the fields present in this page.

Interface - Displays the Interface, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).

Frames out - The number of LLDP packets sent out from switch in the interface.

Entries Aged - The number of LLDP neighbor entries aged out.

Frames In - The number of LLDP packets received in by switch in the interface.

Frames Rx In Error - The number of LLDP packets received with Error.

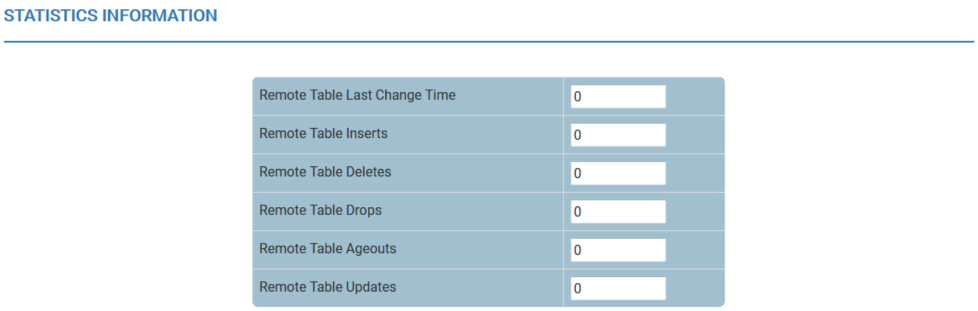
Frames Discarded - The number of LLDP packets received with Error.

Unrecognized TLVs - The number of LLDP packets discarded due to error and other failure conditions.

Total TLVs Discarded The number of TLVs discarded due to invalidity.

PDU length error Drops The number of LLDP packets dropped due to LLDPDU length error.

8.7.2 Statistics



STATISTICS INFORMATION

Remote Table Last Change Time	0
Remote Table Inserts	0
Remote Table Deletes	0
Remote Table Drops	0
Remote Table Ageouts	0
Remote Table Updates	0

Fig: Statistics Information – Statistics Group

The *Statistics* link opens **Statistics Information** Page.

Statistics Information page displays the LLDP remote table statistics information.

The table below lists the fields present in this page.

Remote Table Last Change Time - The time since the last time remote LLDP information table got changed.

Remote Table Inserts - Number of inserts happened on remote information table.

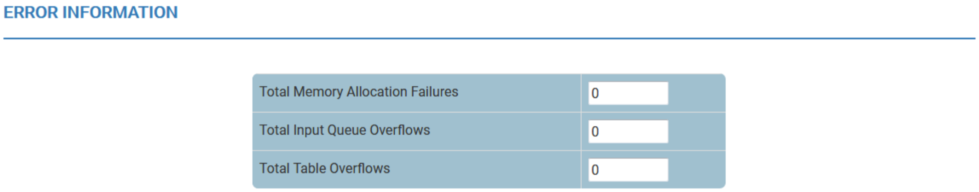
Remote Table Deletes - Number of deletes happened on remote information table.

Remote Table Drops - Number of drops happened on remote information table.

Remote Table Ageouts - Number of ageouts happened on remote information table.

Remote Table Updates - Number of times remote information table got updated.

8.7.3 Errors



ERROR INFORMATION

Total Memory Allocation Failures	0
Total Input Queue Overflows	0
Total Table Overflows	0

Fig: Error Information – Statistics Group

The *Errors* link opens **Error Information** Page.

Error Information page displays the details of LLDP error information.

The table below lists the fields present in this page.

Total Memory Allocation Failures - The number of memory allocation failed in LLDP feature.

Total Input Queue Overflows - The number of times the LLDP input queue overflowed.

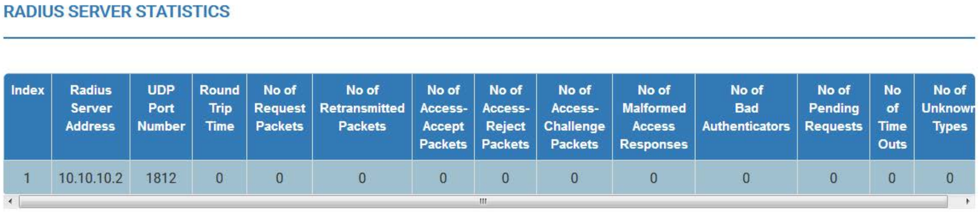
Total Table Overflows - The number of times the LLDP remote table got overflowed.

8.8 Radius

The Radius link allows the user to view the Radius statistics screens through the following tabs.

- Radius Server Statistics

8.8.1 Radius Server Statistics



RADIUS SERVER STATISTICS

Index	Radius Server Address	UDP Port Number	Round Trip Time	No of Request Packets	No of Retransmitted Packets	No of Access-Accept Packets	No of Access-Reject Packets	No of Access-Challenge Packets	No of Malformed Access Responses	No of Bad Authenticators	No of Pending Requests	No of Time Outs	No of Unknown Types
1	10.10.10.2	1812	0	0	0	0	0	0	0	0	0	0	0

Fig: Radius Server Statistics – Statistics Group

The *Radius Server Statistics* link opens **Radius Server Statistics** Page.
Radius Server Statistics page displays the RADIUS Server statistics.

The table below lists the fields present in this page.

Index - A number uniquely identifying each RADIUS Authentication server with which this client communicates.

Radius Server Address - IP address of the RADIUS Authentication server.

UDP Port Number - The UDP port the client is using to send requests to this server.

Round Trip Time - Round trip time in seconds.

No of Request Packets - Number of request packets transmitted.

No of Retransmitted Packets - Number of packets retransmitted.

No of Access-Accept Packets - Number of accept packets.

No of Access-RejectPackets - Number of reject packets.

No of Access-Challenge Packets - Number of challenge packets.

No of Malformed Access Responses - Number of invalid access responses received.

No of Bad Authenticators - Number of failed authentications.

No of Pending Requests - Number of currently pending requests.

No of Time Outs - Number of time outs happened.

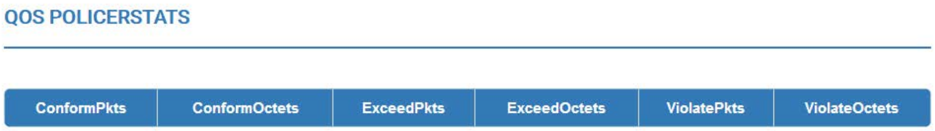
No of Unknown Types - Number of unknown types received.

8.9 QoS

The QoS link allows the user to view the QoS statistics screens through the following tabs.

- PolicerStats
- Cos Stats

8.9.1 PolicerStats



QOS POLICERSTATS

ConformPkts	ConformOctets	ExceedPkts	ExceedOctets	ViolatePkts	ViolateOctets

Fig: QoS PolicerStats– Statistics Group

The *PolicerStat* link opens **QoS PolicerStats** Page.

QoS PolicerStats page displays the statistics for the QoS policer.

The table below lists the fields present in this page.

ConformPkts - Number of Packets marked down as conforming(Green) traffic by this policer.

ConformOctets - Number of Octets of traffic marked down as conforming(Green) by this policer.

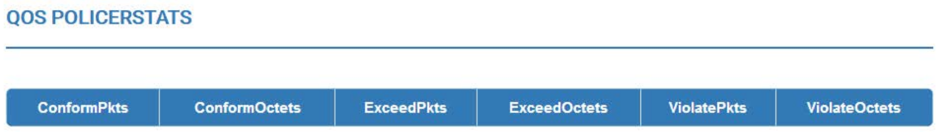
ExceedPkts - Number of Packets marked down as exceeding(Yellow) traffic by this policer.

ExceedOctets - Number of Octets of traffic marked down as exceeding(Yellow) by this policer.

ViolatePkts - Number of Packets marked down as violating(Red) traffic by this policer.

ViolateOctets - Number of Octets of traffic marked down as violating(Red) by this policer.

8.9.2 Cos Stats



QOS POLICERSTATS

ConformPkts	ConformOctets	ExceedPkts	ExceedOctets	ViolatePkts	ViolateOctets

Fig: QoS CoS Stats– Statistics Group

The *Cos Stats* link opens **QoS CoS Stats** Page.

QoS CoS Stats page displays the statistics for the QoS COS queue.

The table below lists the fields present in this page.

Interface - Name of the interface.

Q Id ID of thid CoS Queue.

CoSQEnQPkts - Number of packets enqueued in this CoS Queue.

CoSQEnQBytes - Number of bytes enqueued in this CoS Queue.

CoSQDeQPkts - Number of packets de-queued from this CoS Queue.

CoSQDeQBytes - Number of bytes de-queued from this CoS Queue.

CoSDiscardPkts - Number of packets discarded from this CoS Queue.

CoSQDiscardBytes - Number of bytes discarded from this CoS Queue.

CoSQStatsOccupancy - Number of bytes currently occupied in the CoS Queue.

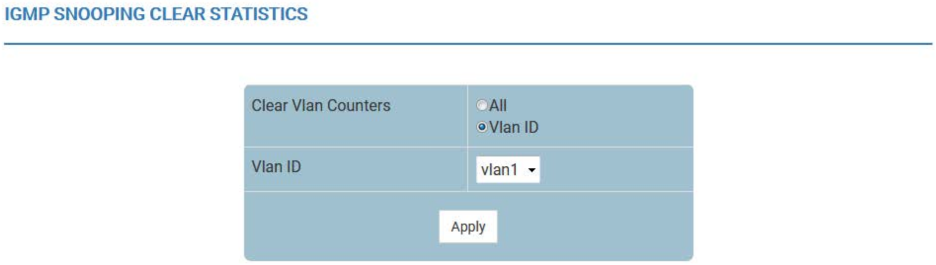
CoSQStatsCongMgntAlgoDrop - Number of bytes discarded due to congestion management algorithm (RED/WRED) in this CoS Queue.

8.10 IGMP Snooping

The IGMP Snooping link allows the user to view the IGMP Snooping related statistics screens through the following tabs.

- IGS Clear Statistics
- IGS Statistics
- IGS V3 Statistics

8.10.1 IGS Clear Statistics



IGMP SNOOPING CLEAR STATISTICS

Clear Vlan Counters	○ All ● Vlan ID
Vlan ID	vlan1

Fig: IGMP Snooping Clear Statistics– Statistics Group

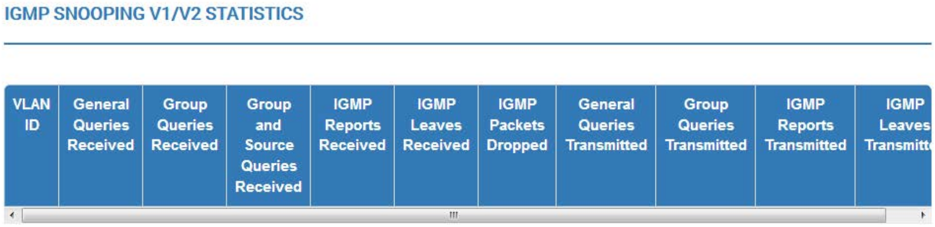
The *IGMP Snooping Clear Statistics* link opens **IGMP Snooping Clear Statistics** Page. IGMP Snooping Clear Statistics page displays the IGMP snooping clear statistics.

To configure IGMP Snooping Clear Statistics, configure the parameters described below and click Apply to apply the configuration to the switch.

The table below lists the fields present in this page.

Clear Vlan Counters - Select a particular vlan or all the vlan to clear the IGMP statistics.
By default, Clear Vlan Counters is set as Vlan ID.
The list contains:
* All - Select all the vlan.
* Vlan ID - Select a particular vlan.
Vlan ID - Select the vlan identifier.

8.10.2 IGS Statistics



IGMP SNOOPING V1/V2 STATISTICS

VLAN ID	General Queries Received	Group Queries Received	Group and Source Queries Received	IGMP Reports Received	IGMP Leaves Received	IGMP Packets Dropped	General Queries Transmitted	Group Queries Transmitted	IGMP Reports Transmitted	IGMP Leaves Transmitt

Fig: IGMP Snooping V1/V2 Statistics– Statistics Group

The *IGS Statistics* link opens **IGMP Snooping V1/V2 Statistics** Page.

IGMP Snooping V1/V2 Statistics page displays the IGMP snooping statistics pertaining to IGMP snooping v1 and v2.

The table below lists the fields present in this page.

VLAN ID - VLAN identifier.

General Queries Received - Number of general query packets received.

Group Queries Received - Number of group query packets received.

Group and Source Queries Received - Number of group and source query packets received.

IGMP Reports Received - Number of IGMP report packets received.

IGMP Leaves Received - Number of IGMP leave packets received.

IGMP Packets Dropped - Number of IGMP dackets dropped.

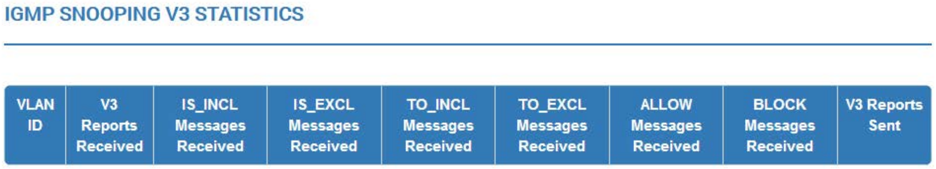
General Queries Transmitted - Number of general query packets transmitted.

Group Queries Transmitted - Number of group query packets transmitted.

IGMP Reports Transmitted - Number of IGMP report packets transmitted.

IGMP Leaves Transmitted - Number of IGMP leave packets transmitted.

8.10.3 IGS V3 Statistics



IGMP SNOOPING V3 STATISTICS

VLAN ID	V3 Reports Received	IS_INCL Messages Received	IS_EXCL Messages Received	TO_INCL Messages Received	TO_EXCL Messages Received	ALLOW Messages Received	BLOCK Messages Received	V3 Reports Sent

Fig: IGMP Snooping V3 Statistics– Statistics Group

The *IGS V3 Statistics* link opens **IGMP Snooping V3 Statistics** Page.
IGMP Snooping V3 Statistics page displays the IGMP snooping statistics pertaining to IGMP snooping v3.

The table below lists the fields present in this page.

VLAN ID - VLAN identifier.

V3 Reports Received - Number of Reports messages received

IS_INCL Messages Received - Number of messages received with is include field.

IS_EXCL Messages Received - Number of messages received with is exclude field.

TO_INCL Messages Received - Number of messages received with to include field.

TO_EXCL Messages Received - Number of messages received with to exclude field.

ALLOW Messages Received - Number of allow messages received.

BLOCK Messages Received - Number of block messages received.

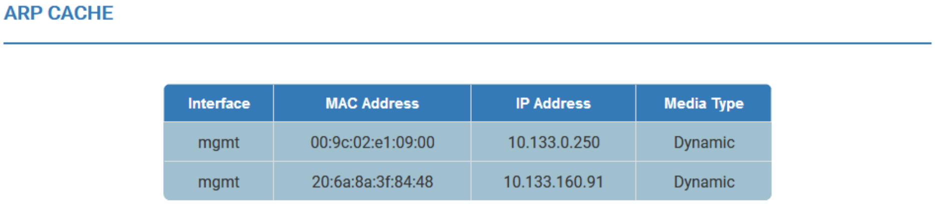
V3 Reports Sent - Number of V3 reports transmitted.

8.11 IP

The IP link allows the user to view the IPv4 related statistics screens through the following tabs.

- ARP Cache
- ICMP Statistics
- IPV4 IfSp Stats
- IPV4 SysSp Stats

8.11.1 ARP Cache



ARP CACHE

Interface	MAC Address	IP Address	Media Type
mgmt	00:9c:02:e1:09:00	10.133.0.250	Dynamic
mgmt	20:6a:8a:3f:84:48	10.133.160.91	Dynamic

Fig: ARP Cache– Statistics Group

The *ARP Cache* link opens **ARP Cache** Page.

ARP Cache page displays the ARP cache related statistics information such as MAC address for all interfaces of the switch.

The table below lists the fields present in this page.

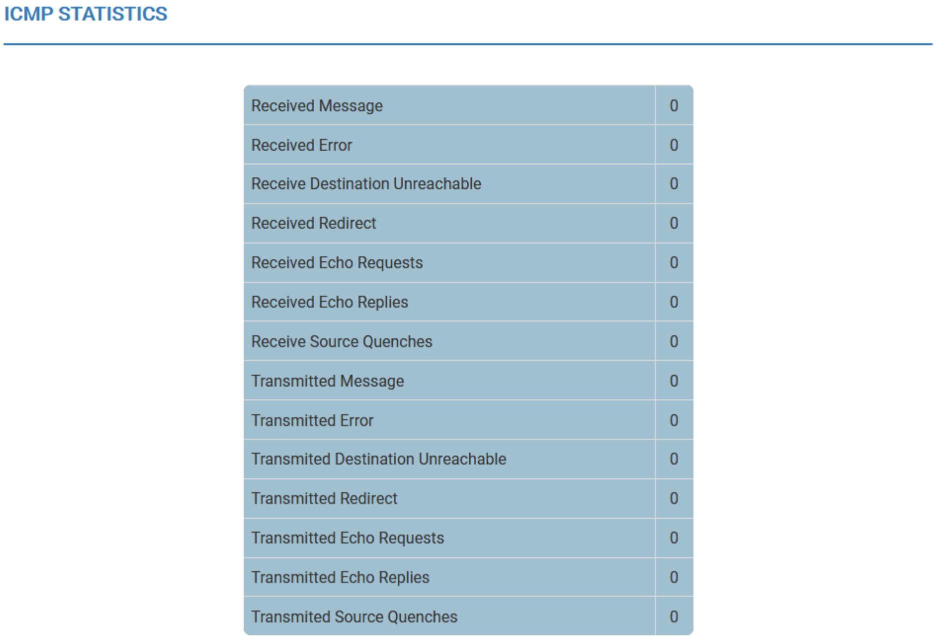
Interface – The ARP entry is learnt from the Interface.

MAC Address - MAC Address from which this ARP entry is learned.

IP Address IP Address from which this ARP entry is learned.

Media Type Static ARP or dynamic ARP.

8.11.2 ICMP Statictics



ICMP STATISTICS

Received Message	0
Received Error	0
Receive Destination Unreachable	0
Received Redirect	0
Received Echo Requests	0
Received Echo Replies	0
Receive Source Quenches	0
Transmitted Message	0
Transmitted Error	0
Transmited Destination Unreachable	0
Transmitted Redirect	0
Transmitted Echo Requests	0
Transmitted Echo Replies	0
Transmited Source Quenches	0

Fig: ICMP Statistics– Statistics Group

The *ICMP Statistics* link opens **ICMP Statistics** Page.

ICMP Statistics page displays the ICMP transmission and reception related statistics information.

The table below lists the fields present in this page.

Received Message – The total received number of ICMP message.

Received Error - The total received number of ICMP message but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

Receive Destination Unreachable The number of ICMP Destination Unreachable messages received.

Received Redirect - The number of ICMP Redirect messages received.

Received Echo Requests - The number of ICMP Echo Request messages received.

Received Echo Replies - The number of ICMP Echo Reply messages received.

Receive Source Quenches - The number of ICMP Source Quench messages received.

Transmitted Message - The total number of ICMP messages which this entity attempted to send.

Transmitted Error - The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers.

Transmited Destination Unreachable - The number of ICMP Destination Unreachable messages sent.

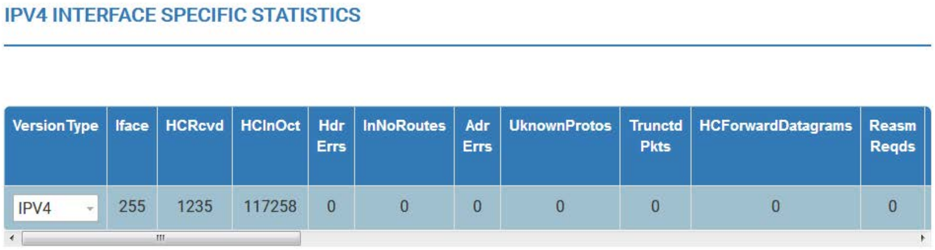
Transmitted Redirect - The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

Transmitted Echo Requests - The number of ICMP Echo Request messages sent.

Transmitted Echo Replies - The number of ICMP Echo Reply messages sent.

Transmited Source Quenches - The number of ICMP Source Quench messages sent.

8.11.3 IPV4 IfSp Stats



IPV4 INTERFACE SPECIFIC STATISTICS

VersionType	Iface	HCRcvd	HCInOct	Hdr Errs	InNoRoutes	Adr Errs	UknownProtos	Trunctd Pkts	HCForwardDatagrams	Reasm Reqds
IPV4	255	1235	117258	0	0	0	0	0	0	0

Fig: IPV4 Interface Specific Statistics– Statistics Group

The *IPV4 IfSp Stats* link opens **IPV4 Interface Specific Statistics** Page.
IPV4 Interface Specific Statistics page displays the IPv4 specific statistics information such as HCInOct, for all interfaces available in the switch.

The table below lists the fields present in this page.
VersionType – This entry‘s IP version.
Iface- The index value to uniquely identifies the interface.
HCRcvd - The total number of input IP datagrams received, including those received in error.
HCInOct - The total number of octets received in input IP datagrams, including those received in error.
Hdr Errs - The number of input IP datagrams discarded due to errors in their IP headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IP options, etc.
InNoRoutes - The number of input IP datagrams discarded because no route could be found to transmit them to their destination.
Adr Errs - The number of input IP datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity.
UknownProtos - The number of locally-addressed IP datagrams received successfully but discarded because of an unknown or unsupported protocol.
Trunctd Pkts - The number of input IP datagrams discarded because the datagram frame didn't carry enough data.
HCForwardDatagrams - The number of input datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination.
Reasm Reqds - The number of IP fragments received that needed to be reassembled at this interface.
Reasm OKs - The number of IP datagrams successfully reassembled.

Reasm Fails - The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).

Discdrs - The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but were discarded (e.g., for lack of buffer space).

HCInDelivers - The total number of datagrams successfully delivered to IP user-protocols (including ICMP).

HCOut Rqst - The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

HCOut FwdDgms - The number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination.

Out Discards - The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space).

Out FragRqds - The number of IP datagrams that would require fragmentation in order to be transmitted.

Out FragOks - The number of IP datagrams that have been successfully fragmented.

Out FragFails - The number of IP datagrams that have been discarded because they needed to be fragmented but could not be.

Frag Creates - The number of output datagram fragments that have been generated as a result of IP fragmentation.

HcOut Transmits - The total number of IP datagrams that this entity supplied to the lower layers for transmission.

HCOutOct - The total number of octets in IP datagrams delivered to the lower layers for transmission.

HCRcvd Mcast Pkts - The number of IP multicast datagrams received.

HCRcvd Mcast Octs - The total number of octets received in IP multicast datagrams.

HCSend Mcast Pkts - The number of IP multicast datagrams transmitted.

HCSend Mcast Octs - The total number of octets transmitted in IP multicast datagrams.

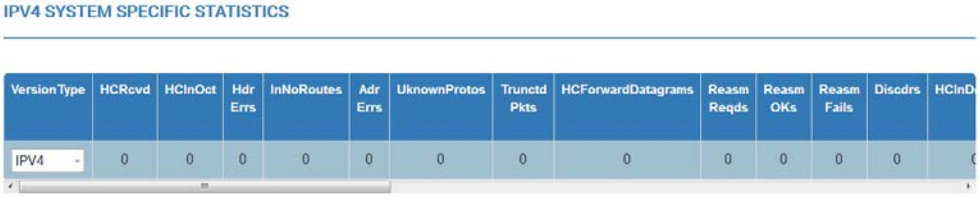
HCRcvd Bcast Pkts - The number of IP broadcast datagrams received.

HCSend Bcast Pkts - The number of IP broadcast datagrams transmitted.

DisConty time - The value of sysUpTime on the most recent occasion at which any one or more of this entry's counters suffered a discontinuity.

Refresh Rate - The minimum reasonable polling interval for this entry.

8.11.4 IPV4 SysSp Stats



IPV4 SYSTEM SPECIFIC STATISTICS

VersionType	HCRcvd	HCInOct	Hdr Errs	InNoRoutes	Adr Errs	UknownProtos	Trunctd Pkts	HCForwardDatagrams	Reasm Reqds	Reasm OKs	Reasm Fails	Discdrs	HCInD
IPV4	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig: IPV4 IPV4 System Specific Statistics– Statistics Group

The *IPV4 SysSp Stats* link opens **IPV4 System Specific Statistics** Page.
IPV4 System Specific Statistics page displays the IPv4 specific global statistics information such as HCRcvd, forthe switch.

The table below lists the fields present in this page.
VersionType - The IP version of this entry.
HCRcvd - The total number of input IP datagrams received, including those received in error.
HCInOct - The total number of octets received in input IP datagrams, including those received in error.
Hdr Errs - The number of input IP datagrams discarded due to errors in their IP headers, including version number mismatch, other packet format errors, hop count exceeded, errors discovered in processing their IP options, etc.
InNoRoutes - The number of input IP datagrams discarded because no route could be found to transmit them to their destination.
Adr Errs - The number of input IP datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity.
UknownProtos - The number of locally-addressed IP datagrams received successfully but discarded because
of an unknown or unsupported protocol.
Trunctd Pkts - The number of input IP datagrams discarded because the datagram frame didn't carry enough data.
HCForwardDatagrams - The number of input datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination.
Reasm Reqds- - The number of IP fragments received that needed to be reassembled at this interface.
Reasm OKs - The number of IP datagrams successfully reassembled.
Reasm Fails - The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).

Discdrs - The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but were discarded (e.g., for lack of buffer space).

HCInDelivers - The total number of datagrams successfully delivered to IP user-protocols (including ICMP).

HCOut Rqst - The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

HCOut FwdDgms - The number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination.

Out Discards The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space).

Out FragRqds - The number of IP datagrams that would require fragmentation in order to be transmitted.

Out FragOks - The number of IP datagrams that have been successfully fragmented.

Out FragFails - The number of IP datagrams that have been discarded because they needed to be fragmented but could not be.

Frag Creates - The number of output datagram fragments that have been generated as a result of IP fragmentation.

HcOut Transmits - The total number of IP datagrams that this entity supplied to the lower layers for transmission.

HCOutOct - The total number of octets in IP datagrams delivered to the lower layers for transmission.

HCRcvd Mcast Pkts - The number of IP multicast datagrams received.

HCRcvd Mcast Octs - The total number of octets received in IP multicast datagrams.

HCSend Mcast Pkts - The number of IP multicast datagrams transmitted.

HCSend Mcast Octs - The total number of octets transmitted in IP multicast datagrams.

HCRcvd Bcast Pkts - The number of IP broadcast datagrams received.

HCSend Bcast Pkts - The number of IP broadcast datagrams transmitted.

DisConty time - The value of sysUpTime on the most recent occasion at which any one or more of this entry's counters suffered a discontinuity.

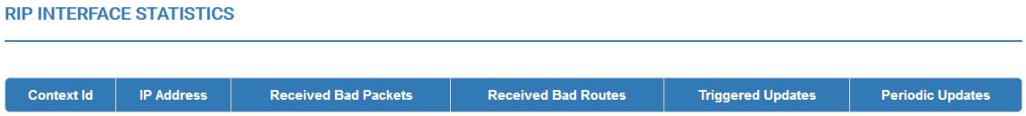
Refresh Rate - The minimum reasonable polling interval for this entry.

8.12 RIP

The RIP link allows the user to view the RIP statistics screens through the following tabs.

- Interface Statistics

8.12.1 Interface Statistics



RIP INTERFACE STATISTICS

Context Id	IP Address	Received Bad Packets	Received Bad Routes	Triggered Updates	Periodic Updates

Fig: RIP Interface Statistics– Statistics Group

The *Interface Statistics* link opens **RIP Interface Statistics** Page.

RIP Interface Statistics displays the Routing Information Protocol statistics for each of the interface in the device.

The table below lists the fields present in this page.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. By default, the basic configuration of the protocols having MI support are mapped to the default context ID (0). This value ranges between 0 and 65535. The default value is 0.

IP Address - The IP Address of this system on the indicated subnet.

Received Bad Packets - The number of RIP response packets received by the RIP process which were subsequently discarded for any reason (e.g. a version 0 packet, or an unknown command type).

Received Bad Routes - The number of routes in valid RIP packets which were ignored for any reason (e.g. unknown address family or invalid metric).

Triggered Updates - The number of triggered RIP updates actually sent on this interface.

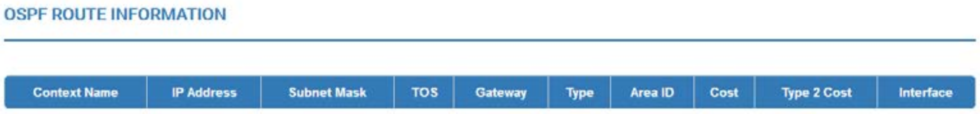
Periodic Updates - The number of Periodic RIP updates sent on this interface.

8.13 OSPF

The OSPF link allows the user to view the OSPF statistics screens through the following tabs.

- Route Information
- Link State Database
- Redundancy Information

8.13.1 Route Information



OSPF ROUTE INFORMATION

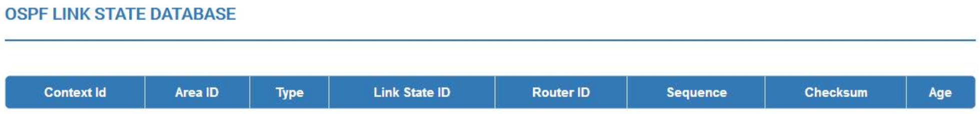
Context Name	IP Address	Subnet Mask	TOS	Gateway	Type	Area ID	Cost	Type 2 Cost	Interface

Fig: OSPF Route Information– Statistics Group

The *Router Information* link opens **OSPF Route Information** Page.
OSPF Route Information page displays the information regarding the OSPF routes.

The table below lists the fields present in this page.
Context Name –The context alias name this Route entry belongs to.
IP Address - IP Address of the route.
Subnet Mask - IP Address Mask of the route.
TOS - IP TOS of the route.
Gateway - IP Next Hop of the route.
Type - Type of the route.
Area ID - Area ID associated with the route.
Cost - It is a Type 1 external metrics which is expressed in the same units as OSPF interface cost (i.e. In terms of the OSPF link state metric). If Type1 and Type2 cost are present, Type1 external metrics always take precedence.
Type 2 Cost - Type 2 external metrics are configured with the cost greater than any path internal to the AS. Use of Type 2 external metrics assumes that routing between AS is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link state metrics.
Interface - Interface Index associated with the route

8.13.2 Link State Database



OSPF LINK STATE DATABASE

Context Id	Area ID	Type	Link State ID	Router ID	Sequence	Checksum	Age

Fig: OSPF Link State Database– Statistics Group

The *Link State Database* link opens **OSPF Link State Database** Page.
OSPF Link State Database page displays the information on a single link state advertisement.

The table below lists the fields present in this page.

Context Id - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. y default, the basic configuration of the protocols having MI support are mapped to the default context ID (0). This value ranges between 0 and 65535. The default value is 0.

Area ID - The 32 bit identifier of the Area from which the LSA was received.

Type - The type of the link state advertisement.

Link State ID - An LS Type Specific field containing either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement.

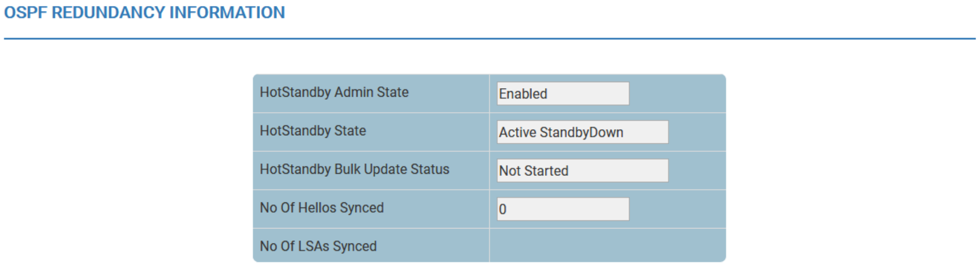
Router ID - The 32 bit number that uniquely identifies the originating router in the Autonomous System.

Sequence - The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number the more recent the advertisement.

Checksum - This field is the checksum of the complete contents of the advertisement, excepting the age field.

Age - This field is the age of the link state advertisement in seconds.

8.13.3 Redundancy Information



OSPF REDUNDANCY INFORMATION

HotStandby Admin State	Enabled
HotStandby State	Active StandbyDown
HotStandby Bulk Update Status	Not Started
No Of Hellos Synced	0
No Of LSAs Synced	

Fig: OSPF Redundancy Information– Statistics Group

The *Redundancy Information* link opens **OSPF Redundancy Information** Page.

OSPF Redundancy Information page displays the information for the state of OSPF redundancy.

The table below lists the fields present in this page.

HotStandby Admin State - High Availability feature enabled or disabled in OSPF.

HotStandby State - Internal State of the OSPF instance.

HotStandby Bulk Update Status - Status of dynamic bulk update between active and dynamic OSPF instance.

No Of Hellos Synced - Total number of hello packets synced.

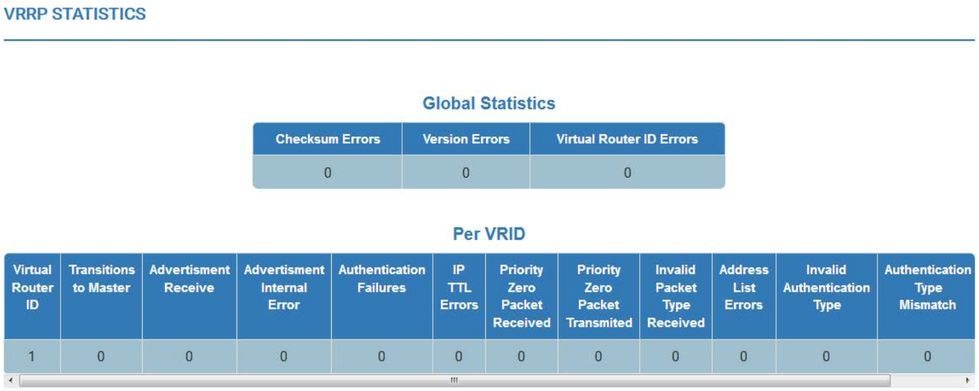
No Of LSAs Synced - Total number of LSAs synced.

8.14 VRRP

The VRRP link allows the user to view the VRRP statistics screens through the following tabs.

- VRRP Statistics

8.14.1 VRRP Statistics



VRRP STATISTICS

Global Statistics

Checksum Errors	Version Errors	Virtual Router ID Errors
0	0	0

Per VRID

Virtual Router ID	Transitions to Master	Advertisment Receive	Advertisment Internal Error	Authentication Failures	IP TTL Errors	Priority Zero Packet Received	Priority Zero Packet Transmited	Invalid Packet Type Received	Address List Errors	Invalid Authentication Type	Authentication Type Mismatch
1	0	0	0	0	0	0	0	0	0	0	0

Fig: VRRP Statistics– Statistics Group

The *VRRP Statistics* link opens **VRRP Statistics** Page.

VRRP Statistics page displays the VRRP Global Statistics and per VRID Statistics.

The table below lists the fields present for Global Statistics in this page.

Checksum Errors - Number of checksum errors happened.

Version Errors - Number of version errors happened.

Virtual Router ID Errors - Number of virtual router ID errors happened.

The table below lists the fields present for per VRID Statistics in this page.

Virtual Router ID - Virtual router identifier.

Transitions to Master - Number of transitions as Master.

Advertisment Receive Number of advertisement packets received.

Advertisment Internal Error - Number of advertisement errors happened.

Authentication Failures - Number of authentication failures.

IP TTL Errors - Number of IP TTL errors happened.

Priority Zero Packet Received - Number of priority zero packets received.

Priority Zero Packet Transmitted - Number of priority zero packets transmitted.

Invalid Packet Type Received - Number of invalid packets received.

Address List Errors - Number of address list errors.

Invalid Authentication Type - Number of invalid authentication types received.

Authentication Type Mismatch - Number of authentication type mismatch received.

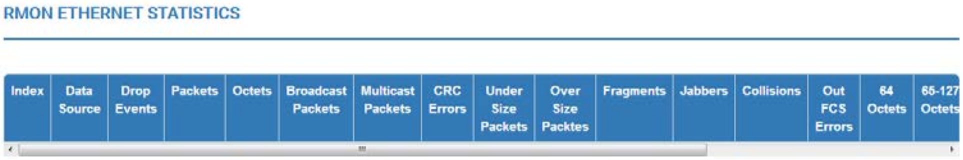
Packet Length Errors - Number of VRRP packets received with invalid length.

8.15 RMON

The RMON link allows the user to view the RMON statistics screens through the following tabs.

- ❖ Ethernet Statistics

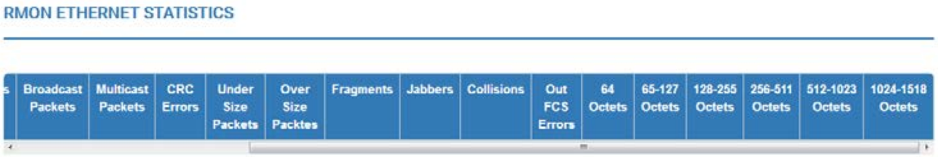
8.15.1 Ethernet Statistics



RMON ETHERNET STATISTICS

Index	Data Source	Drop Events	Packets	Octets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packtes	Fragments	Jabbers	Collisions	Out FCS Errors	64 Octets	65-127 Octets

Fig: RMON Ethernet Statistics – Statistics Group-Part A



RMON ETHERNET STATISTICS

s	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packtes	Fragments	Jabbers	Collisions	Out FCS Errors	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets

Fig: RMON Ethernet Statistics – Statistics Group-Part B

The *Ethernet Statistics* link opens **RMON Ethernet Statistics** Page.

RMON Ethernet Statistics page displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.

The table below lists the fields present for Global Statistics in this page.

Index –The index of the entity

Data Source The SNMP object ID of the variable on which the statistics is being collected. This object identifies the instance of the ifIndex object. For successful configuration the Data Source has to be a valid Object ID.

Drop Events - Number of events in which the packets were dropped due to lack of resources.

Packets - Number of packets received.

Octets - Number of octets received.

Broadcast Packets - Number of packets received.

Multicast Packets - Number of multicast packets received.

CRC Errors - Number of packets received with CRC errors.

Under Size Packets - Number of under size packets received.

Over Size Packets - Number of oversize packets received.

Fragments - Number of fragments received.

Jabbers - Number of jabbers.

Collisions - Number of collisions.

64 Octets - Number of Ethernet packets received with size less than 64 bytes.

65-127 Octets - Number of Ethernet packets received with size between 65 and 127 bytes.

128-255 Octets - Number of Ethernet packets received with size between 128 and 255 bytes.

256-511 Octets - Number of Ethernet packets received with size between 256 and 511 bytes.

512-1023 Octets - Number of Ethernet packets received with size between 512 and 1023 bytes.

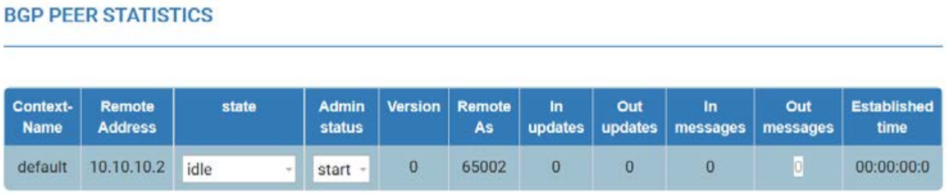
1024-1518 Octets - Number of Ethernet packets received with size between 1024 and 1518 bytes.

8.16 BGP

The BGP link allows the user to view the BGP statistics screens through the following tabs.

- Peer Details
- GR Details

8.16.1 Peer Details



BGP PEER STATISTICS

Context-Name	Remote Address	state	Admin status	Version	Remote As	In updates	Out updates	In messages	Out messages	Established time
default	10.10.10.2	idle	start	0	65002	0	0	0	0	00:00:00:0

Fig: BGP Peer Statistics – Statistics Group

The *Peer Details* link opens **BGP Peer Statistics** Page.

BGP Peer Statistics page displays the BGP neighbor statistics information.

The table below lists the fields present in this page.

Context Name – The context alias name this BGP entry belongs to.

Remote Address – The BGP peer IP address.

State The BGP peer connection state.

Admin status - The desired state of the BGP connection.

Version - The negotiated version of BGP running between the two peers.

Remote As – The remote autonomous system's number.

In updates - The number of BGP UPDATE messages received on this connection.

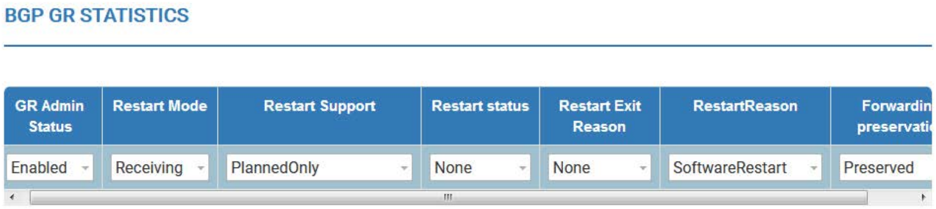
Out updates - The number of BGP UPDATE messages transmitted on this connection.

In messages - The total number of messages received from the remote peer on this connection.

Out messages - The total number of messages transmitted to the remote peer on this connection.

Established time - This timer indicates how long (in seconds) this peer has been in the Established state or how long since this peer was last in the Established state. It is set to zero when a new peer is configured or the router is booted.

8.16.2 GR Details



BGP GR STATISTICS

GR Admin Status	Restart Mode	Restart Support	Restart status	Restart Exit Reason	RestartReason	Forwardin preservati
Enabled	Receiving	PlannedOnly	None	None	SoftwareRestart	Preserved

Fig: BGP GR Statistics – Statistics Group

The *GR Details* link opens **BGP GR Statistics** Page.

BGP GR Statistics page displays the BGP graceful restart configurations.

The table below lists the fields present in this page.

GR Admin Status - The status of GR capability in BGP speaker.

Restart Mode - The status of GR mode in BGP speaker.

Restart Support - The router's support for BGP graceful restart Options.

Restart status - Current status of BGP graceful restart.

Restart Exit Reason - Describes the outcome of the last attempt at a graceful restart.

RestartReason – The reason code of BGP graceful restart.

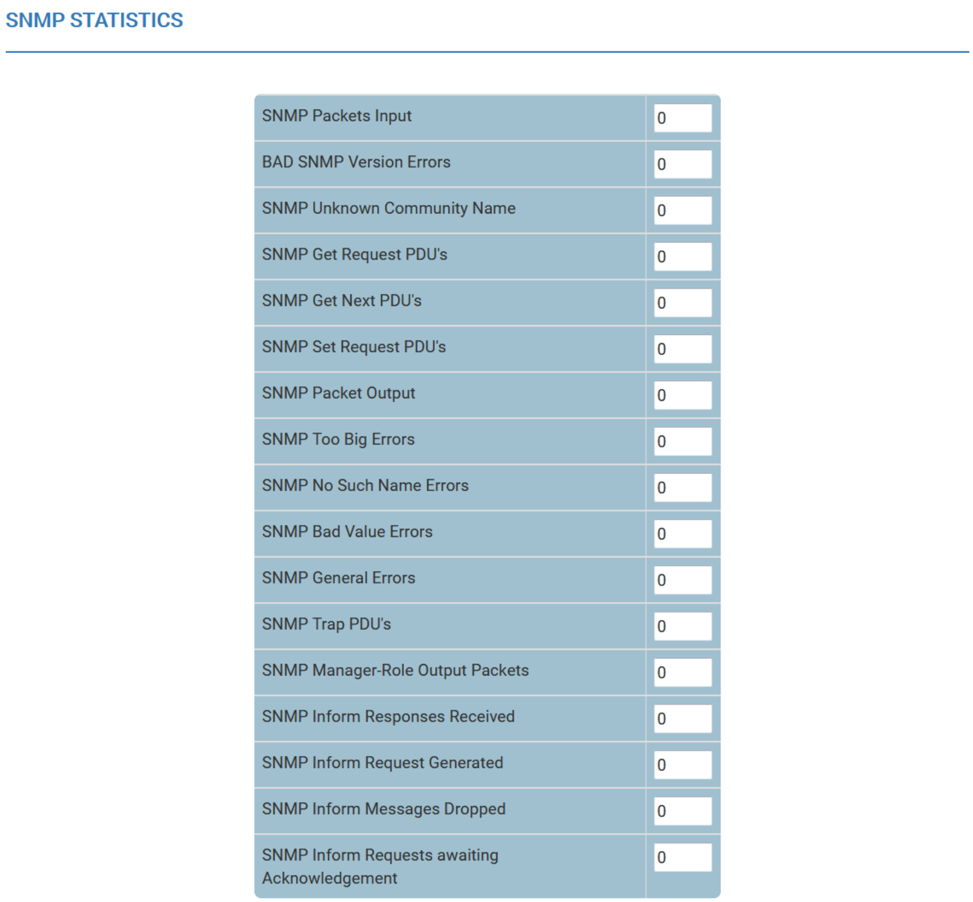
Forwarding preservation - The status of the forwarding preservation during restart

8.17 SNMP

The SNMP link allows the user to view the SNMP statistics screens through the following links.

- AGENT
- AGENTX

8.17.1 AGENT



SNMP STATISTICS

SNMP Packets Input	0
BAD SNMP Version Errors	0
SNMP Unknown Community Name	0
SNMP Get Request PDU's	0
SNMP Get Next PDU's	0
SNMP Set Request PDU's	0
SNMP Packet Output	0
SNMP Too Big Errors	0
SNMP No Such Name Errors	0
SNMP Bad Value Errors	0
SNMP General Errors	0
SNMP Trap PDU's	0
SNMP Manager-Role Output Packets	0
SNMP Inform Responses Received	0
SNMP Inform Request Generated	0
SNMP Inform Messages Dropped	0
SNMP Inform Requests awaiting Acknowledgement	0

Fig: SNMP Statistics – Statistics Group

The *AGNET* link opens **SNMP Statistics** Page.

SNMP Statistics page displays the statistics information related to SNMP Agent. This page can be viewed only if the option Agent is selected in the SNMP Agent Control Settings page.

The table below lists the fields present in this page.

SNMP Packets Input - The total number of messages delivered to the SNMP entity from the transport service.

BAD SNMP Version Errors - The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.

SNMP Unknown Community Name - The total number of community-based SNMP messages delivered to the SNMP entity which used an SNMP community name not known to said entity.

SNMP Get Request PDU's - The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.

SNMP Get Next PDU's - The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.

SNMP Set Request PDU's - The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.

SNMP Packet Output - The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.

SNMP Too Big Errors - The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was 'tooBig'.

SNMP No Such Name Errors - The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status was 'noSuchName'.

SNMP Bad Value Errors - The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was 'badValue'.

SNMP General Errors - The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was 'genErr'.

SNMP Trap PDU's - The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.

SNMP Manager-Role Output Packets - The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDU (such as a Response-PDU) with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.

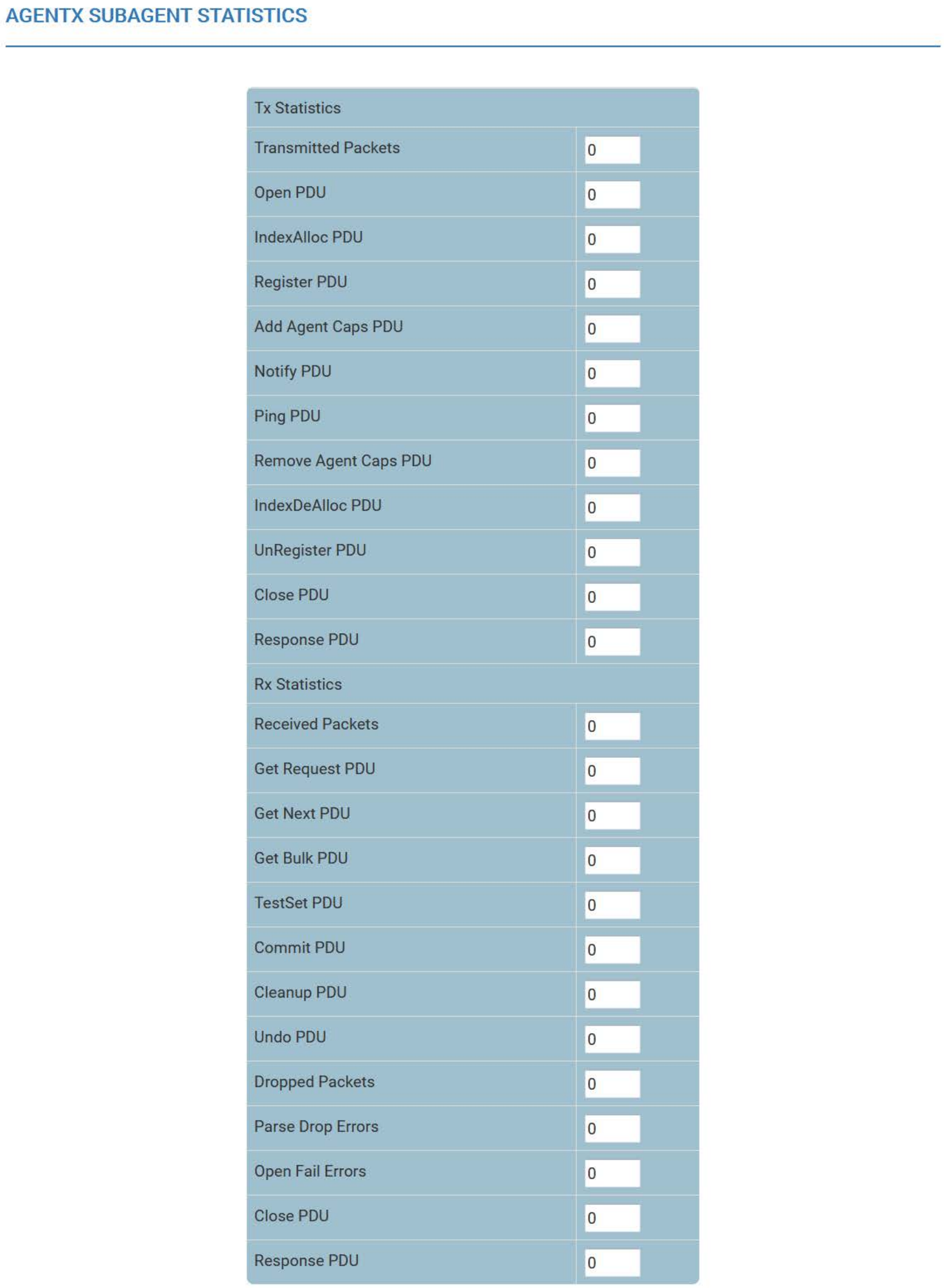
SNMP Inform Responses Received - Total number of SNMP Inform responses received by the Agent from manager.

SNMP Inform Request Generated - Total number of SNMP Inform requests sent by the Agent to manager.

SNMP Inform Messages Dropped - Total number of SNMP Inform messages dropped by the Agent after retransmission.

SNMP Inform Requests awaiting Acknowledgement - Total number of SNMP Inform messages for which Acknowledgement is expected from manager.

8.17.2 AGENTX



AGENTX SUBAGENT STATISTICS

Tx Statistics	
Transmitted Packets	0
Open PDU	0
IndexAlloc PDU	0
Register PDU	0
Add Agent Caps PDU	0
Notify PDU	0
Ping PDU	0
Remove Agent Caps PDU	0
IndexDeAlloc PDU	0
UnRegister PDU	0
Close PDU	0
Response PDU	0
Rx Statistics	
Received Packets	0
Get Request PDU	0
Get Next PDU	0
Get Bulk PDU	0
TestSet PDU	0
Commit PDU	0
Cleanup PDU	0
Undo PDU	0
Dropped Packets	0
Parse Drop Errors	0
Open Fail Errors	0
Close PDU	0
Response PDU	0

Fig: Agentx Subagent Statistics – Statistics Group

The *AGNETX* link opens **Agentx Subagent Statistics** Page.

Agentx Subagent Statistics page displays the statistics information related to SNMP Agentx. This page can be viewedonly if the option AgentXSubagent is selected in the SNMP Agent Control Settings page.

The table below lists the fields present for Transmit Statistics in this page.

Transmitted Packets - Number of packets transmitted.

Open PDU - Number of open PDUs transmitted.

IndexAlloc PDU - Number of IndexAlloc PDUs transmitted.

Register PDU - Number of register PDUs transmitted.

Add Agent Caps PDU - Number of add agent caps PDUs transmitted.

Notify PDU - Number of notify PDUs transmitted.

Ping PDU - Number of ping PDUs transmitted.

Remove Agent Caps PDU - Number of remove agent caps PDUs transmitted.

IndexDeAlloc PDU - Number of IndexDeAlloc PDUs transmitted.

UnRegister PDU - Number of unregister PDUs transmitted.

Close PDU - Number of close PDUs transmitted.

Response PDU - Number of response PDUs transmitted.

The table below lists the fields present for Receive Statistics in this page.

Received Packets - Number of packets received.

Get Request PDU - Number of get request PDUs received.

Get Next PDU - Number of get next PDUs received.

Get Bulk PDU - Number of get bulk PDUs received.

TestSet PDU - Number of test set PDUs received.

Commit PDU - Number of commit PDUs received.

Cleanup PDU - Number of cleanup PDUs received.

Undo PDU - Number of undo PDUs received.

Dropped Packets - Number of dropped packets.

Parse Drop Errors - Number of received PDUs dropped due to parse errors.

Open Fail Errors - Number of open fail PDUs received.

Close PDU - Number of close PDUs received.

Response PDU - Number of response PDUs received.