



**RGS-PR9000-A**  
**Layer 3 Industrial Rack-Mount Ethernet**  
**Switch**

**User Manual**

**Version 1.0**

**June, 2016**

[www.oring-networking.com](http://www.oring-networking.com)


## **COPYRIGHT NOTICE**

Copyright © 2016 ORing Industrial Networking Corp.

All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

## **TRADEMARKS**

 is a registered trademark of ORing Industrial Networking Corp.

All other trademarks belong to their respective owners.

## **REGULATORY COMPLIANCE STATEMENT**

Product(s) associated with this publication complies/comply with all applicable regulations.

Please refer to the Technical Specifications section for more details.

## **WARRANTY**

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

## **DISCLAIMER**

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

## **CONTACT INFORMATION**

### **ORing Industrial Networking Corp.**

3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.

Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014

Website: [www.oring-networking.com](http://www.oring-networking.com)

### **Technical Support**

E-mail: [support@oring-networking.com](mailto:support@oring-networking.com)

### **Sales Contact**

E-mail: [sales@oring-networking.com](mailto:sales@oring-networking.com) (Headquarters)

[sales@oring-networking.com.cn](mailto:sales@oring-networking.com.cn) (China)

# Table of Content

<b>Getting Started .....</b>	<b>11</b>
1.1 About RGS-PR9000-A .....	11
1.2 Software Features .....	11
1.3 Hardware Specifications.....	12
<b>Hardware Overview.....</b>	<b>13</b>
2.1 Front Panel.....	13
2.1.1 Ports and Connectors .....	13
2.1.2 LED .....	14
2.2 Rear Panel .....	14
<b>Hardware Installation.....</b>	<b>16</b>
3.1 Rack-mount Installation.....	16
3.2 Module Installation .....	17
3.2.1 RJ-45 Module .....	17
3.2.2 SFP Module.....	17
3.2.3 Power Module .....	18
3.3 Wiring .....	18
3.3.1 Grounding.....	19
3.3.2 Fault Relay .....	19
3.3.3 Redundant Power Inputs.....	19
3.4 Connection .....	20
3.4.1 Cables .....	20
1000/100BASE-TX/10BASE-T Pin Assignments.....	20
RS-232 port wiring .....	22
3.4.2 SFP.....	22
3.4.3 O-Ring/O-Chain.....	23
O-Ring	23
<b>Management.....</b>	<b>26</b>
4.1 System .....	27
4.1.1 System Information .....	27
4.1.2 NVRAM Settings .....	31
4.1.3 ACL .....	35
4.1.3.1 MAC ACL.....	36
4.1.3.2 IP Standard ACL.....	39

4.1.3.3	IP Extended ACL .....	42
4.1.3.4	User Defined Filter Configuration .....	47
4.1.3.5	Redirect Interface Group .....	51
4.1.3.6	Provision Mode .....	53
4.1.3.7	Egress Filter Mode .....	53
4.1.4	IP Authorized Manager .....	53
4.1.5	Save and Restore .....	55
4.1.5.1	Save .....	56
4.1.5.2	Erase .....	57
4.1.5.3	Remote Restore .....	58
4.1.6	Firmware Upgrade .....	58
4.1.7	Reboot.....	59
4.1.8	TACACS.....	60
4.1.8.1	Settings .....	60
4.1.8.2	Server Settings.....	61
4.1.9	SNTP.....	62
4.1.9.1	SNTP Scalars .....	62
4.1.9.2	SNTP Unicast.....	65
4.1.10	SSH.....	66
4.1.11	SSL .....	67
4.1.11.1	SSL Global Settings .....	68
4.1.11.2	SSL Digital Certificate .....	69
4.1.12	HTTP.....	70
4.1.12.1	Web Session .....	70
4.1.13	SNMP.....	70
4.1.13.1	Agent .....	70
	Community.....	70
4.1.13.2	Proxy .....	81
4.1.13.3	SCALARS.....	83
4.1.13.4	Agentx .....	85
4.1.14	Syslog .....	86
4.1.14.1	Scalars Conf.....	86
4.1.14.2	Logging.....	88
4.1.14.3	Mail Table .....	90
4.1.14.4	Fwd Table .....	90
4.1.14.5	SysLog .....	91
4.1.15	DDM.....	92

4.1.15.1	SFP Monitor .....	93
4.1.16	Backup Unit.....	93
4.1.16.1	Backup Unit Config.....	93
4.1.17	ModBus .....	94
4.1.17.1	ModBus Config.....	94
4.2	Layer 2 Management .....	94
4.2.1	Port Manager .....	94
4.2.1.1	Basic Settings.....	94
4.2.1.2	Port Monitoring .....	99
4.2.1.3	Traffic Class.....	100
4.2.1.4	Port Control .....	102
4.2.1.5	Rate Limiting .....	106
4.2.2	VLAN .....	106
4.2.2.1	Basic Setting .....	106
4.2.2.2	Port Setting.....	110
4.2.2.3	Static VLANs .....	114
4.2.2.4	Protocol Group .....	116
4.2.2.5	Port Protocol.....	118
4.2.2.6	Port MAC Map.....	120
4.2.2.6	Unicast MAC .....	121
4.2.2.7	Wildcard .....	122
4.2.2.8	Switch Port Filtering .....	123
4.2.2.9	FDB Flush .....	124
4.2.3	VLAN Subnet.....	125
4.2.4	GARP.....	126
4.2.5	Dynamic VLAN .....	127
4.2.5.1	Dynamic VLAN .....	127
4.2.5.2	Port Settings.....	128
4.2.5.3	Garp Timers.....	129
4.2.6	MSTP.....	131
4.2.6.1	Basic Settings.....	131
4.2.6.2	Timers.....	134
4.2.6.3	Port Configuration .....	135
4.2.6.4	VLAN Mapping .....	139
4.2.6.5	Port Settings.....	140
4.2.6.6	CIST Port Status.....	142
4.2.6.7	Bridge Priority.....	144

4.2.7	RSTP .....	145
4.2.7.1	Global Settings .....	146
4.2.7.2	Basic Settings.....	147
4.2.7.3	Port Settings.....	149
4.2.7.4	Port Status .....	153
4.2.8	Link Aggregation .....	155
4.2.8.1	Basic Settings.....	155
4.2.8.2	Interface Settings .....	156
4.2.8.3	Port Channel Settings .....	158
4.2.8.4	Protocol Group .....	162
4.2.8.5	Port Settings.....	164
4.2.8.6	Load Balancing.....	165
4.2.8.7	DLAG Remote Port Channel Settings.....	167
4.2.8.8	DLAG Remote Port Settings .....	168
4.2.9	LLDP .....	169
4.2.9.1	Global Settings .....	169
4.2.9.2	Port Settings.....	170
4.2.9.3	Interfaces.....	173
4.2.9.4	Neighbors .....	174
4.2.10	802.1x.....	175
4.2.10.1	Basic Settings .....	175
4.2.10.2	Port Settings .....	178
4.2.10.3	Timers .....	184
4.2.10.4	Local AS.....	185
4.2.10.5	Radius Settings .....	187
4.2.10.6	MAC Session Info .....	188
4.2.11	Mirroring .....	190
4.2.12	Redundancy .....	192
4.2.12.1	O-Ring .....	192
4.2.12.2	O-Chain .....	194
4.3	Layer 3 Management .....	195
4.3.1	IP .....	196
4.3.1.1	VLAN Interface .....	196
4.3.1.2	IPV4 AddrConf.....	198
4.3.1.3	IP Route.....	199
4.3.1.4	LoopBack Settings .....	199
4.3.1.5	IVR-VLAN Mapping.....	200

4.3.2	IP (contd...)	201
4.3.2.1	IP	201
4.3.2.2	IP PMTU	203
4.3.2.3	Static ARP	204
4.3.2.4	IP Ping	206
4.3.2.5	IPV4 TRACEROUTE	207
4.3.3	Layer 3 Tunnel	208
4.3.4	DHCP Server	210
4.3.4.1	Basic Settings	210
4.3.4.2	Pool Settings	212
4.3.4.3	Pool Options	213
4.3.4.4	Exclude List	214
4.3.4.5	Host Settings	215
4.3.4.6	Host Options	215
4.3.4.7	Bootfile Configuration	216
4.3.5	DHCP Relay	217
4.3.5.1	Basic Settings	217
4.3.5.2	Interface Settings	218
4.3.6	DHCP Client	219
4.3.6.1	DHCP Option Type	219
4.3.6.2	DHCP ClientId	220
4.3.7	RIP	221
4.3.7.1	RIP VRF Creation	221
4.3.7.2	Basic Setting	222
4.3.7.3	Interface Configuration	224
4.3.7.4	Neighbors List	226
4.3.7.5	Security Settings	227
4.3.7.6	Address Summary	229
4.3.8	OSPF	230
4.3.8.1	OSPF VRF Creation	230
4.3.8.2	Basic Settings	231
4.3.8.3	Area	234
4.3.8.4	Interface	236
4.3.8.5	Virtual Interface	239
4.3.8.6	Neighbor	241
4.3.8.7	RRD Route	242
4.3.8.8	Aggregation	243

4.3.8.9	AsExAggregation.....	244
4.3.8.10	GraceRestart .....	246
4.3.9	PRD .....	248
4.3.10	VRRP .....	250
4.3.10.1	VRRP Global Settings .....	250
4.3.10.2	Track Settings.....	251
4.3.10.3	VRRP Virtual Router Settings.....	252
4.3.10.4	Associated IP.....	254
4.4	Multicast.....	254
4.4.1	IGMP Snooping .....	254
4.4.1.1	Basic Settings.....	254
4.4.1.2	Timer .....	259
4.4.1.3	VlanConfiguration.....	260
4.4.1.4	InterfaceConfiguration .....	264
4.4.1.5	RouterPortConf .....	266
4.4.1.6	RouterPorts .....	267
4.4.1.7	Static Entry .....	268
4.4.1.8	FwdInformation.....	268
4.4.1.9	McastReceiverInfo.....	269
4.4.2	MLD Snooping .....	269
4.4.2.1	Basic Settings.....	270
4.4.2.2	Timer .....	274
4.4.2.3	VlanConfiguration.....	274
4.4.2.4	RouterPortConf .....	277
4.4.2.5	RouterPorts .....	278
4.4.2.6	FwdInformation.....	279
4.4.3	GMRP .....	279
4.4.3.1	GMRP.....	279
4.4.3.2	Port Settings.....	280
4.4.4	IGMP.....	281
4.4.4.1	Basic Settings.....	281
4.4.4.2	Interface Configuration .....	282
4.4.4.3	Croup Information.....	283
4.4.4.4	Source Information .....	284
4.4.4.5	GroupList Configuration .....	285
4.4.5	MLD.....	285
4.4.5.1	Basic Settings.....	286



4.4.5.2	Interface Configuration .....	286
4.4.5.3	MLD Source Information .....	288
4.4.6	IGMP Proxy.....	288
4.4.6.1	Basic Settings.....	289
4.4.6.2	Upstream Interface.....	289
4.4.6.3	MRoute Information.....	290
4.4.6.4	NextHop Information .....	290
4.4.7	PIM.....	291
4.4.7.1	Basic Settings.....	291
4.4.7.2	Component.....	293
4.4.7.3	Interface .....	294
4.4.7.4	CandidateRP .....	295
4.4.7.5	StaticRP .....	297
4.4.7.6	Global .....	298
4.4.7.7	DM.....	299
4.4.7.8	RouteInfo.....	300
4.4.7.9	RPInfo.....	301
4.4.7.10	PimHA .....	302
4.4.7.11	ElectedRP .....	303
4.4.7.12	DFInfo.....	304
4.5	Ethernet OAM .....	305
4.5.1	Basic Settings .....	305
4.5.2	Port Settings .....	306
4.5.3	LinkEvent Settings .....	309
4.5.4	Loopback Settings .....	314
4.6	RMON .....	315
4.6.1	Basic Settings .....	315
4.6.2	Alarms .....	316
4.6.3	Ethernet Statistics .....	318
4.6.4	Events .....	319
4.6.5	History .....	321
4.7	Statistics .....	322
4.7.1	Interface .....	322
4.7.1.1	Interface Clear .....	322
4.7.1.2	Interface .....	323
4.7.1.3	Ethernet.....	323
4.7.2	MSTP .....	323

4.7.2.1	Information .....	323
4.7.2.2	CIST Port Statistics .....	324
4.7.2.3	MSTI Port Statistics .....	324
4.7.3	RSTP .....	324
4.7.3.1	Information .....	324
4.7.3.2	Port Statistics .....	324
4.7.4	LA .....	325
4.7.4.1	PortLACP Stats .....	325
4.7.4.2	Neighbour Stats .....	325
4.7.5	LLDP .....	325
4.7.5.1	Traffic .....	325
4.7.5.2	Statistics .....	326
4.7.5.3	Errors .....	326
4.7.6	802.1x .....	326
4.7.6.1	Session Stats .....	326
4.7.6.2	Supp-Session Stats .....	327
4.7.6.3	Mac-Session Stats .....	327
4.7.7	Radius .....	327
4.7.8	IGMP Snooping .....	327
4.7.8.1	IGS Clear Statistics .....	327
4.7.8.2	IGS Statistics .....	327
4.7.8.3	IGS V3 Statistics .....	328
4.7.9	MLD Snooping .....	328
4.7.9.1	MLDS Statistics .....	328
4.7.9.2	MLDS V2 Statistics .....	328
4.7.10	IP .....	328
4.7.10.1	ARP Cache .....	328
4.7.10.2	ICMP Statistics .....	329
4.7.10.3	IPV4 IfSp Stats .....	329
4.7.10.4	IPV4 SysSp Stats .....	330
4.7.11	RIP .....	330
4.7.12	OSPF .....	330
4.7.12.1	Route Information .....	330
4.7.12.2	Link State Database .....	330
4.7.12.3	Redundancy Information .....	330
4.7.13	VRRP .....	331
4.7.14	IGMP .....	331

4.7.15 MLD.....	331
4.7.16 IGMP Proxy.....	332
4.7.17 RMON .....	332
<b>Command Line Interface Management .....</b>	<b>333</b>

# **Getting Started**

## **1.1 About RGS-PR9000-A**

RGS-PR9000-A is a rack-mount modular Ethernet switch with 3 slots, which support up to 24 10/100/1000BaseT(X) and 4 10Gigabit Ethernet ports. Featuring Layer 3 for faster forwarding via hardware, the switch is designed for power substation application and rolling stock application, fully compliant with the requirement of IEC 61850-3 and IEEE 1613. With completely support for Ethernet redundancy protocols such as I-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible), the switch can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Featuring a wide operating temperature from -40°C to 85°C, the switch can be managed centrally and conveniently via Open-Vision, web browsers, Telnet and console (CLI) configuration, making it one of the most reliable choice for highly-managed and Fiber Ethernet power substation and rolling stock application.

## **1.2 Software Features**

- Supports GRE (Generic Routing Encapsulation) tunneling protocol
- Supports O-Ring (recovery time < 30ms over 250 units of connection) and MSTP(RSTP/STP compatible) for Ethernet redundancy
- Supports Open-Ring to interoperate with other vendors' ring technology in open architecture
- Supports O-Chain to allow multiple redundant network rings
- Supports standard IEC 62439-2 MRP (Media Redundancy Protocol) function
- Supports IEEE 1588v2 clock synchronization
- Supports IPV6 new internet protocol version
- Supports Modbus TCP protocol
- Supports priority-tagged frames to be received by specific IEDs
- Supports IEEE 802.3az Energy-Efficient Ethernet technology
- Provides HTTPS/SSH protocols to enhance network security
- Supports SMTP client
- Supports IP-based bandwidth management
- Supports application-based QoS management
- Supports Device Binding security function
- Supports DOS/DDOS auto prevention
- Supports IGMP v2/v3 (IGMP snooping support) to filter multicast traffic

- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN network management
- Supports ACL, TACACS+ and 802.1x user authentication for security
- Supports 10K Bytes Jumbo Frame
- Supports multiple notifications for incidents
- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)
- Support LLDP Protocol

## **1.3 Hardware Specifications**

- Modular design
- Redundant DC power inputs
- 19-inch rack mountable design
- Compliant with IEC 61850-3 and IEEE 1613
- Houses 3 x module slots for a maximum of 24 10/100/1000Base-T(X) RJ-45 ports or 100/1000Base-X SFP ports or 12 10/100/1000Base-T(X) RJ-45 ports and 100/1000Base-X SFP ports
- 4 x 10G Ethernet ports
- Operating temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions : 440(W) x 325(D) x 44(H) mm (17.32x12.8x1.73 inches)

# Hardware Overview

## 2.1 Front Panel

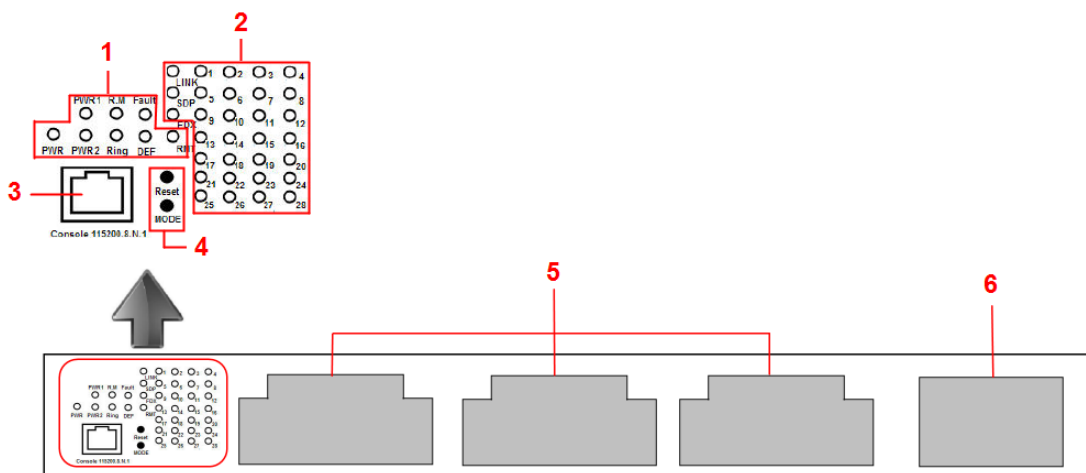
### 2.1.1 Ports and Connectors

The switch provides four 10 Gigabit ports and three 10/100/1000Base-T module slots to enable different modular combinations based on your needs. For applications requiring long-distance data transmission, you can also use SFP modules to meet your needs. Please refer to the following table for available modules.



The modules are not hot-swappable. Be sure to turn off power before changing modules, otherwise the system will not detect newly inserted modules.

Modules	Description	
<b>SWM-80GT-A</b>	Industrial 8-port Gigabit Ethernet switch module with 8x10/100/1000Base-T(X) ports	Gigabit Ethernet module
<b>SWM-44GTP-A</b>	Industrial 8-port Gigabit Ethernet switch module with 4x10/100/1000Base-T(X) and 4x100/1000Base-X, SFP socket	Gigabit combo module
<b>SWM-08GP-A</b>	Industrial 8-port Gigabit fiber module with 8x100/1000Base-X, SFP socket	SFP module



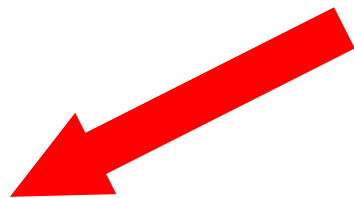
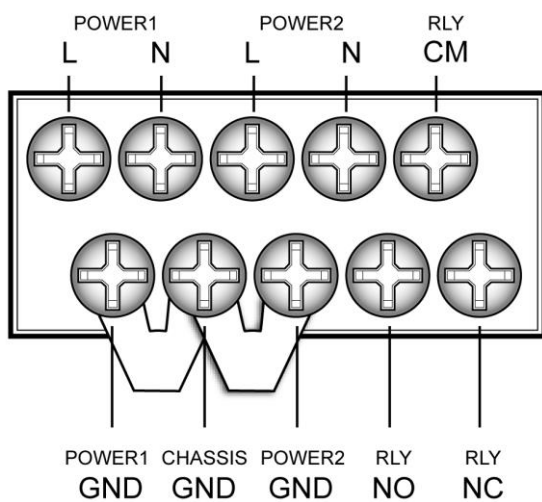
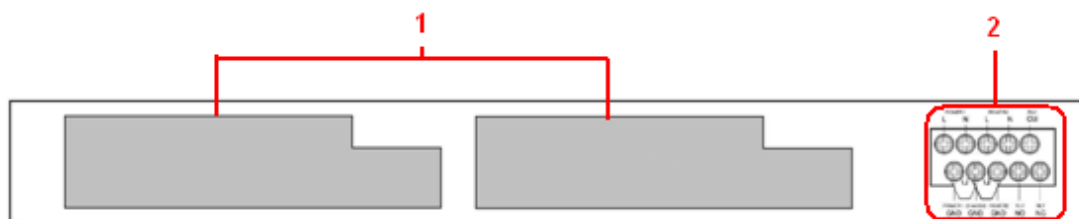
1. System indication LEDs: PWR/PWR1/PWR2/R.M/Ring/Fault/DEF
2. Port status LEDs: LINK/SPD/FDX/port number
3. Console port
4. Buttons: Rest/LED Mode (Press **Reset** for 3 seconds to reset and 5 seconds to return to factory default. To change port LED mode, press the **Mode** button)
5. RJ-45/SFP module slots
6. 10G Ethernet ports

### 2.1.2 LED

LED	Color	Status	Description
<b>PWR</b>	Green	On	DC power on
		Blinking	Upgrading firmware
<b>PW1</b>	Green	On	DC power module 1 activated
<b>PW2</b>	Green	On	DC power module 2 activated
<b>R.M</b>	Green	On	Ring Master
<b>Ring</b>	Green	On	Ring enabled
		Slowly blinking	Ring structure is broken (i.e. part of the ring is disconnected)
		Fast blinking	Ring disabled
<b>Fault</b>	Amber	On	Errors (power failure or port malfunctioning)
<b>DEF</b>	Green	On	System reset to default
<b>RMT</b>	Green	On	Accessed remotely
<b>LNK</b>	Green	On	Port link up
<b>SPD</b>	Green	Blinking	Data transmitted
<b>FDX</b>	Amber	On	Port works under full duplex.

## 2.2 Rear Panel

On the rear panel of the switch sit two panel module slots and one terminal block. The terminal blocks include two power pairs for redundant power supply.



**Note :**  
 RLY COM– Relay Com  
 RLY NO – Relay Normal Open  
 RLY NC – Relay Normal Close

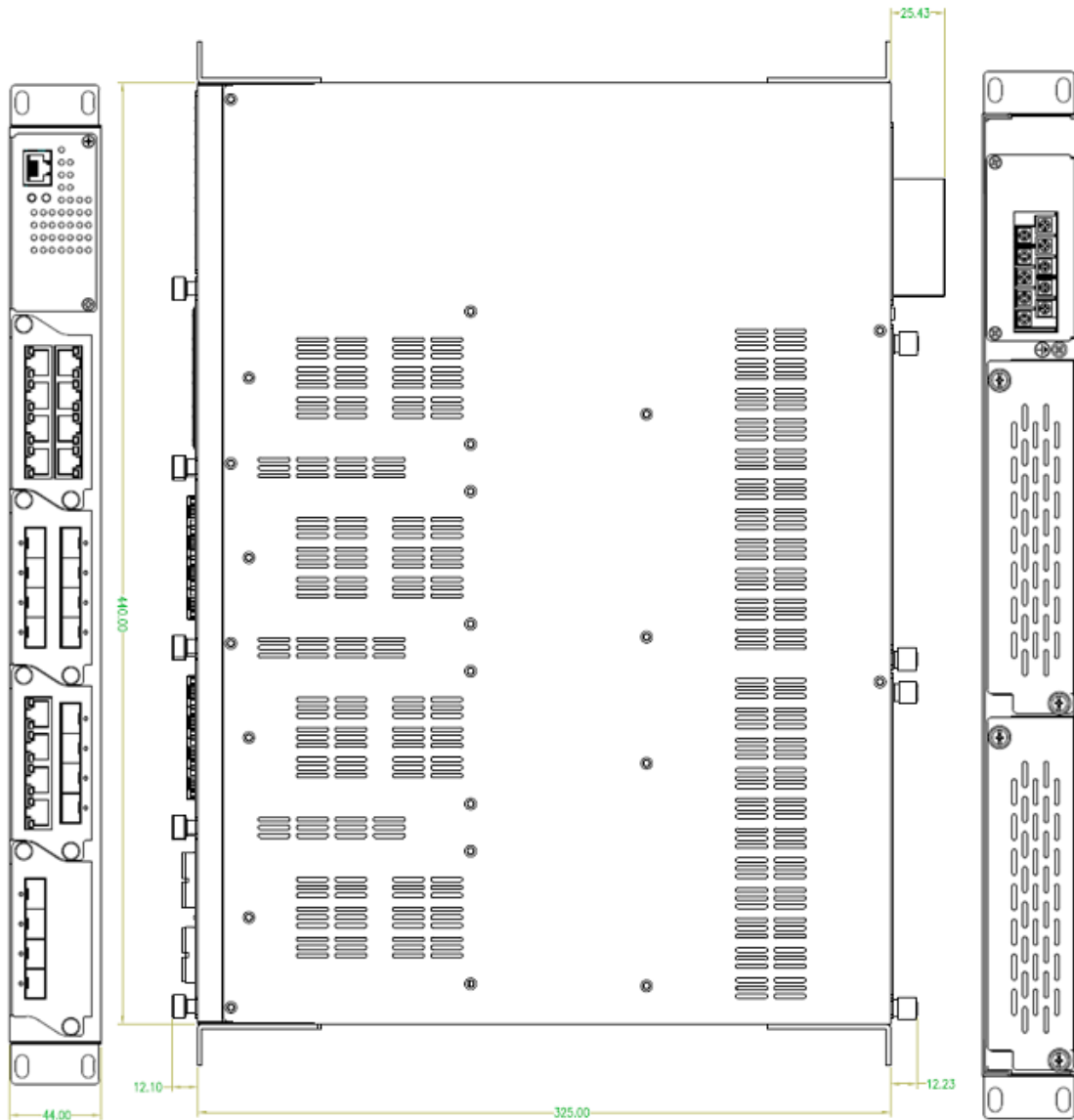
1. Power panel modules
2. Terminal block



# Hardware Installation

## 3.1 Rack-mount Installation

The switch comes with two rack-mount kits to allow you to fasten the switch to a rack in any environments.



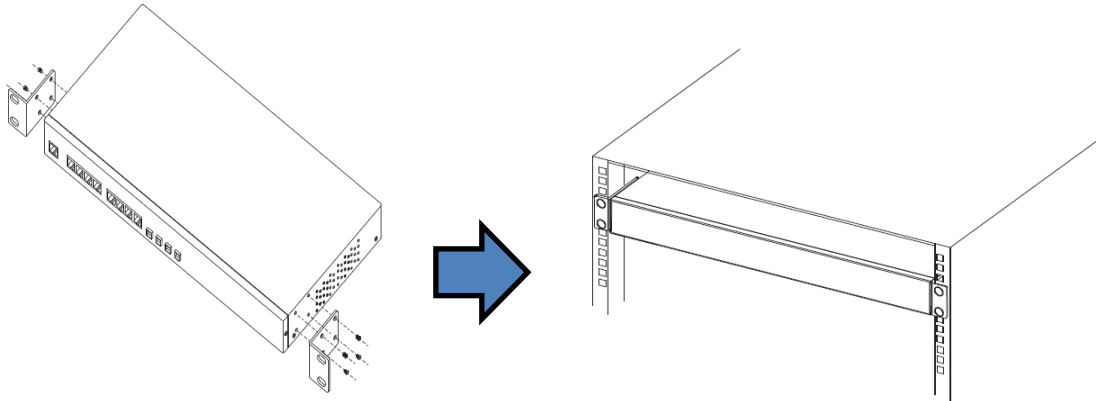
Follow the following steps to install the switch to a rack.

Step 1: Install left and right front mounting brackets to the switch using 4 M3 screws on each side provided with switch.

Step 2: With front brackets orientated in front of the rack, nest front and rear brackets together.

Fasten together using remaining M4 screws into counter sunk holes.

Step 3: Fasten the front mounting bracket to the front of the rack.



## 3.2 Module Installation

### 3.2.1 RJ-45 Module

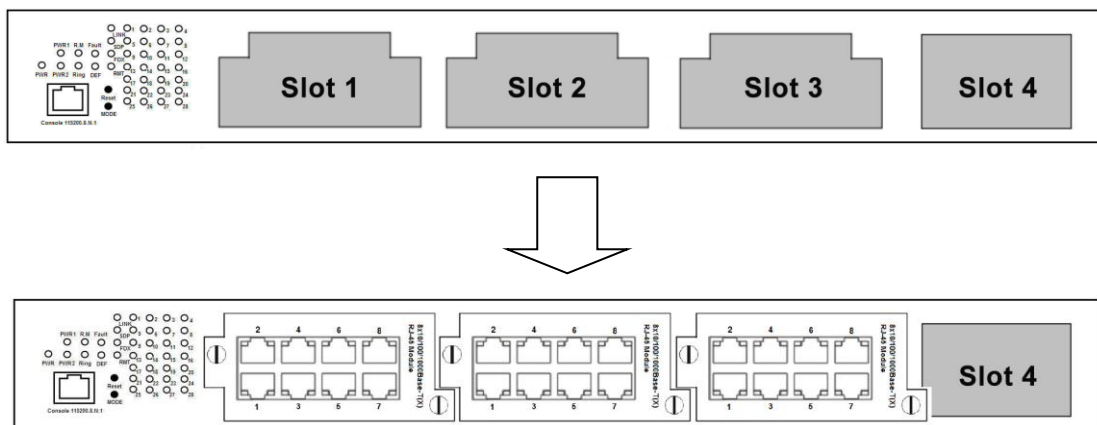
The switch supports maximum three RJ-45 modules, giving you a total of 24 RJ-45 ports.

Follow the steps bellows for installation.

Step 1: Switch off the power of the switch.

Step 2: Insert the modules in Slot 1, 2, and 3 respectively.

Step 3: Switch on the power of the switch



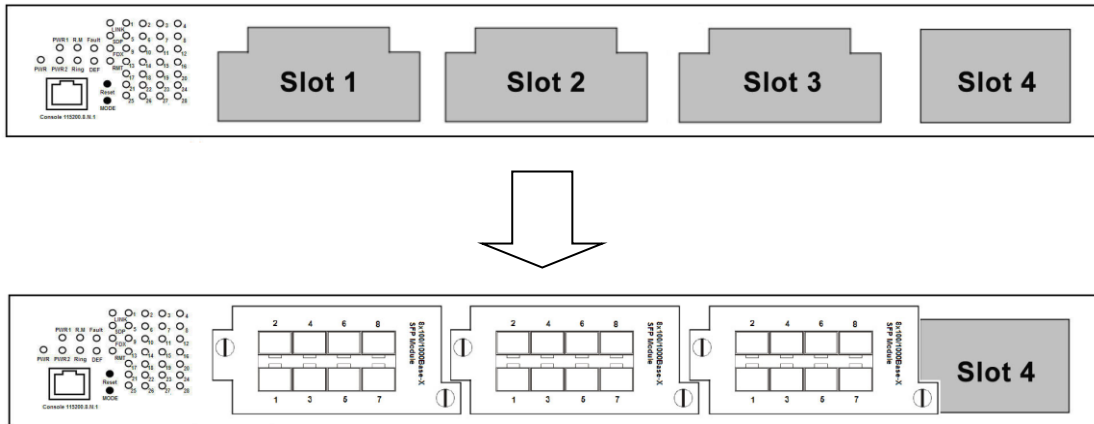
### 3.2.2 SFP Module

The switch supports maximum three SFP modules, giving you a total of 24 SFP ports. Follow the steps bellows for installation.

Step 1: Switch off the power of the switch.

Step 2: Insert the modules in Slot 1, 2, and 3 respectively.

Step 3: Switch on the power of the switch



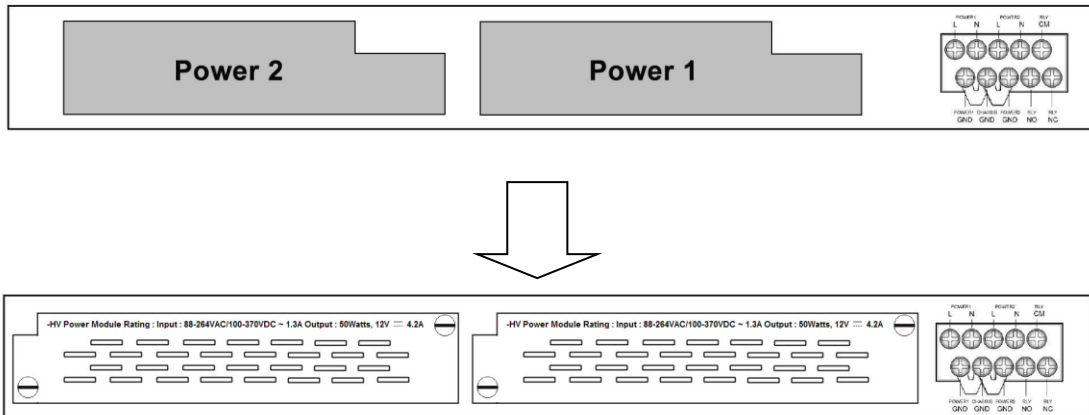
### 3.2.3 Power Module

Each RGS-PR9000-A series switch supports maximum two power modules. Follow the steps bellows for installation.

Step 1: Switch off the power of the switch.

Step 2: Insert the modules in Power 1 and 2 slots respectively.

Step 3: Switch on the power of the switch



## 3.3 Wiring



### WARNING

Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.

**ATTENTION**

1. Be sure to disconnect the power cord before installing and/or wiring your switches.
  2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
  3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
  4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
  5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
  6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together
  7. You should separate input wiring from output wiring
  8. It is advised to label the wiring to all devices in the system
- 

**3.3.1 Grounding**

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screws to the grounding surface prior to connecting devices.

**3.3.2 Fault Relay**

The relay contact of the 2-pin terminal block connector is used to detect user-configured events. The two wires attached to the fault contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains closed.

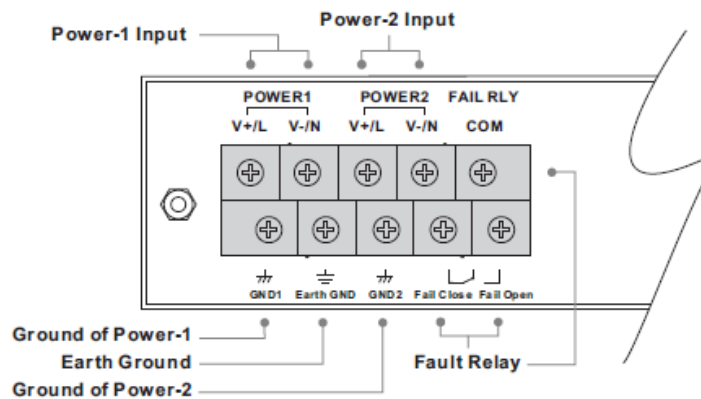
**3.3.3 Redundant Power Inputs**

The RGS-PR9000-A series support dual redundant power supplies, Power Supply 1 (PWR1) and Power Supply 2 (PWR2). The connections for PWR1, PWR2 and the RELAY are located on the terminal block.

Step 1: Insert the negative/positive DC wires into the V-/V+ terminals, respectively.

Step 2: To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

Step 3: Insert the plastic terminal block connector prongs into the terminal block receptor.



## 3.4 Connection

### 3.4.1 Cables

#### 1000/100BASE-TX/10BASE-T Pin Assignments

RGS-PR9000-A comes with standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5, 5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications:

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

With 1000/100BASE-TX/10BASE-T cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T RJ-45 Pin Assignments:

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used

8	Not used
---	----------

1000 Base-T RJ-45 Pin Assignments:

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The RGS-PR9000-A series switches support auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-T MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000 Base-T MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-

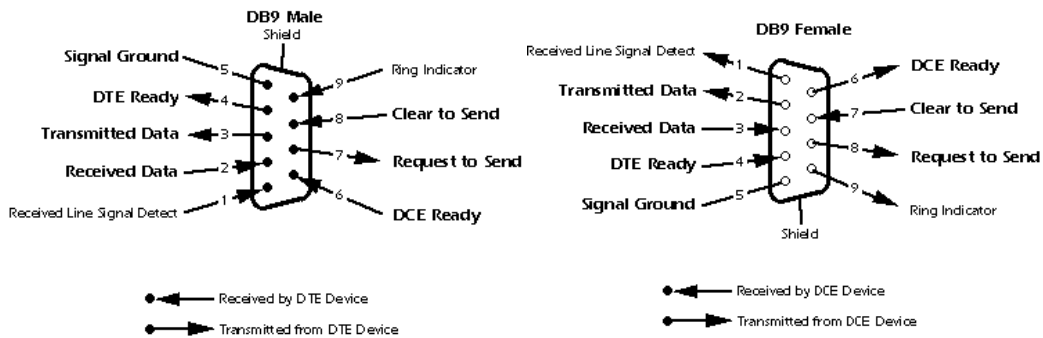
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

**Note:** “+” and “-” signs represent the polarity of the wires that make up each wire pair.

**RS-232 port wiring**

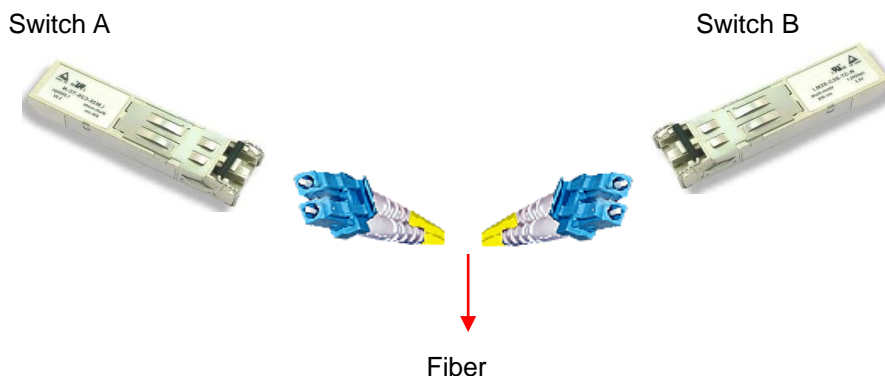
RGS-PR9000-A can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (RJ-45 connector) should be connected to the console port of the switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



**3.4.2 SFP**

The switch comes with fiber optical ports that can connect to other devices using SFP modules. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 μm, 62.5/125 μm fiber) and single-mode with LC connectors. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

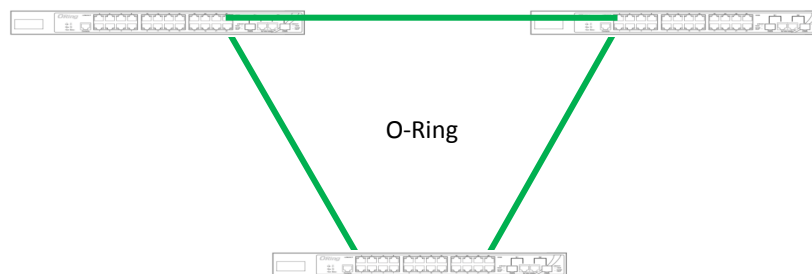


### 3.4.3 O-Ring/O-Chain

#### O-Ring

You can connect three or more switches to form a ring topology to gain network redundancy capabilities through the following steps.

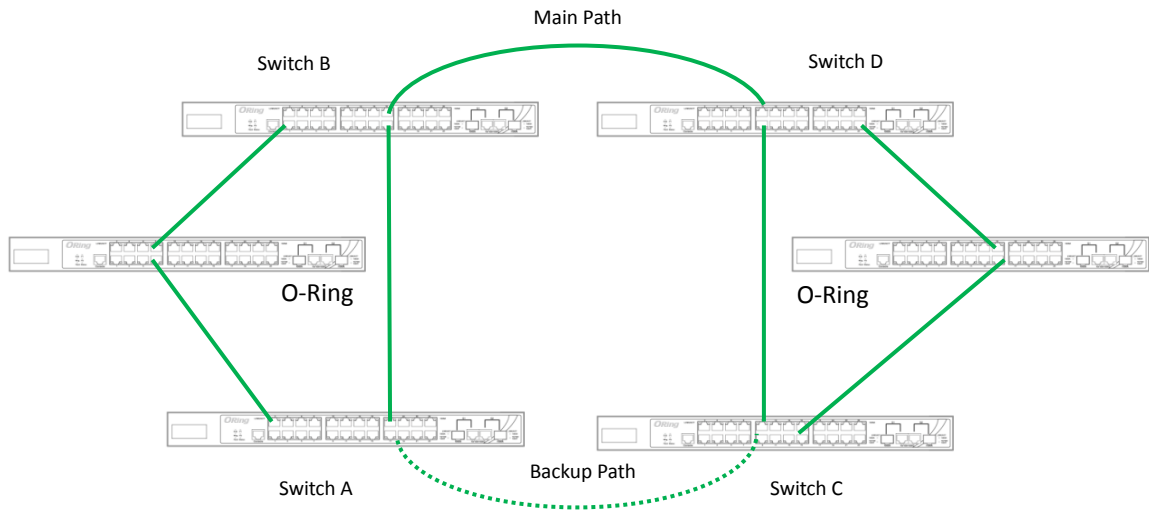
1. Connect each switch to form a daisy chain using an Ethernet cable.
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, please refer to [錯誤! 找不到參照來源。 Configurations](#).
3. Connect the last switch to the first switch to form a ring topology.



#### Coupling Ring

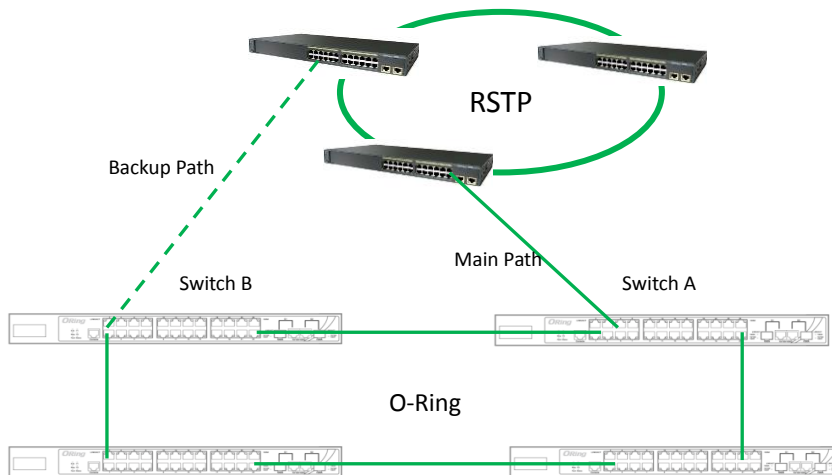
If you already have two O-Ring topologies and would like to connect the rings, you can form them into a coupling ring. All you need to do is select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from ring 2. Decide which port on each switch to be used as the coupling port and then link them together, for example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring option by checking the checkbox on the management page and select the coupling ring in correspondance to the connected port. For more information on port setting, please refer to [錯誤! 找不到參照來源。 Configurations](#). Once the setting is completed, one of the connections will act as the main path while the other will act as the backup path.





**Dual Homing**

If you want to connect your ring topology to a RSTP network environment, you can use dual homing. Choose two switches (Switch A & B) from the ring for connecting to the switches in the RSTP network (Ciscos switches). The connection of one of the switches (Switch A or B) will act as the primary path, while the other will act as the backup path that is activated when the primary path connection fails.

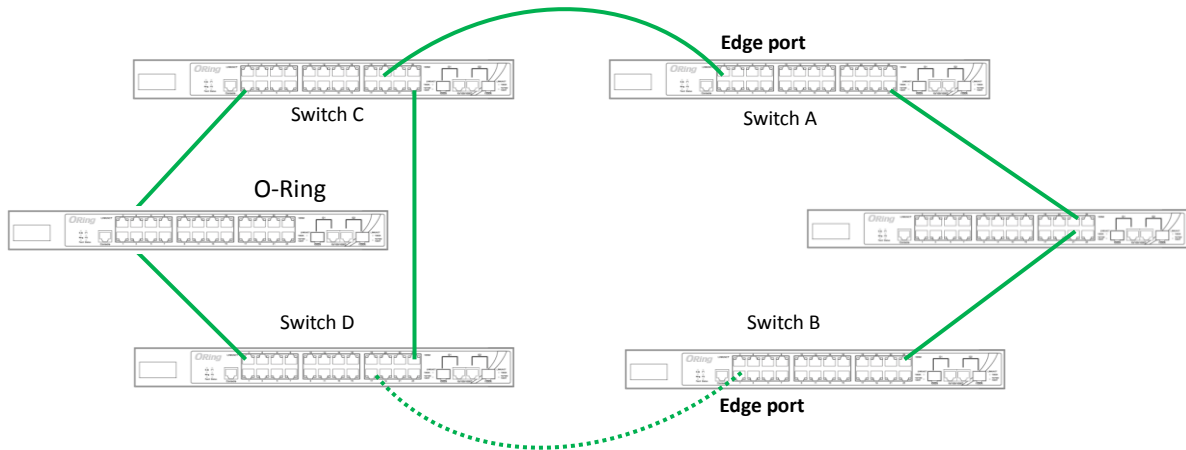


**O-Chain**

When connecting multiple O-Rings to meet your expansion demand, you can create an O-Chain topology through the following steps.

1. Select two switches from the chain (Switch A & B) that you want to connect to the O-Ring and connect them to the switches in the ring (Switch C & D).

2. In correspondence to the port connected to the ring, configure an edge port for both of the connected switches in the chain by checking the box in the management page (see 錯誤! 找不到參照來源。 Configurations).
3. Once the setting is completed, one of the connections will act as the main path, and the other as the back up path.



# Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Firefox. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.



By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

## Preparing for Web Management

You can access the management page of the switch via the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

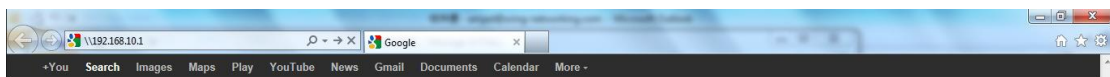
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

## System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press **Enter**.



3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Click **Enter** or **OK** button, the management Web page appears.



After logging in, you can see a list of functions in the left pane. You can click on each link to access the configuration pages of different functions.

## 4.1 System

This section allows you to configure the basic functions of the switch.

### 4.1.1 System Information

This page shows the general information of the switch.

Hardware Version	5.9.1
Firmware Version	6.7.2
Hardware Part Number	1-0-0
Software Serial Number	1-0-0
System Name	RGS-PR9000-A
Software Version	S81
Switch Name	<input type="text" value="RGS-PR9000-A"/>
System Contact	<input type="text"/>
System Location	<input type="text"/>
Device Up Time	0 Days 0 Hrs, 50 Mins, 13 Secs
System Time	<input type="text" value="Sat"/> <input type="text" value="January"/> <input type="text" value="01"/> <input type="text" value="2000"/> <input type="text" value="00"/> <input type="text" value="49"/> <input type="text" value="59"/>
Login Authentication Mode	<input type="text" value="Local"/>
Configuration Save Status	Not Initiated
Remote Save Status	Not Initiated
Configuration Restore Status	Not Initiated
Http Server Status	Enable
Http Port Number	<input type="text" value="80"/>
Reset Http Port Number	<input type="checkbox"/>
Telnet Status	<input type="text" value="Enable"/>
Logging Option	<input type="text" value="CONSOLE"/>
System MTU	1500
ISS Health Status	Up & Recoverable Runtime Error
ISS Health Error Reason	MemAlloc Failed. Pool ID: 451
Traffic Separation Control	None

Label	Description
<b>Hardware Version</b>	Displays the hardware version number of the system.

<b>Firmware Version</b>	Displays the firmware version number of the system.
<b>Hardware Part Number</b>	Displays the hardware part number of the system
<b>Software Serial Number</b>	Displays the software serial number of the system.
<b>System Name</b>	Displays the switch name.
<b>Software Version</b>	Displays the software version number of the system.
<b>Switch Name</b>	Enter the name for identifying the device. The default value is <b>RGS-PR9000-A</b> . This value range is a string of size <b>15</b> .
<b>System Contact</b>	Enter the contact person details for this managed node. This value range is a string of size <b>50</b> . If the contact information is not available, this value takes a zero-length string.
<b>System Location</b>	Enter the physical location of this node. This value range is a string of size <b>50</b> . If the location is unknown, this value takes a zero-length string.
<b>Device Up Time</b>	Displays the time from which the device is up. The format is Days Hours, Minutes, Seconds. Example: 0 Days 1Hrs, 15Mins, 27 Secs.
<b>System Time</b>	Select the current date and time The format is Day Month Date Year Hours Minutes Seconds Example: Fri May 07 2010 13: 40: 00. This value range is a string of size <b>40</b> .
<b>Login Authentication Mode</b>	<p>Select the login authentication mode. The list contains:</p> <ul style="list-style-type: none"> <li>– Local – Sets the authentication mode as Local. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.</li> <li>– Remote – Sets the authentication mode as Remote. Authentication is done in the remote location through a RADIUS (Remote Authentication Dial-In User Service) or TACACS server. RADIUS is a protocol that 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 (Terminal Access Controller Access-Control System) is a remote authentication protocol that is used to communicate with an authentication server commonly used in networks.</li> <li>– Tacacs - Sets the authentication mode as TACACS.</li> </ul>

	Authentication is done through a TACACS+ server.
<b>Configuration Save Status</b>	<p>Displays the configuration save status. The default option is <b>Not Initiated</b> Once the configuration is done, the save status will be displayed as any of the following:</p> <ul style="list-style-type: none"> <li>– Successful – System information is configured and saved successfully.</li> <li>– Failure - System information configuration save failed.</li> <li>– In progress - System information configuration save is in progress.</li> <li>– Not Initiated - System information configuration save is not initiated.</li> </ul>
<b>Remote Save Status</b>	<p>Displays the remote save status. The default option is <b>Not Initiated</b> This status represents the status of save operation to the remote location as any of the following:</p> <ul style="list-style-type: none"> <li>– Successful –Remote information is configured and saved successfully</li> <li>– Failure - Remote information configuration save failed.</li> <li>– Inprogress - Remote information configuration save is in progress.</li> <li>– Not Initiated - Remote information configuration save is not initiated.</li> </ul>
<b>Configuration Restore Status</b>	<p>Displays the configuration restoration status. The default option is <b>Not Initiated</b> The already configured parameter will be restored and the status will be displayed as any of the following</p> <ul style="list-style-type: none"> <li>– Successful – Configuration is restored successfully.</li> <li>– Failure – Configuration restoration failed.</li> <li>– In progress – Configuration restoration is in progress.</li> <li>– Not Initiated – Configuration restoration is not initiated.</li> </ul>
<b>HTTP Server Status</b>	<p>Displays the status of the HTTP server as either enable or disable. The default option is <b>Enable</b>.</p>
<b>HTTP Port Number</b>	<p>Displays the port to be used by the host to configure the router using the Web interface. This value ranges from 1 to 65535. The default value is <b>80</b>. Once the port number is changed, the Http Server Status is disabled and enabled. Open the HTTP session</p>

	with IP address and new port number. For example, enter as 12.0.0.1:100, where 12.0.0.1 represents the IP of the switch and 100 represents the port number.
<b>Reset HTTP Port Number</b>	Click the check box to reset the configured <b>Http Port Status</b> to its default value of 80. Once the port number is set to default value, the Http Server Status is disabled and enabled. Open the HTTP session with the IP address alone. For example, enter as 12.0.0.1, where 12.0.0.1 represents the IP of the switch.
<b>Telnet Status</b>	Select to set the status of TELNET in the system. The default option is <b>Enable</b> . The list contains the following; <ul style="list-style-type: none"> <li>– Enable – Sets the Telnet status as enabled.</li> <li>– Disable – Sets the Telnet status as disabled.</li> <li>– enableInProgress - Sets the Telnet status as enableInProgress.</li> <li>– disableInProgress – Sets the Telnet status as disableInProgress.</li> </ul>
<b>Logging Option</b>	Select the path to log the debug details. The default option is <b>Console</b> . The list contains: <ul style="list-style-type: none"> <li>– Console – Logs the debug details in a console.</li> <li>– File – Logs the debug details in a file (system buffer).</li> </ul>
<b>System MTU</b>	Enter the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. This value ranges from 90 to 9216. The default value is <b>1500</b> .
<b>ISS Health Status</b>	Displays the RGS-PR9000-A health status. The default option is Up & Running. The options are: <ul style="list-style-type: none"> <li>– Up &amp; Running - Indicates that the health status of RGS-PR9000-A is up and running and performing its job smoothly.</li> <li>– downNonRecoverableErr - Indicates that the health status of RGS-PR9000-A is down due to occurrence of some non-recoverable error.</li> <li>– upRecoverableRuntimeErr - Indicates that the health status of RGS-PR9000-A is up but indicates the occurrence of a runtime error that is recoverable</li> </ul>
<b>ISS Health Error Reason</b>	Displays the reason for errors encountered. The default option is <b>None</b> . The options are:

	<ul style="list-style-type: none"> <li>– nonRecovTaskInitializationFailure - Indicates the occurrence of non-recoverable failure during Task initialization.</li> <li>– nonRecovInsufficientStartupMemory - Indicates that there is insufficient memory for successful startup. This error is non-recoverable and requires sufficient memory to be available in the system for successful RGS-PR9000-A startup.</li> <li>– recovCruBuffExhausted - Indicates that CRU Buffer Exhausted.</li> <li>– recovConfigRestoreFailed - Indicates that config-restore failed for RGS-PR9000-A. This is a recoverable error.</li> <li>– recovProtocolMemPoolExhausted - Indicates that a mem-pool associated with a specific module in RGS-PR9000-A has drained out. This error may affect the functioning of the specific protocol alone and is treated as a recoverable error</li> <li>– None - Does not indicate any reason for errors encountered.</li> </ul>
<b>Traffic Separation Control</b>	<p>Displays the traffic separation control status. This implies the method for receiving control packets to CPU. The default option is <b>none</b>. The options can be</p> <ul style="list-style-type: none"> <li>– System_default - Specifies the method for receiving control packets to CPU as system default. This implies that the software can automatically install the ACL and QoS rules for all the control packets.</li> <li>– User_defined - Specifies the method for receiving control packets to CPU as user defined. This implies that the software cannot automatically install the ACL and QoS rules for all the control packets. Only the administrator can install the required rules for receiving control packets to CPU</li> <li>– none - Specifies the method for receiving control packets to CPU as none.</li> </ul>

## 4.1.2 NVRAM Settings

The NVRAM Settings tab allows the user to configure the initialization parameters. Whenever the switch is started or reboot, RGS-PR9000-A reads these initialization parameters before the task initialization and updates them in the local data structure. These parameters are applied to their specific RGS-PR9000-A component such as SNMP, when the task is created



for that component.

IP Address Mode	Manual
IP Address Alloc Protocol	DHCP
Default IP Address	192.168.10.1 *
Subnet Mask	255.255.255.0
Switch Base MAC Address	00:1e:94:00:00:01
Default Interface Name	Gi0/1
SNMP EngineID	80.00.08.1c.04.46.53
PIM Mode	Sparse
Snoop Forward Mode	MAC Based
Cli Serial Console	Yes
Default VLAN Identifier	1
Dynamic Port Count	28
Reset Dynamic Port Count	<input type="checkbox"/>
Incremental Save	Disable
Auto-Save Trigger	Disable
Rollback	Enable
<input type="button" value="Apply"/>	

Label	Description
<b>IP Address Mode</b>	<p>Select the mode by which the default interface in the device gets the IP address. The default option is <b>Manual</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Manual – Assigns the Static IP address to the default interface. The IP address defined in the field Default IP Address and the IP mask defined in the field Subnet Mask are assigned to the interface.</li> <li>- Dynamic – Assigns IP address dynamically, that is, IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client, RARP client, BOOTP client and the like.</li> </ul>
<b>IP Address Alloc Protocol</b>	<p>Select the dynamic IP address configuration protocol to be used for fetching the IP address dynamically, if the field IP Address</p>

	<p>Mode is selected as Dynamic. Allows the user to only view the selected dynamic IP address configuration protocol, if the field IP Address Mode is selected as Manual. The default option is <b>DHCP</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– RARP – Reverse Address Resolution Protocol that allows a client device to dynamically find its IP address, when it has only its hardware address such as MAC address.</li> <li>– DHCP – Dynamic Host Configuration Protocol that allows a client device to obtain configuration parameters such as network address, from the server.</li> <li>– BOOTP – Bootstrap Protocol that allows a client device to obtain its own IP address, address of a server host and name of a boot file to be executed.</li> </ul>
<b>Default IP Address</b>	<p>Enter the default IP address to change the IP address, if the field IP Address Mode is selected as Manual. The default value is <b>10.0.0.1</b>.</p>
<b>Subnet Mask</b>	<p>Enter the subnet mask for the configured IP address, if the field IP Address Mode is selected as Manual. Allows the user to only view the configured subnet mask, if the field IP Address Mode is selected as Dynamic. The default value is <b>255.0.0.0</b>.</p>
<b>Switch Base MAC Address</b>	<p>Enter the base MAC address of the switch. This MAC address is assigned to the default interface of the switch. The switch uses this address as its hardware address. Layer 3 modules use the switch MAC address as the source MAC address in the transmitted packets. The default value is <b>00:01:02:03:04:01</b>.</p>
<b>Default Interface Name</b>	<p>Enter the interface to be set as the default interface. 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 &lt;interface type&gt;&lt;slot number/port number&gt;. 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.). The default value is <b>Gi0/1</b>.</p>
<b>SNMP EngineID</b>	<p>Enter the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the</p>

	exchange of messages between the source and the destination. The default value is <b>80.00.08.1c.04.46.53</b> .
<b>PIM Mode</b>	Select the operation mode of the PIM. The default option is <b>Sparse</b> . The list contains: <ul style="list-style-type: none"> <li>– Dense – Sets operation mode of PIM as Dense Mode. PIM implements a flood and prune mechanism. PIM floods multicast traffic periodically and prunes branches of shortest-path tree where no interested receivers are present. This mode is best suited for networks where few or no prunes occur.</li> <li>– Sparse sets operation mode of PIM as Sparse Mode. PIM forwards multicast traffic to the device only if an explicit request is received from that device for this traffic. This mode is best suited for Internet.</li> </ul>
<b>Snoop Forward Mode</b>	Select the mode to be used for building the forwarding table that is used during IGS / MLDS. The default option is <b>MAC Based</b> . The list contains: <ul style="list-style-type: none"> <li>– IP Based – Uses table containing IP multicast forwarding information based on both outer and inner VLAN, during snooping.</li> <li>– MAC Based – Uses table containing MAC based multicast forwarding information, during snooping.</li> </ul>
<b>Cli Serial Console</b>	Select whether the CLI console prompt is required for the session through serial console. The default option is <b>Yes</b> . The list contains: <ul style="list-style-type: none"> <li>– Yes – Specifies that CLI prompt is made available in the serial console session.</li> <li>– No – Specifies that CLI prompt is not made available in the serial console session.</li> </ul>
<b>Default VLAN Identifier</b>	Enter the default VLAN identifier to be used at system startup. This VLAN is set as the default VLAN on switch reboot. The format of this field is integer. This value ranges from 1 to 4094. The default value is <b>1</b> which implies that VLAN 1 is set as the default VLAN.
<b>Dynamic Port Count</b>	Enter the number of ports required for the RGS-PR9000-A. The maximum count equal to the system defined maximum physical

	<p>interfaces. The default value is the system defined maximum physical interfaces.</p>
<b>Reset Dynamic Port Count</b>	<p>Click to enable the Reset Dynamic Port Count. If this check box is enabled, the system takes the default value on restarting the system again.</p>
<b>Incremental Save</b>	<p>Select one of the options to indicate whether SNMP Update Trigger for Incremental Save is to be generated or not. The default option is <b>Enable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enable – Enables the incremental save which generates the update trigger for each time a nmhSet operation is successful.</li> <li>– Disable – Disables the incremental save option which will not generate the update trigger at all.</li> </ul>
<b>Auto-Save Trigger</b>	<p>The auto-save trigger option to save the configuration done automatically or manually. The default option is <b>Disable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enable – Specifies that all the configuration is saved automatically.</li> <li>– Disable – Specifies that configuration done will not be saved automatically</li> </ul>
<b>Rollback</b>	<p>Select the SNMP rollback feature. The default option is <b>Enable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enable – Enables the SNMP rollback feature. The enabled value specifies that it allows the failure in set operation for any varbind which result in rollback of all varbinds whose value has been set in this SET PDU</li> <li>– Disable – Disables the SNMP rollback feature. The disabled value specifies that it allows the failure in set operation to simply return error</li> </ul>

### 4.1.3 ACL

An ACL (Access Control List) is a list of permissions attached to an object. An ACL specifies which users or system processes are authorized to access the objects and what operations are allowed on given objects.

### 4.1.3.1 MAC ACL

This screen allows the user to create a MAC (Media Access Control ) ACL and configure its parameters

ACL Number	<input type="text"/> *
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Action	Permit <input type="button" value="v"/>
Priority	<input type="text"/> *
VLAN ID	- <input type="button" value="v"/>
Port List (Incoming)	<input type="text"/>
Port List (Outgoing)	<input type="text"/>
Encapsulation	<input type="text"/>
Protocol	- <input type="button" value="v"/> <input type="text" value="0"/>
Sub-Action	None <input type="button" value="v"/>
Sub-Action-Id	<input type="text"/>
OuterEtherType	<input type="text"/>
SVLAN-ID	<input type="text"/>
SVlan Priority	<input type="text"/>
CVlan Priority	<input type="text"/>
Packet Tag Type	Single-Tag <input type="button" value="v"/>
CFI/DEI	<input type="text"/>
Drop Precedence	Green <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Number	Source MAC	Destination MAC	Action	Priority	VLAN ID	Port List (Incoming)	Port List (Outgoing)	Encapsulation	Protocol	Protocol Number	SubAction	SubAction-Id (VLAN-ID)	OuterEtherType	SVLAN ID	SVLAN Priority	CVLAN Priority	Packet Tag Type	CFI/DEI	Drop Precedence
--------	--------	------------	-----------------	--------	----------	---------	----------------------	----------------------	---------------	----------	-----------------	-----------	------------------------	----------------	----------	----------------	----------------	-----------------	---------	-----------------

Label	Description
<b>ACL Number</b>	Enter the ACL number which is the unique identifier for the access list. This value ranges from 1 to 65535.
<b>Source MAC</b>	Enter the source unicast MAC address for which the access control must be applied. The default value is 0 which implies that any source mac address can be filtered.

<b>Destination MAC</b>	Enter the destination unicast MAC address for which the access control must be applied. The default value is <b>0</b> , which implies that any destination mac address can be filtered.
<b>Action</b>	Select the action to be taken on the packet if the filter rule matches. The default option is <b>Permit</b> . The list contains: <ul style="list-style-type: none"> <li>– Permit – Forwards the packet according to the forwarding rules.</li> <li>– Deny – Discards the packet.</li> <li>– Redirect – Switches the packet according to the redirect rules.</li> </ul>
<b>Priority</b>	Enter priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255. The default value is <b>1</b> .
<b>VLAN ID</b>	Select the VLAN ID (Identifier) for which the access control has to be applied. This value ranges from 0 to 4094. The default value is <b>0</b> , which implies that this object is not used.
<b>Port List (Incoming)</b>	Enter the in port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list.
<b>Port List (Outgoing)</b>	Enter the out port list which is the set of ports over which the filter is to be applied for packets egress at ports in this list.
<b>Encapsulation</b>	Enter the encapsulation type of the packet for which the access control has to be applied. This value ranges from 1 to 65535.
<b>Protocol</b>	Select the non-IP Protocol type of the packet for which the access control has to be applied. The default value is <b>0</b> , which implies that the filter is applicable for all protocols. The list contains: <ul style="list-style-type: none"> <li>– aarp – Specifies Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address</li> <li>– amber – Specifies EtherType DEC-Amber</li> <li>– dec-spanning – Specifies EtherType Digital Equipment Corporation (DEC) spanning tree</li> <li>– decnet_iv – Specifies EtherType DECnet Phase IV protocol</li> <li>– diagnostic – Specifies EtherType DEC-Diagnostic</li> <li>– dsm – Specifies EtherType DEC-DSM/DDP</li> <li>– etype-6000 – Specifies EtherType 0x6000</li> <li>– etype-8042 – Specifies EtherType 0x8042</li> </ul>

	<ul style="list-style-type: none"> <li>- lat – Specifies EtherType DEC-LAT</li> <li>- lavc-sca – Specifies EtherType DEC-LAVC-SCA</li> <li>- mop-consol – Specifies EtherType DEC-MOP Remote Console</li> <li>- mop_dump – Specifies EtherType DEC-MOP Dump</li> <li>- msdos – Specifies EtherType DEC-MSDOS</li> <li>- mumps – Specifies EtherType DEC-MUMPS</li> <li>- netbios – Specifies EtherType DEC- Network Basic Input/Output System (NETBIOS)</li> <li>- vines-echo – Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems</li> <li>- vines-ip – Specifies EtherType VINES IP</li> <li>- xns-id – Specifies EtherType Xerox Network Systems (XNS) protocol suite</li> <li>- other - Specifies other protocols</li> </ul>
<b>Sub-Action</b>	<p>Select the VLAN specific sub action to be performed on the incoming packet. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- None – Performs no action. Does not consider the actions related to the VLAN ID.</li> <li>- Modify VLAN - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>- Nested VLAN - Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> <li>- Strip Outer Header - Strips the outer header of the traffic matching ACL rule.</li> <li>- Modify CFI DEI -Modifies the CFI or DEI bit of the packet.</li> <li>- Modify DP - Modifies the Drop Precedence of the traffic.</li> <li>- Modify TC - Modifies the TC of the traffic.</li> </ul>
<b>Sub-Action-Id</b>	<p>Enter the unique identifier for the VLAN specific sub action to be performed on the packet. This value ranges from 0 to 4094. The default value is <b>0</b>.</p>
<b>OuterEtherType</b>	<p>Enter the ether type value of the outer VLAN tag of a packet. This</p>

	value ranges from 1 to 65535. The default value is <b>0</b> , which implies the don't care condition, packet with any ether type value are considered.
<b>SVLAN-ID</b>	Enter the SVLAN-ID present in the outer tag to be filtered. This value ranges from 1 to 4094. The default value is <b>0</b> .
<b>SVlan Priority</b>	Enter the service VLAN priority present in the outer tag to be filtered. This value ranges from 0 to 7. The default value is <b>-1</b> .
<b>CVlan Priority</b>	Enter the customer VLAN priority value present in the outer tag to be filtered This value ranges from 0 to 7. The default value is <b>-1</b>
<b>Packet Tag Type</b>	Select the packet tag type for which the access control has to be applied. The list contains Single-Tag and Double-Tag. The default value is <b>Single-Tag</b> . <ul style="list-style-type: none"> <li>- Single-Tag - Applies the configured filter parameters on single VLAN tagged packets</li> <li>- Double-Tag - Applies the configured filter parameters on double VLAN tagged packets.</li> </ul>
<b>CFI/DEI</b>	Enter the CFI/DEI bit value in the c-vlan tag or s-vlan tag of the packet for which the access control has to be applied This value ranges from 0 to 1
<b>Drop Precedence</b>	Select the drop precedence level for which the access control has to be applied. The default option is <b>Green</b> . The list contains: <ul style="list-style-type: none"> <li>- None - Sets the drop precedence level as None.</li> <li>- Green - Sets the drop precedence level as Green.</li> <li>- Yellow - Sets the drop precedence level as Yellow.</li> <li>- Red - Sets the drop precedence level as Red.</li> </ul>

#### 4.1.3.2 IP Standard ACL

The screen allows the user to set the IP Standard ACL Configuration. Standard access lists create filters based on IP address and network mask only (L3 filters only).



ACL Number	<input type="text"/> *
Action	Permit <input type="button" value="v"/>
Source IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Destination IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Port List (Incoming)	<input type="text"/>
Port List (Outgoing)	<input type="text"/>
Priority	<input type="text"/>
SubAction	None <input type="button" value="v"/>
SubAction-Id(VLAN-ID)	<input type="text"/>
SVLAN-ID	<input type="text"/>
SVlan Priority	<input type="text"/>
CVLAN-ID	<input type="text"/>
CVlan Priority	<input type="text"/>
Packet Tag Type	Single-Tag <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

ACL Number	Action	Source IP	Subnet Mask	Destination IP	Subnet Mask	Port List (Incoming)	Port List (Outgoing)	Priority	SubAction	SubAction-Id(VLAN-ID)	SVLAN-ID	SVLAN Priority	CVLAN-ID	CVLAN Priority	Packet Tag Type
------------	--------	-----------	-------------	----------------	-------------	----------------------	----------------------	----------	-----------	-----------------------	----------	----------------	----------	----------------	-----------------

Label	Description
<b>ACL Number</b>	Enter the standard ACL Number which is the unique identifier for the standard access list. This value ranges from 1 to 1000.
<b>Action</b>	Select the action to be taken for the access list. The default option is <b>Permit</b> . The list contains: <ul style="list-style-type: none"> <li>- Permit – Allows the packets when a match has been found.</li> <li>- Deny – Drops the packets when a match has been found.</li> </ul>

	<ul style="list-style-type: none"> <li>– Redirect – Switches the packet according to the redirect rules.</li> </ul>
<b>Source IP Address</b>	Enter the IP Address to match against the packet's source IP address.
<b>Destination IP Address</b>	Enter the destination IP Address to match against the packet's destination IP address.
<b>Subnet Mask</b>	Enter the address mask corresponding to the IP Address.
<b>Port List (Incoming)</b>	Enter the in port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list.
<b>Port List (Outgoing)</b>	Enter the out port list which is the set of ports over which the filter is to be applied for packets egress at ports in this list.
<b>Priority</b>	Enter priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255. The default value is <b>1</b> .
<b>Sub-Action</b>	<p>Select the VLAN specific sub action to be performed on the incoming packet. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– None – Performs no action. Does not consider the actions related to the VLAN ID.</li> <li>– Modify VLAN - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>– Nested VLAN - Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul>
<b>Sub-Action-Id</b>	Enter the unique identifier for the VLAN specific sub action to be performed on the packet. This value ranges from 0 to 4094.
<b>SVlan ID</b>	Enter the SVLAN-ID present in the outer tag for which the access control has to be applied This value ranges from 1 to 4094. The default value is <b>0</b> .
<b>Svlan Priority</b>	Enter the service VLAN priority present in the outer tag to be filtered. This value ranges from 0 to 7. The default value is <b>-1</b> .
<b>CVLAN-ID</b>	Enter the customer VLAN id for which the access control has to be applied. This value ranges from 1 to 4094. The default value is <b>0</b> .
<b>CVlan Priority</b>	Enter the customer VLAN priority value present in the outer tag to be filtered. This value ranges from 0 to 7. The default value is <b>-1</b> .
<b>Packet Tag Type</b>	Select the packet tag type for which the access control has to be

applied. The list contains Single-Tag and Double-Tag. The default value is **Single-Tag**.

- Single-Tag - Applies the configured filter parameters on single VLAN tagged packets
- Double-Tag - Applies the configured filter parameters on double VLAN tagged packets.

### 4.1.3.3 IP Extended ACL

The screen allows the user to set the IP Extended ACL Configuration. Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

ACL Number	<input type="text"/> *		
Action	Permit <input type="button" value="v"/>		
Address Type	IPV4 <input type="button" value="v"/>		
Source IP Address	<input type="text"/>		
Subnet Mask	<input type="text"/>		
Destination IP Address	<input type="text"/>		
Subnet Mask	<input type="text"/>		
Port List (Incoming)	<input type="text"/>		
Port List (Outgoing)	<input type="text"/>		
Protocol	ICMP <input type="button" value="v"/>	<input type="text"/>	
Message Code	255 <input type="text"/>		
Message Type	255 <input type="text"/>		
Priority	<input type="text"/>		
Dscp	<input type="text"/>		
TOS	<input type="text"/>		
ACK Bit	<input type="button" value="v"/>		
RST Bit	<input type="button" value="v"/>		
Source Port (Min)	<input type="text"/>	Source Port (Max)	<input type="text"/>
Destination Port (Min)	<input type="text"/>	Destination Port (Max)	<input type="text"/>
Destination Prefix Length	<input type="text"/>	Source Prefix Length	<input type="text"/>
Flow Id	<input type="text"/>		
Storage	Volatile <input type="button" value="v"/>		
Sub-Action	None <input type="button" value="v"/>		
SubAction-Id(VLAN-ID)	<input type="text"/>		
SVLAN-ID	<input type="text"/>		
SVlan Priority	<input type="text"/>		
CVLAN-ID	<input type="text"/>		
CVlan Priority	<input type="text"/>		
Packet Tag Type	Single-Tag <input type="button" value="v"/>		

Select	Filter	Action	Address	Source	Subnet	Destination	Subnet	Port List	Port List	Protocol	Other	Code	Type	Priority	Dscp	TOS	ACK	RST	Source	Source	Destination	Destination	Destination	Source
No	Type		IP	IP	Mask	IP	Mask	(Incoming)	(Outgoing)							Bit	Bit	Port	Port	Port	Port	Port	Prefix	Prefix
																		(Min)	(Max)	(Min)	(Max)	Length	Length	

FlowId	Storage	SubAction	SubAction- Id(VLAN- ID)	SVLAN- ID	SVLAN Priority	CVLAN- ID	CVLAN Priority	Packet Tag Type
--------	---------	-----------	-------------------------------	--------------	-------------------	--------------	-------------------	-----------------------

Label	Description
<b>ACL Number</b>	Enter the ACL Number which is the unique identifier for the Extended access list. This value ranges from 1001 to 65535.
<b>Action</b>	Select the action to be taken for the access list. The default option is <b>Permit</b> . The list contains: <ul style="list-style-type: none"> <li>– Permit – Allows the packets when a match has been found.</li> <li>– Deny – Drops the packets when a match has been found.</li> <li>– Redirect – Switches the packet according to the redirect rules.</li> </ul>
<b>Address Type</b>	Select the type of IP address used by the entry. The list contains: <ul style="list-style-type: none"> <li>– None - Sets the address type as none, which implies that address type is not considered.</li> <li>– IPV4 – Sets the IP address type for the ACL as IPv4.</li> <li>– IPV6 – Sets the IP address type for the ACL as IPv6.</li> </ul>
<b>Source IP Address</b>	Enter the IP address to match against the packet's source IP address.
<b>Subnet Mask</b>	Enter the address mask corresponding to the IP Address.
<b>Destination IP Address</b>	Enter the IP Address to match against the packet's destination IP address.
<b>Port List (Incoming)</b>	Enter the in port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list.
<b>Port List (Outgoing)</b>	Enter the out port list which is the set of ports over which the filter is to be applied for packets egress at ports in this list.
<b>Protocol</b>	Select the Protocol type to be checked against the packet. The default option is <b>ICMP</b> . The list contains: <ul style="list-style-type: none"> <li>– ICMP – Specifies that the filter is to be applied for Internet Control Message Protocol packets.</li> <li>– IP – Specifies that the filter is to be applied for Internet Protocol packets</li> <li>– TCP – Specifies that the filter is to be applied for Transmission Control Protocol packets</li> <li>– UDP – Specifies that the filter is to be applied for User</li> </ul>

	<p>Datagram Protocol packets</p> <ul style="list-style-type: none"> <li>– OSPF – Specifies that the filter is to be applied for Open Shortest Path First packets</li> <li>– PIM – Specifies that the filter is to be applied for Protocol Independent Multicasting packets</li> <li>– OTHER – Specifies that the filter is to be applied for any other protocol packets</li> </ul> <p>The protocol number for the respective protocol can be entered in the text box next to this field. This value ranges from 1 to 255. The default value is <b>255</b>, which implies that any protocol packet can be filtered.</p>
<p><b>Message Code</b></p>	<p>Enter the message code to be checked for ICMP (Internet Control Message Protocol) Packets. This value ranges from 0 to 255. The default value is <b>255</b>, which implies that the message code is not checked against the packet. Some of the ICMP message Codes are:</p> <ul style="list-style-type: none"> <li>0 Network Unreachable</li> <li>1 Host Unreachable</li> <li>2 Protocol Unreachable</li> <li>3 Port Unreachable</li> <li>4 Fragment Need</li> <li>5 Source Route Fail</li> <li>6 Destination Network Unknown</li> <li>7 Destination Host Unknown</li> <li>8 Source Host Isolated</li> <li>9 Destination Network Administratively Prohibited</li> <li>10 Destination Host Administratively Prohibited</li> <li>11 Network Unreachable TOS</li> <li>12 Host Unreachable TOS</li> <li>255 No ICMP Code</li> </ul>
<p><b>Message Type</b></p>	<p>Enters the message type to be checked for ICMP Packets. This value ranges from 0 to 255. The default value is <b>255</b>, which implies that the message type is not checked against the packet. Some of the ICMP message types are:</p> <ul style="list-style-type: none"> <li>0 Echo Reply</li> <li>3 Destination Unreachable</li> <li>4 Source Quench</li> </ul>

	5 Redirect 8 Echo Request 11 Time Exceeded 12 Parameter Problem 13 Timestamp Request 14 Timestamp Reply 15 Information Request 16 Information Reply 17 Address Mask Request 18 Address Mask Reply 255 No ICMP type
<b>Priority</b>	Enter priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255. The default value is <b>1</b> .
<b>Dscp</b>	Enter the DSCP (Differentiated Services Code Point) value to be checked against the packet. This value ranges from 0 to 63. The default value is <b>-1</b> .
<b>TOS</b>	Select the type of service for the access list. The default option is <b>None</b> . The list contains: <ul style="list-style-type: none"> <li>– None - The ACL does not match the TOS field in the packets.</li> <li>– High Reliability - The ACL matches the packets with TOS field as high reliability,</li> <li>– High Throughput - The ACL matches the packets with TOS field as high throughput.</li> <li>– High Reliability and High Throughput - The ACL matches the packets with TOS field as high reliability and High throughput.</li> <li>– Low Delay - The ACL matches the packets with TOS field as Low delay.</li> <li>– Low Delay and High Reliability - The ACL matches the packets with TOS field as Low Delay and High Reliability,</li> <li>– Low Delay and High Throughput - The ACL matches the packets with TOS field as Low Delay and High Throughput.</li> <li>– Low Delay, High Throughput and High Reliability - The ACL matches the packets with TOS field as Low Delay, High</li> </ul>

	Throughput and High Reliability.
<b>ACK Bit</b>	<ul style="list-style-type: none"> <li>– Select the TCP Ack Bit to be checked against the incoming packet. The default value is <b>Any</b>. The list contains:</li> <li>– Establish - Sets the TCP Ack bit as Establish.</li> <li>– Not Establish - Sets the TCP Ack bit as Not Establish.</li> <li>– Any - Sets the TCP Ack bit as <b>Any</b>. This implies that the ACK bit is not checked to decide the action.</li> </ul>
<b>RST Bit</b>	<p>Select the TCP Reset Bit to be checked against the incoming packet. The default value is <b>Any</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Set - Sets the TCP RST bit</li> <li>– Not Set - Does not set the TCP RST Bit.</li> <li>– Any - Sets the TCP RSTbit as Any. This implies that the RST bit is not checked against the packet.</li> </ul>
<b>Source Port (Min)</b>	Enter the TCP/UDP (User Datagram Protocol) source port from which the access list has to be applied. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Source Port (Max)</b>	Enter the TCP/UDP source ports to which the access list has to be applied. This value ranges from 0 to 65535. The default value is <b>65535</b> .
<b>Destination Port (Min)</b>	Enter the TCP/UDP destination port from which the access list has to be applied. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Destination Port (Max)</b>	Enter the TCP/UDP destination port to which the access list has to be applied. This value ranges from 0 to 65535. The default value is <b>65535</b> .
<b>Destination Prefix Length</b>	Enter the length of the CIDR (Classless Inter Domain Routing) prefix carried in the destination IP address. This value ranges from 0 to 32 for IPv4 addresses and from 0 to 128 for IPv6 addresses. The default value is <b>0</b> .
<b>Source Prefix Length</b>	Enter the length of the CIDR prefix carried in the source IP address. This value ranges from 0 to 32 for IPv4 addresses and from 0 to 128 for IPv6 addresses. The default value is <b>0</b> .
<b>Flow Id</b>	Enter the flow identifier in an IPv6 header. This value ranges from 0 to 1048575.
<b>Storage</b>	Select the storage type for this entry. The list contains:

	<ul style="list-style-type: none"> <li>- Volatile - Specifies that the configurations are present.</li> <li>- Non-Volatile - Reflects the configuration for an interface whose interface index has been assigned but for which the supporting implementation is currently not present.</li> </ul>
<b>Sub-Action</b>	<p>Select the VLAN specific sub action to be performed on the packet. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- None - Performs no action. Does not consider the actions related to the VLAN ID.</li> <li>- Modify VLAN - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> </ul>
<b>SubAction-Id(VLAN-ID)</b>	<p>Enter the unique identifier for the VLAN specific sub action to be performed on the packet. This value ranges from 1 to 4094.</p>
<b>SVLAN-ID</b>	<p>Enter the SVLAN-ID present in the outer tag for which the access control has to be applied This value ranges from 1 to 4094 The default value is <b>0</b>.</p>
<b>SVlan Priority</b>	<p>Enter the service VLAN priority for which the access control has to be applied This value ranges from 0 to 7. The default value is <b>-1</b>.</p>
<b>CVLAN-ID</b>	<p>Enter the customer VLAN id for which the access control has to be applied. This value ranges from 1 to 4094. The default value is <b>0</b>.</p>
<b>CVlan Priority</b>	<p>Enter the customer VLAN priority value for which the access control has to be applied This value ranges from 0 to 7. The default value is <b>-1</b>.</p>
<b>Packet Tag Type</b>	<p>Select the packet tag type for which the access control has to be applied. The list contains Single-Tag and Double-Tag. The default value is <b>Single-Tag</b></p> <ul style="list-style-type: none"> <li>- Single-Tag - Applies the configured filter parameters on single VLAN tagged packets</li> <li>- Double-Tag - Applies the configured filter parameters on double VLAN tagged packets.</li> </ul>

#### 4.1.3.4 User Defined Filter Configuration

The screen allows the user to set the User Defined Filter configurations. User defined filters are required for specifying the user defined packet header elements for application of filter



rules. The user defined filters table is also used for supporting AND, OR,NOT operations on existing filter rules and deriving new user defined ACL rules.

User Defined Filter Id	<input type="text"/> *
Action	Permit <input type="button" value="v"/>
Packet Type	User Defined <input type="button" value="v"/>
Offset Base	L2 <input type="button" value="v"/>
Offset Position 1	<input type="text"/>
Offset Value 1	<input type="text"/>
Offset Position 2	<input type="text"/>
Offset Value 2	<input type="text"/>
Offset Position 3	<input type="text"/>
Offset Value 3	<input type="text"/>
Offset Position 4	<input type="text"/>
Offset Value 4	<input type="text"/>
Offset Position 5	<input type="text"/>
Offset Value 5	<input type="text"/>
Offset Position 6	<input type="text"/>
Offset Value 6	<input type="text"/>
Sub-Action	None <input type="button" value="v"/>
SubAction-Id	<input type="text"/>
Priority	<input type="text"/> *
Port List (Incoming)	<input type="text"/>
Filter One Type	MAC Based <input type="button" value="v"/>
Filter One Id	<input type="text"/>
Filter Two Type	MAC Based <input type="button" value="v"/>
Filter Two Id	<input type="text"/>

Select	User Defined Id	Action	Packet Type	Offset Base	Offset Position1	Offset Value1	Offset Position2	Offset Value2	Offset Position3	Offset Value3	Offset Position4	Offset Value4	Offset Position5	Offset Value5	Offset Position6	Offset Value6	Offset Mask	SubAction	SubAction Id	Priority	Port List (Incoming)
--------	-----------------	--------	-------------	-------------	------------------	---------------	------------------	---------------	------------------	---------------	------------------	---------------	------------------	---------------	------------------	---------------	-------------	-----------	--------------	----------	----------------------

Label	Description
<b>User Defined Filter Id</b>	Enter the unique identifier for the user defined filter. This value ranges from 1 to 65535.
<b>Action</b>	<p>Select the filter action. The default option is <b>Permit</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Permit – Allows the packets when a match has been found.</li> <li>– Deny – Drops the packets when a match has been found.</li> <li>– Redirect – Switches the packet according to the redirect rules.</li> <li>– Concatenate - Applies logical AND operation on base filter rules.</li> <li>– Disjunction - Applies logical OR operations on base filter rules.</li> <li>– Negate - Applies logical NOT operations on base filter rules.</li> </ul>
<b>Packet Type</b>	<p>Select the packet type to apply the packet-filter match on incoming traffic. The default option is <b>User Defined</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– User Defined - Specifies the packet type as User defined</li> <li>– IPv4 - Specifies the packet type as IPv4.</li> <li>– IPv6 - Specifies the packet type as IPv6.</li> <li>– IPv4TCP - Specifies the packet type as TCP in the IPV4 packet.</li> <li>– IPv4UDP -Specifies the packet type as UDP in the IPV4 packet.</li> <li>– MPLS - Specifies the packet type as MPLS</li> <li>– Fragmented IP – Specifies the packet type as Fragmented IP.</li> </ul>
<b>Offset Base</b>	<p>Select the offset base start of the packet from which the user defined byte must be considered. The list contains:.</p> <ul style="list-style-type: none"> <li>– L2 – Specifies the start of layer 2 Header.</li> <li>– L3 – Specifies the start of layer 3 Header</li> <li>– L4 – Specifies the start of layer 4 Header.</li> <li>– IPv6 Extension Header– Specifies the start of ipv6 extended header</li> </ul>

	<ul style="list-style-type: none"> <li>- Ether Type – Specifies the start from ether type</li> </ul>
<b>Offset Position 1-6</b>	Enter the offset position that needs to be considered as the match for offset 1 to 6. This value ranges from 0 to 127.
<b>Offset Value 1-6</b>	Enter the Offset Value that needs to be considered as the match for offset 1 to 6. This value ranges from 0 to 255.
<b>Sub-Action</b>	<p>Select the VLAN specific sub action to be performed on the packet. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- None - Does not consider the actions related to the VLAN ID.</li> <li>- Modify VLAN - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>- Nested VLAN - Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul>
<b>SubAction-Id</b>	Enter the unique identifier for the VLAN specific sub action to be performed on the packet. This value ranges from 1 to 4094.
<b>Priority</b>	Enter priority of the User defined filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255. The default value is 1.
<b>Port List (Incoming)</b>	Enter the in port list which is the set of ports over which the filter is to be applied for packets ingress at ports in this list.
<b>Filter One Type</b>	<p>Select the filter one type which is the type of the Base ACL rule 1 that is used for deriving new ACL rule The default option is <b>Mac Based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Mac Based - Specifies that the ACL for rule 1 is an MAC based ACL.</li> <li>- IP Based - Specifies that the ACL for rule 1 is an MAC based ACL.</li> </ul>
<b>Filter One Id</b>	Enter the. ID of the Base ACL rule 1 (MAC-based or IP-based) that is used for deriving new ACL rule. This value ranges from 1 to 65535.
<b>Filter Two Type</b>	<p>Select the filter two type which is the type of the Base ACL rule 2 that is used for deriving new ACL rule. The default option is <b>Mac Based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Mac Based - Specifies that the ACL for rule 2 is an MAC</li> </ul>

	<p>based ACL.</p> <ul style="list-style-type: none"> <li>- IP Based - Specifies that the ACL for rule 2 is an MAC based ACL.</li> </ul>
<b>Filter Two Id</b>	<p>Enter the ID of the Base ACL rule 2 (MAC-based or IP-based) that is used for deriving new ACL rule. This value ranges from 1 to 65535.</p>

### 4.1.3.5 Redirect Interface Group

This screen allows you to configure the details of Redirect Interface Group. An interface group is a collection of physical ports (or) trunks that are grouped together for distributing traffic received on an ingress interface. Based on the access-list match on an incoming interface, traffic is distributed among the member ports of an interface-group/ virtual trunk.

Select	Filter Type	Filter ID	Port List	Distribution Byte	UDB Position
--------	-------------	-----------	-----------	-------------------	--------------

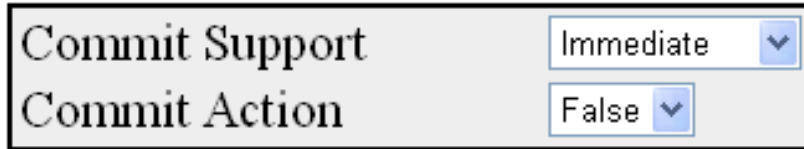
Label	Description
<b>Filter Type</b>	<p>Select the filter type. The default option is L2 Filter. The list contains</p> <ul style="list-style-type: none"> <li>- L2 Filter - Specifies that redirect action is to be applied on L2 filter rules in the system.</li> <li>- L3 Filter - Specifies that redirect action is to be applied on L3 filter rules in the system.</li> <li>- User Defined - Specifies that redirect action is to be applied on user defined filter rules in the system.</li> </ul>
<b>Filter ID</b>	<p>Enter the unique filter identifier. This value ranges from 1 to 65535.</p>

<b>Port/Port List</b>	Enter the single port or multiple ports list for which the access control has to be applied.
<b>Distribution Byte</b>	<p>Select the Distribution Byte that needs to be used for deriving the traffic distribution hash-logic for the set of interfaces. The output of the hash-logic is an egress interface from amongst the member ports of a virtual trunk. Traffic is redirected to this egress interface. The list contains</p> <ul style="list-style-type: none"> <li>– NONE - Sets the distribution byte as none.</li> <li>– UDB - Sets the distribution byte as UDB.</li> <li>– SRC IP- Uses the source IP in the packet header for distributing traffic.</li> <li>– DST IP - Uses the Destination IP in the packet header for distributing traffic.</li> <li>– SRC MAC - Uses the source MAC in the packet header for distributing traffic.</li> <li>– DST MAC - Uses the destination MAC in the packet header for distributing traffic.</li> <li>– SRC TCP PORT - Uses the source TCP Port value in the packet header for distributing traffic.</li> <li>– DST TCP PORT - Uses the destination TCP Port value in the packet header for distributing traffic.</li> <li>– SRC UDP PORT - Uses the source UDP Port value in the packet header for distributing traffic.</li> <li>– DST UDP PORT - Uses the destination UDP Port value in the packet header for distributing traffic.</li> <li>– VLAN ID - Uses the VLAN Id in the packet header for distributing traffic.</li> <li>– ETHERTYPE - Uses the ethertype value in the packet header for distributing traffic.</li> <li>– INNER IP - Uses the Inner IP in the packet header for distributing traffic. This option is used for encapsulating IP packets.</li> </ul>
<b>UDB Position</b>	Enter the user defined position of a byte in the packet which is to be looked for distribution. This value ranges from 0 to 128. The

	default value is <b>0</b> .
--	-----------------------------

### 4.1.3.6 Provision Mode

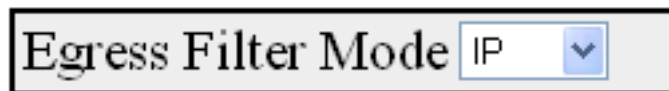
This screen allows the user to configure the details of provision mode.



Label	Description
<b>Commit Support</b>	Select the commit support for which access control rule needs to be applied. The default option is <b>Immediate</b> . The list contains: <ul style="list-style-type: none"> <li>– Immediate – Applies the rules directly</li> <li>– Consolidated - Applies the rules after the commit is issued.</li> </ul>
<b>Commit Action</b>	Select the commit action to be taken for the access list. The default option is <b>False</b> . The list contains: <ul style="list-style-type: none"> <li>– False - Does not set the commit action</li> <li>– True - Sets the commit action</li> </ul>

### 4.1.3.7 Egress Filter Mode

This screen allows the user to configure the egress filter mode.



Label	Description
<b>Egress Filter Mode</b>	Select the egress filter mode for the L3 Filter. The default value is <b>IP</b> . The list contains: <ul style="list-style-type: none"> <li>– IP – Supports IP based PCL (Policy Control List) at egress.</li> <li>– MAC - Supports MAC based PCL (Policy Control List) at egress.</li> </ul>

## 4.1.4 IP Authorized Manager

This page allows you to configure how a user is authenticated when he/she logs into the switch

via one of the management interfaces.

Deny

IP Address	<input type="text"/>	*
Subnet Mask	<input type="text"/>	*
Port List (Incoming)	<input type="text"/>	
VLANs Allowed	<input type="text"/>	
Services Allowed	<input type="checkbox"/> ALL <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> SSH	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

<b>IP Address</b>	<b>Subnet Mask</b>	<b>Port List (Incoming)</b>	<b>VLANs Allowed</b>	<b>Cpu0</b>	<b>Services Allowed</b>
<input type="button" value="Apply"/> <input type="button" value="Delete"/>					

Label	Description
<b>IP Address</b>	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 <b>Any Manager</b> .
<b>Subnet Mask</b>	Enter the subnet mask for the configured IP address. The maximum length of subnet mask is 15. Value 0.0.0.0 indicates mask for <b>Any Manager</b> .
<b>Port List (Incoming)</b>	Enter the port numbers through which the manager can access the switch.
<b>VLANs Allowed</b>	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.
<b>Services Allowed</b>	<p>Click the allowed services through which the manager can access the switch. The default option is <b>ALL</b>. Options are:</p> <ul style="list-style-type: none"> <li>- ALL – Supports all the services</li> <li>- 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</li> </ul>

	<p>requesters</p> <ul style="list-style-type: none"><li>- 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.</li><li>- HTTP – HTTP (Hyper Text 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 screen</li><li>- 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.</li><li>- 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.</li></ul>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.1.5 Save and Restore

The **Save and Restore** link allows the user to configure the current configuration Save and Restore options for the switch:



**4.1.5.1 Save**

Save option	<input type="radio"/> Save to Startup-config <input checked="" type="radio"/> Remote Backup
Transfer Mode	TFTP <input type="button" value="v"/>
Address Type	IPv4 <input type="button" value="v"/>
IP Address	<input type="text" value="0.0.0.0"/>
SFTP User Name	<input type="text"/>
SFTP Password	<input type="text"/>
File Name	<input type="text" value="iss.conf"/>
	<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Label	Description
<b>Save Option</b>	<p>Click one of the option buttons to specify the save option to be used for the Switch. The options are:</p> <ul style="list-style-type: none"> <li>– Flash Save – Saves the configurations in the specified file name of Flash</li> <li>– Remote Save – Saves the configurations in the remote system which is specified by <b>Address Type</b> and <b>IP address</b></li> </ul>
<b>Transfer Mode</b>	<p>Select the transfer mechanism to save the Switch configurations in the remote system. The remote host machine should have a TFTP / SFTP capable Server running for this operation to be successful. The default option is <b>TFTP</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– TFTP – Saves the Switch configurations to the remote system through TFTP (Trivial File Transfer Protocol) mode.</li> <li>– SFTP – Saves the Switch configurations to the remote system through SFTP (SSH File Transfer Protocol) mode.</li> </ul>
<b>Address Type</b>	<p>Select the IP Address type of the remote system in which the Switch configurations are to be saved. The default option is <b>IPv4</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– IPv4 – Sets the Address type as IPv4.</li> <li>– IPv6 – Sets the Address type as IPv6.</li> </ul>
<b>IP Address</b>	<p>Enter the IP Address of the remote system in which the Switch configurations are to be saved.</p>

<b>SFTP User Name</b>	Enter the user name required for saving the Switch configurations to the remote system in SFTP mode. This field is a string of maximum size 20.
<b>SFTP Password</b>	Enter the password required for saving the Switch configurations on to the remote system in SFTP mode. This field is a string of maximum size 20. The specified SFTP username / password should have been configured in the SFTP server running the remote station, for the remote save operation through SFTP to be successful.
<b>File Name</b>	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 <b>RGS-PR9000-A.conf</b> . All configurations are saved in a single configuration file only.

### 4.1.5.2 Erase

This screen allows the user to reset the system startup configurations. The default system startup configuration takes effect after the system reboot. You can also Erase or delete the saved configuration from Flash or delete any file present in the Flash

Label	Description
Erase Option	<p>Click one of the option buttons to specify the erase or delete configuration or file. Options are:</p> <ul style="list-style-type: none"> <li>- Erase Nvram – Resets the System startup parameter values to default values. These default values take effect only after the system reboot.</li> <li>- 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.</li> <li>- Erase Flash File – Deletes any file from Flash specified in the</li> </ul>

	<b>File Name</b> field of this screen.
File Name	Enter the configuration file name to be erased. The default file name is <b>RGS-PR9000-A.conf</b> . Any other file which needs to be deleted from Flash can also be specified.

### 4.1.5.3 Remote Restore

This screen allows the user to load the previously saved configuration file from the remote system to the Flash

#### Load File

Browse to locate the file, then press Submit to begin the Loading Process.

Label	Description
<b>Browse</b>	To locate and down load the file.
<b>Submit</b>	To begin the Loading Process. The message "Loading the File may take few minutes." displays on the screen. Once the loading process begins, the message "! LOADING" displays on the screen.
<b>Reset</b>	To reset to default value for respective fields and discard all user inputs.

### 4.1.6 Firmware Upgrade

This screen allows the user to perform an image download operation on a switch stack or on a standalone switch to download a new image from a TFTP or SFTP from a remote location, to the switch and to overwrite or keep the existing image.

Label	Description
<b>Upgrade from</b>	Select the type of server from which the image is to be downloaded. The default option is <b>TFTP</b> . The list contains: <ul style="list-style-type: none"> <li>– TFTP – Sets the server type as TFTP (Trivial File Transfer Protocol) mode.</li> <li>– SFTP – Sets the server type as SFTP (SSH File Transfer Protocol) mode.</li> </ul>
<b>Address Type</b>	Select the IP Address type of the machine from which the image is to be downloaded. The default option is <b>IPv4</b> . The list contains: <ul style="list-style-type: none"> <li>– IPv4 – Sets the Address type as IPv4.</li> <li>– IPv6 – Sets the Address type as IPv6.</li> </ul>
<b>Server IP Address</b>	Enter the IP address of the machine from which the image is to be downloaded.
<b>SFTP User Name</b>	Enter the user name required for downloading the image from SFTP server. This field is a string with the maximum size 20.
<b>SFTP Password</b>	Enter the password required for downloading the image from SFTP server. This field is a string with the maximum size 20.
<b>File Name</b>	Enter the name of the image to be downloaded from the remote system.

### 4.1.7 Reboot

This screen allows the user to restart the switch/ target. Wait for 5 minutes before logging in after reboot.

## Rebooting the System

### 4.1.8 TACACS

TACACS (Terminal Access Controller Access-Control System) is a remote authentication protocol that is used to communicate with an authentication server commonly used in networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

TACACS uses a client-server mechanism. The TACACS server authenticates the TACACS client using information such as user name and password.

#### 4.1.8.1 Settings

This screen allows the user to configure the TACACS server configuration.

Server Address Type	<input type="button" value="IPv4"/>
IP Address	<input type="text"/>
Shared Secret	<input type="text"/>
Single Connection	<input type="button" value="No"/>
Server Port	<input type="text"/>
Server Timeout (secs)	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Address Type	IP Address	Shared secret	Single Connection	Server Port	Server Timeout
<input type="button" value="Apply"/> <input type="button" value="Delete"/>						

Label	Description
<b>Server Address Type</b>	Select the address type of the TACACS+ server. The default option is <b>IPV4</b> . The list contains: <ul style="list-style-type: none"> <li>- IPV4 – Sets the address type of the server as Internet Protocol Version 4.</li> <li>- IPV6 - Sets the address type of the server as Internet Protocol</li> </ul>

	Version 6.
<b>IP Address</b>	Enter the IPv4 or IPv6 address of the TACACS+ server. The TACACS+ client interacts with the server having this IP address.
<b>Shared Secret</b>	Enter the secret key shared between the client and server (IPv4 or IPv6) for encryption and decryption. The default value is <b>RGS-PR9000-A</b> .
<b>Single Connection</b>	Select whether single connect support is enabled/ disabled for the server. The default option is <b>No</b> . The list contains: <ul style="list-style-type: none"> <li>- Yes – Allows multiple sessions over a single TCP connection. Thus the authentication, authorization and accounting process are carried out in a single TCP connection.</li> <li>- 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.</li> </ul>
<b>Server Port</b>	Enter the server port number for TACACS protocol. This value ranges from 0 to 65535. The default value is <b>49</b> for IPv4 and <b>4949</b> for IPv6.
<b>Server Timeout (secs)</b>	Enter the timeout value within which the TACACS client expects a response from server. This value ranges from 1 to 255. The default value is <b>5</b> seconds. The TACACS client assumes that the primary server is down and gets connected with secondary server, after the expiry of this time.

### 4.1.8.2 Server Settings

This screen allows the user to set the TACACS server that should be used as primary server

Active Server Address Type  ▾

Active Server IP Address

Retransmit (secs)

Select	Active Server Address
<input checked="" type="radio"/>	<input style="width: 150px; height: 20px;" type="text"/>

Label	Description
Active Server Address Type	Select the address type of the active server. The list contains: <ul style="list-style-type: none"> <li>- IPV4 – Sets the address type of the active server as Internet Protocol Version 4.</li> <li>- IPV6 - Sets the address type of the active server as Internet Protocol Version 6.</li> </ul>
<b>Active Server IP Address</b>	Enter the IP address of the TACACS server that should be set as primary server. Maximum of 5 server's (IPv4 or IPv6) information can be configured for TACACS. This object indicates the active server among these 5 servers created using TACACS Server Configuration screen. The TACACS+ client interacts with the configured server IP address. When set to zero, TACACS disables the active server concept
<b>Retransmit (secs)</b>	Enter the number of times the TACACS client remote server searches the list of Maximum number of TACACS servers. This value ranges from 1 to 100 seconds. The default value is <b>2</b> seconds. 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.
<b>Select</b>	Select the Active Server IP address to be deleted.

### 4.1.9 SNTP

SNTP (Simple Network Time Protocol) is a simplified version of the NTP protocol. The NTP protocol is meant for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

#### 4.1.9.1 SNTP Scalars

This screen allows the user to configure the details of SNTP scalars.

Sntp Admin Status	Disabled <input type="button" value="v"/>
Client Version	Version 4 <input type="button" value="v"/>
Addressing Mode	Unicast <input type="button" value="v"/>
Time Display Format	Hours <input type="button" value="v"/>
TimeZone	<input type="text" value="+00:00"/>
DST StartTime	<input type="text"/>
DST EndTime	<input type="text"/>
	<input type="button" value="Apply"/> <input type="button" value="Refresh"/>

Label	Description
<b>Sntp Admin Status</b>	<p>Select the SNTP client module status. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the SNTP client module. On enabling, the server starts sending the request to the host for synchronization.</li> <li>– Disabled – Disables the SNTP client module.</li> </ul>
<b>Client Version</b>	<p>Select the SNTP client module version. The default option is <b>Version 4</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Version 1 - Sets the SNTP client version as Version 1</li> <li>– Version 2 - Sets the SNTP client version as Version 2</li> <li>– Version 3 – Sets the SNTP client version as Version 3</li> <li>– Version 4 – Sets the SNTP client version as Version 4</li> </ul>
<b>Addressing Mode</b>	<p>Select the SNTP client addressing mode. The default option is <b>Unicast</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> <li>– 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.</li> <li>– Multicast. - 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</li> </ul>
<b>Time Display Format</b>	<p>Select the time display format. The default option is <b>Hours</b>. The</p>



	<p>list contains:</p> <ul style="list-style-type: none"> <li>- Hours – Sets the time display as 24 hours format.</li> <li>- Am/Pm – Sets the time display as 12 hours AM/PM format.</li> </ul>
<b>TimeZone</b>	<p>Enter the system time zone with respect to UTC. The format is (+/-) HH:MM. Where:</p> <ul style="list-style-type: none"> <li>- +/- denotes the difference with the Greenwich Mean Time. + indicates forward time zone and - indicates backward time zone.</li> <li>- HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.</li> <li>- mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is +05:30.</li> </ul>
<b>DST StartTime</b>	<p>Enter the DST (Daylight Saving Time) start time. The format is weekofmonth-weekofday-month,HH:MM. Where:</p> <ul style="list-style-type: none"> <li>- weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.</li> <li>- weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.</li> <li>- 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</li> <li>- HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.</li> <li>- mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is First-Sun-Jan,23:45.</li> </ul>
<b>DST EndTime</b>	<p>Enter the DST end time. The valid format is [weekofmonth-weekofday-month, HH:MM]. The format is weekofmonth-weekofday- month,HH:MM. Where:</p> <ul style="list-style-type: none"> <li>- weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.</li> <li>- weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.</li> <li>- month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr,</li> </ul>

	<p>May, Jun, Jul, Aug, Sep, Oct, Nov, Dec</p> <ul style="list-style-type: none"> <li>- HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.</li> <li>- mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is First-Mon-Jan,23:45.</li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.1.9.2 SNTP Unicast

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

Forward Address Type

Unicast ServerIp Addr \*

Server Port

SNTP Version

Unicast Server Type

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

Label	Description
<b>Forward Address Type</b>	<p>Select the address type of the unicast server in the Unicast addressing mode. The list contains:</p> <ul style="list-style-type: none"> <li>- IPV4 – Sets the address type of the unicast server as Internet Protocol Version 4</li> <li>- IPV6 - Sets the address type of the unicast server as Internet Protocol Version 6</li> </ul>
<b>Unicast ServerIP Addr</b>	Enter the unicast IPv4/IPv6 server address in the Unicast addressing mode.
<b>Server Port</b>	Enter the SNTP port on which the server is UP. The value ranges between 123, 1025 to 65535. The default value is <b>123</b> .
<b>SNTP Version</b>	<p>Select the SNTP version supported by the server. The list contains:</p> <ul style="list-style-type: none"> <li>- Version 3 – Sets the SNTP version as version 3.</li> <li>- Version 4– Sets the SNTP version as version 4.</li> </ul>
<b>Unicast Server Type</b>	<p>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:</p>

	<ul style="list-style-type: none"> <li>- Primary – Sets the unicast server type as primary server</li> <li>- Secondary – Sets the unicast server type as secondary server</li> </ul>
<b>Select</b>	Click to select the server address for which the configuration need to be modified or deleted.
<b>Last Updated</b>	Specifies the local time when the system time was successful.
<b>Tx Request</b>	Specifies the number of SNTP requests sent in the Unicast addressing mode.

### 4.1.10 SSH

**SSH** is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary. SSH is typically used to log into a remote machine and execute commands.

This screen allows the user to configure SSH initial Settings.

The screenshot shows a configuration panel with the following elements:

- SSH Status:** A dropdown menu currently set to "Disable".
- SSH Version Compatibility:** A dropdown menu currently set to "V2".
- SSH CipherList:** A set of checkboxes for "DES-CBC", "3DES-CBC", "AES-CBC-128", "AES-CBC-256", "HMAC-MD5", and "HMAC-SHA1". "3DES-CBC" and "HMAC-SHA1" are checked.
- SSH MacList:** A text input field.
- Max Packet size:** A text input field containing the value "32768".
- Buttons:** An "Apply" button and a "Configure Trace Options" link.

Label	Description
<b>SSH Status</b>	<p>Select the status of the SSH module. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enable – Enables the SSH feature in the switch. SSH feature enables the user to log into a remote machine and execute commands.</li> <li>- Disable – Disables the SSH feature in the switch. This action disconnects the secure channel.</li> </ul>
<b>SSH Version Compatibility</b>	<p>Select the version of the SSH. The default option is <b>V2</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Both V1, V2 – Supports both SSH version-1 and version-2.</li> <li>- V2 – Supports only the SSH version-2.</li> </ul>
<b>SSH CipherList</b>	<p>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. The default option is <b>DES-CBC</b> in NON-FIPS mode and <b>3DES- CBC</b> in FIPS mode. The options are:</p>

	<ul style="list-style-type: none"> <li>– DES-CBC – This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key.</li> <li>– 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.</li> <li>– 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.</li> <li>– AES-CBC-256 - This is a 3 bit cipherlist. It is based on symmetric-key</li> <li>– algorithm that uses a 256-bit key with cipher-block chaining (CBC) as mode of operation.</li> </ul>
<b>SSH MacList</b>	<p>Select the <b>MAC</b> 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. The default option is <b>HMAC-SHA1</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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</li> <li>– HMAC-SHA1 – This is a similar version to MD5 and works on 512 bit blocks</li> </ul>
<b>Max Packet Size</b>	<p>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. This value ranges from 1 to 32768. The default value is <b>32768</b>.</p>

### 4.1.11 SSL

**SSL (Secured Socket Layers)** is used by the subscribers of HTTPS protocol. SSL offers secured data transfer. 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.

### 4.1.11.1 SSL Global Settings

This screen should be refreshed after making any changes.

HTTP Secure Server	<input type="button" value="Disable"/>
SSL Version	<input type="button" value="tls1"/>
HTTP Secure Cipher suite	<input type="checkbox"/> RSA-NULL-MD5 <span style="float:right"><input type="checkbox"/> RSA-NULL-SHA</span> <input checked="" type="checkbox"/> RSA-DES-SHA <span style="float:right"><input checked="" type="checkbox"/> RSA-3DES-SHA</span> <input type="checkbox"/> DH-RSA-DES-SHA <span style="float:right"><input type="checkbox"/> DH-RSA-3DES-SHA</span> <input checked="" type="checkbox"/> RSA-EXP1024-DES-SHA <input type="checkbox"/> RSA-WITH-AES-128-CBC-SHA <input type="checkbox"/> RSA-WITH-AES-256-CBC-SHA <input type="checkbox"/> DHE-RSA-WITH-AES-128-CBC-SHA <input type="checkbox"/> DHE-RSA-WITH-AES-256-CBC-SHA
<input type="button" value="Apply"/> <input type="button" value="Configure Trace Options"/>	

Label	Description
<b>HTTP Secure Server</b>	Select the status of the HTTP secure server. The default option is <b>Disable</b> . The list contains: <ul style="list-style-type: none"> <li>– Enable – Enables secure HTTP in the system. When the server status is enabled it establishes the secure layer in the network.</li> <li>– Disable – Disables secure HTTP in the system.</li> </ul>
<b>HTTP Secure Ciphersuite</b>	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. The default options are <b>RSA_3DES_SHA</b> , <b>RSA_DES_SHA</b> and <b>RSA_EXP1024_DES_SHA</b> . The options are: <ul style="list-style-type: none"> <li>– RSA-NULL-MD5 – cipher suites using RSA key exchange and offering no authentication combined with cipher suites using MD5.</li> <li>– RSA-NULL-SHA – cipher suites using RSA key exchange and offering no authentication combined with cipher suites using SHA1.</li> <li>– RSA-DES-SHA – cipher suites using RSA key exchange. and cipher suites using DES combined with cipher suites using SHA1</li> <li>– RSA-3DES-SHA – cipher suites using RSA key exchange. and cipher suites using triple DES combined with cipher suites using SHA1</li> </ul>

	<ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.1.11.2 SSL Digital Certificate

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.

**Generate Certificate Signing Request**

RSA Key Size

Common Name

**Enter Certificate Signed By Certification Authority**

Label	Description
<b>Generate Certificate signing Request</b>	Select to generate certificate based on the RSA key size and common name. The certificate is awarded to users who utilize the HTTPS protocol.
<b>RSA Key Size</b>	Select the desired Key size. The list contains: <ul style="list-style-type: none"> <li>– 512 – The key size is set as 512.</li> <li>– 1024 – The key size is set as 1024.</li> </ul>
<b>Common Name</b>	Enter the details of the user requesting for the Digital Certificate.
<b>Enter Certificate Signed by Certification Authority</b>	Select to enter Certificate Signed by Certification Authority. The user manually enters the details of the certificate.

## 4.1.12 HTTP

### 4.1.12.1 Web Session

This page allows you to specify how long a web session should stay active before it times out. The unit of the duration is seconds and the range is between 30 to 3600 seconds (1 hour)

#### Web Session TimeOut

Web Session TimeOut (30~3600) 600

## 4.1.13 SNMP

**SNMP (Simple Network Management Protocol)** 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.

### 4.1.13.1 Agent Community

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

Community Index	<input type="text"/>	*
Community Name	<input type="text"/>	*
Security Name	<input type="text"/>	*
Context Name	<input type="text"/>	
Transport Tag	<input type="text"/>	
Storage Type	<input type="text"/>	▼
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Community Index	Community Name	Security Name	Context Name	Transport Tag	Storage Type
<input type="radio"/>	NETMAN	NETMAN	none			NonVolatile ▼
<input checked="" type="radio"/>	public	public	none			NonVolatile ▼

Label	Description
<b>Community Index</b>	Enter the Index to the community table. The communities NETMAN and PUBLIC are created, once the RGS-PR9000-A is started to provide SNMP access to the RGS-PR9000-A.
<b>Community Name</b>	Enter the community name. The communities NETMAN and PUBLIC are created, once the RGS-PR9000-A is started to provide SNMP access to the RGS-PR9000-A.
<b>Security Name</b>	Enter the security name. The default value is <b>None</b> .
<b>Context Name</b>	Enter the context name. The default value is <b>Null</b> .
<b>Transport Tag</b>	Enter the transport tag. The default value is <b>Null</b> .
<b>Storage Type</b>	<p>Select the required Storage type for the community. The default option is <b>Non Volatile</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Volatile – Sets the storage type as temporary and erases the configuration setting on restarting the system.</li> <li>– 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.</li> </ul>

## Group

This screen allows the user to configure the SNMP Group Settings



Security Model

Security Name  \*

Group Name  \*

Storage Type

Select	Security Model	Security Name	Group Name	Storage Type
<input type="radio"/>	v1 <input type="button" value="v"/>	<input type="text" value="none"/>	<input type="text" value="iso"/>	NonVolatile <input type="button" value="v"/>
<input type="radio"/>	v2c <input type="button" value="v"/>	<input type="text" value="none"/>	<input type="text" value="iso"/>	NonVolatile <input type="button" value="v"/>
<input type="radio"/>	v3 <input type="button" value="v"/>	<input type="text" value="noAuthUser"/>	<input type="text" value="noAuthUser"/>	NonVolatile <input type="button" value="v"/>
<input type="radio"/>	v3 <input type="button" value="v"/>	<input type="text" value="templateMD5"/>	<input type="text" value="noAuthUser"/>	NonVolatile <input type="button" value="v"/>
<input checked="" type="radio"/>	v3 <input type="button" value="v"/>	<input type="text" value="templateSHA"/>	<input type="text" value="noAuthUser"/>	NonVolatile <input type="button" value="v"/>

Label	Description
<b>Security Model</b>	Select the version of the SNMP. The security model v1, v2c and v3 are created, once the RGS-PR9000-A is started. The list contains: <ul style="list-style-type: none"> <li>- v1 – Sets the SNMP version as Version 1.</li> <li>- v2c – Sets the SNMP version as Version 2.</li> <li>- v3 – Sets the SNMP version as Version 3.</li> </ul>
<b>Security Name</b>	Enter the security name of the group. The security name none, noAuthUser, templateMD5 and templateSHA are created, once the RGS-PR9000-A is started. This is a Read only field.
<b>Group Name</b>	Enter the name of the SNMP group. The SNMP groups iso and initial are created, once the RGS-PR9000-A is started.
<b>Storage Type</b>	Select the required Storage type for the group entry. The default option is <b>NonVolatile</b> The list contains: <ul style="list-style-type: none"> <li>- Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> </ul>

	<ul style="list-style-type: none"> <li>– Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Group Access**

Group Name  \*

Security Model v1 ▾

Security Level NoAuthentication ▾

Read View

Write View

Notify View

Storage Type NonVolatile ▾

Add Reset

Select	Group Name	Context Prefix	Security Model	Security Level	Read View	Write View	Notify View	Storage Type
<input type="radio"/>	iso		v1 ▾	NoAuthentication ▾	iso	iso	iso	NonVolatile ▾
<input type="radio"/>	iso		v2c ▾	NoAuthentication ▾	iso	iso	iso	NonVolatile ▾
<input type="radio"/>	noAuthUser		v3 ▾	NoAuthentication ▾	restricted	restricted	restricted	NonVolatile ▾
<input type="radio"/>	noAuthUser		v3 ▾	Authentication ▾	iso	iso	iso	NonVolatile ▾
<input checked="" type="radio"/>	noAuthUser		v3 ▾	Private ▾	iso	iso	iso	NonVolatile ▾

Apply Delete

Label	Description
<b>Group Name</b>	Enter the name of the group. The maximum size is 32.
<b>Security Model</b>	Select the version of the SNMP. The list options are: <ul style="list-style-type: none"> <li>– v1 – Sets the SNMP version as Version 1.</li> <li>– v2c – Sets the SNMP version as Version 2.</li> <li>– v3 – Sets the SNMP version as Version 3.</li> </ul>
<b>Security Level</b>	<ul style="list-style-type: none"> <li>– Select the version of the SNMP. The list contains:</li> <li>– NoAuthentication – Sets no authentication</li> <li>– Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.</li> <li>– Private – Sets both authentication and privacy.</li> </ul>
<b>Read View</b>	Enter the read view identifier from which the user can read the data. The maximum size is 32.
<b>Write View</b>	Enter the write view identifier from which the user has both the read and write access. The maximum size is 32.
<b>Notify View</b>	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.
<b>Storage Type</b>	<p>Select the required Storage type for the group access entry.</p> <p>The list contains:</p> <ul style="list-style-type: none"> <li>- Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>- Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>

**View**

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

Select	View Name	SubTree	Mask	View Type	Storage Type
<input type="radio"/>	iso	1	1	Included	NonVolatile
<input checked="" type="radio"/>	restricted	1	1	Included	NonVolatile

Label	Description
<b>View Name</b>	Enter the View Name for which the view details are to be configured. The default option is ISO and restricted. The View name iso and restricted are created, once the RGS-PR9000-A is started.
<b>SubTree</b>	Enter the Sub Tree value for the particular view. The default value is 1.
<b>Mask</b>	Enter the Mask value for the particular view. The default value is 1.
<b>View Type</b>	Select the View Type. The default option is <b>Included</b> The list

	<p>contains:</p> <ul style="list-style-type: none"> <li>- Included – Allows access to the subtree.</li> <li>- Excluded – Denies access to the subtree.</li> </ul>
<b>Storage Type</b>	<p>Select the required Storage type for the view tree entry. The default option is <b>NonVolatile</b> The list contains:</p> <ul style="list-style-type: none"> <li>- Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>- Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>

**User**

This screen allows the user to create a user and configure the security parameters for that user.

Engine ID  \*

User Name  \*

Authentication Protocol  ▾

Authentication Key

Privacy Protocol  ▾

Privacy Key

Storage Type  ▾

Select	Engine Id	User Name	Authentication Protocol	Private Protocol	Storage Type
<input type="radio"/>	80:00:08:1c:04:46:53	noAuthUser	<input type="button" value="No Authentication"/> ▾	<input type="button" value="No Privacy"/> ▾	<input type="button" value="NonVolatile"/> ▾
<input type="radio"/>	80:00:08:1c:04:46:53	templateMD5	<input type="button" value="HMAC-MD5"/> ▾	<input type="button" value="No Privacy"/> ▾	<input type="button" value="NonVolatile"/> ▾
<input checked="" type="radio"/>	80:00:08:1c:04:46:53	templateSHA	<input type="button" value="HMAC-SHA"/> ▾	<input type="button" value="DES"/> ▾	<input type="button" value="NonVolatile"/> ▾

Label	Description
<b>Engine ID</b>	Enter the global SNMP engine id. The value is an octet string of maximum size 5 to 32 octets. E.g. 80:00:08:1c:04:46:53.
<b>User Name</b>	Enter the user name which is the User-based Security Model dependent security ID.
<b>Authentication Protocol</b>	Select the type of authentication protocol used for authentication. The default option is <b>No Authentication</b> . The

	<p>list contains:</p> <ul style="list-style-type: none"> <li>– No Authentication – Sets the authentication status as no authentication required.</li> <li>– HMAC-MD5 – Sets the Message Digest 5 based authentication.</li> <li>– HMAC-SHA – Sets the Security Hash Algorithm based authentication.</li> </ul>
<b>Authentication Key</b>	<p>Enter the secret authentication key used for messages sent on behalf of this user to/from the SNMP. This value is a string of maximum size 40.</p>
<b>Privacy Protocol</b>	<p>Select the type of protocol to be is used in this case. The default option is <b>No Privacy</b> The list contains:</p> <ul style="list-style-type: none"> <li>– No Privacy – Sets no privacy</li> <li>– DES – Sets the privacy protocol as Data Encryption Standard. This protocol provides an algorithm to encrypt PPP encapsulated packets.</li> <li>– AES – Sets the privacy protocol as Advanced Encryption Standard (AES)</li> </ul>
<b>Privacy Key</b>	<p>Enter the privacy key. The messages sent on behalf of a user to/from the SNMP, can be protected from disclosure. This value is a string of maximum size 32.</p>
<b>Storage Key</b>	<p>Select the required Storage type for the security settings entry. The list contains:</p> <ul style="list-style-type: none"> <li>– Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>– Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The Saved configuration can be viewed on restarting the system</li> </ul>

## Trap Manager

This screen allows the user to configure set of management targets to receive notifications.

Notify Name  \*  
 Notify Tag  \*  
 Notify Type  ▾  
 Storage Type  ▾

Select	Notify Name	Notify Tag	Notify Type	Storage Type
<input type="radio"/>	<input type="text" value="iss"/>	<input type="text" value="iss"/>	<input type="text" value="Trap"/> ▾	<input type="text" value="NonVolatile"/> ▾
<input checked="" type="radio"/>	<input type="text" value="iss1"/>	<input type="text" value="iss1"/>	<input type="text" value="Trap"/> ▾	<input type="text" value="NonVolatile"/> ▾

Label	Description
<b>Notify Name</b>	Enter a unique identifier associated with the entry. The maximum size is 32.
<b>Notify Tag</b>	Enter the notification tag used to select entries in the Target Address Table. The maximum size is 32.
<b>Notify Type</b>	Select the notification type. The list contains: <ul style="list-style-type: none"> <li>– 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.</li> <li>– Inform – Allows routers / switches to send inform requests to SNMP managers.</li> </ul>
<b>Storage Type</b>	Select the required Storage type for the trap settings entry. The list contains: <ul style="list-style-type: none"> <li>– Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>– Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>

**Target Address**

This screen allows the user to configure the SNMP Target Address Settings.

Target Name	<input type="text"/>	*
Target IP Address	<input type="text"/>	*
Port	<input type="text" value="162"/>	*
Transport Tag	<input type="text"/>	
Param	<input type="text"/>	*
Storage Type	<input type="text" value="Volatile"/>	▼
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Target Name	Target IP Address	Port	Transport Tag	Param	Storage Type
--------	-------------	-------------------	------	---------------	-------	--------------

Label	Description
<b>Target Name</b>	Enter a unique identifier of the Target. The maximum size is 32.
<b>Target IP Address</b>	Enter a target address to which the generated SNMP notifications are sent.
<b>Port</b>	Enter the port number through which the generated SNMP notifications are sent to the target address.
<b>Transport Tag</b>	Enter the tag identifier that is used to select the target address for the SNMP notifications.
<b>Param</b>	Enter SNMP parameters to be used when generating messages to be sent to transport address. The maximum size is 32.
<b>Storage Type</b>	Select the required Storage type for the target address entry. The list contains: <ul style="list-style-type: none"> <li>– Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>– Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>

**Target Parameter**

This screen allows the user to configure the SNMP target information to be used in the generation of SNMP messages.

Parameter Name  \*

MP Model

Security Model

Security Name  \*

Security Level

Storage Type

Select	Parameter Name	MP Model	Security Model	Security Name	Security Level	Storage Type
<input type="radio"/>	internet	v2c	v2c	none	NoAuthentication	NonVolatile
<input checked="" type="radio"/>	test1	v2c	v1	none	NoAuthentication	NonVolatile

Label	Description
<b>Parameter Name</b>	Enter a unique identifier of the parameter. The maximum size is 32. The default option is <b>Internet</b>
<b>MP Model</b>	Select the MP model of the SNMP. The default option is v2c. The list contains: <ul style="list-style-type: none"> <li>- v1 – Sets the MP model as Version 1.</li> <li>- v2c – Sets MP model as Version 2.</li> <li>- v3 – Sets the MP model as Version 3.</li> </ul>
<b>Security Model</b>	Select the version of the SNMP. The default option is v2c. The list contains: <ul style="list-style-type: none"> <li>- v1 – Sets the security model as Version 1</li> <li>- v2c – Sets the security model as Version 2.</li> <li>- v3 – Sets the security model as Version 3.</li> </ul>
<b>Security Name</b>	Enter the security name to generate SNMP messages. The default option is <b>None</b> The maximum size is 32.
<b>Security Level</b>	Select the level of security to be used when generating SNMP messages. The default option is <b>NoAuthentication</b> The list contains: <ul style="list-style-type: none"> <li>- NoAuthentication – Sets no authentication.</li> </ul>



	<ul style="list-style-type: none"> <li>- Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.</li> <li>- Private - Enables both authentication and privacy.</li> </ul>
<b>Storage Type</b>	<p>Select the required Storage type for the target parameter entry. The default option is <b>NonVolatile</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Volatile – Indicates that the storage type is temporary. Erases the configuration setting on restarting the system.</li> <li>- Non Volatile – Indicates that the storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.</li> </ul>

**Filter Conf**

This screen allows the user to configure the notification filters used to determine whether the management target should receive a 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

**Select Filter Profile Name SubTree Mask Filter Type Storage Type**

Label	Description
<b>Profile Name</b>	Enter the filter profile name that should be used during generating notifications. This value is a string of maximum size of 32.

<b>SubTree</b>	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.
<b>Mask</b>	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.
<b>Filter Type</b>	Select the type of filter to be applied for the filter entry. The default option is <b>included</b> . The list contains: <ul style="list-style-type: none"> <li>- Included – Indicates that the family of filter subtrees is defined using MIB subtree and bit mask is included in a filter.</li> <li>- Excluded - Indicates that the family of filter subtrees is defined using MIB subtree and bit mask is excluded from a filter.</li> </ul>
<b>Storage Type</b>	Select the storage type for the filter entry. The default option is <b>NonVolatile</b> . The list contains: <ul style="list-style-type: none"> <li>- Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.</li> <li>- NonVolatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system</li> </ul>

### 4.1.13.2 Proxy

#### Proxy

SNMP Proxy is used as a mediator between a SNMP manager and a SNMP agent. It gets the request from the SNMP agent and forwards it to the SNMP manager.

Proxy Name	<input type="text"/> *
Proxy Type	Read <input type="button" value="v"/>
Proxy Context Engine ID	<input type="text"/> *
Proxy Context Name	<input type="text"/>
Proxy TargetParamIn	<input type="text"/> *
Proxy SingleTargetOut	<input type="text"/> *
Proxy MultipleTargetOut	<input type="text"/> *
Proxy Storage Type	NonVolatile <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Proxy Name	Proxy Type	Proxy ContextEngineID	Proxy ContextName	Proxy TargetParamIn	Proxy SingleTargetOut	Proxy MultipleTargetOut	Proxy Storage Type
<input type="button" value="Apply"/> <input type="button" value="Delete"/>								

Label	Description
<b>Proxy Name</b>	Enter the unique proxy name that identifies an entry in the proxy table. This value is a string of maximum size of 32.
<b>Proxy Type</b>	Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains: <ul style="list-style-type: none"> <li>– Read – Read messages are forwarded to get the request from the manager.</li> <li>– Write – Write messages are forwarded to set configurations.</li> <li>– Inform – Notification messages are forwarded to the agent.</li> <li>– Trap – SNMP trap messages are forwarded to the agent</li> </ul>
<b>Proxy Context Engine ID</b>	Enter the context engine ID of the agent with whom the manager communicates through the proxy.
<b>Proxy Context Name</b>	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.
<b>Proxy TargetParamIn</b>	Enter the SNMP version that the manager sends as request to the proxy
<b>Proxy Single TargetOut</b>	Enter the SNMP version that the proxy uses to communicate with the agent.
<b>Proxy Multiple TargetOut</b>	Enter the SNMP version that the proxy uses to communicate with multiple agents.
<b>Proxy Storage Type</b>	Select the type of storage for the proxy. The list contains: <ul style="list-style-type: none"> <li>– Volatile – The configuration is lost after the switch is reboot, even if the entry is saved.</li> <li>– Non-Volatile – The configuration is available even after the switch is reboot, if the entry is saved.</li> </ul>

## MIB

This screen allows the user to configure SNMP MIB Proxy settings.

Prop Proxy Name	<input type="text"/> *
Prop Proxy Type	Read ▾
Prop MibID	<input type="text"/> *
Prop Proxy TargetParamIn	<input type="text"/> *
Prop Proxy SingleTargetOut	<input type="text"/> *
Prop Proxy MultipleTargetOut	<input type="text"/> *
Prop Storage Type	NonVolatile ▾
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Prop Proxy Name	Prop Proxy Type	Prop MibID	Prop Proxy TargetParamIn	Prop Proxy SingleTargetOut	Prop Proxy MultipleTargetOut	Prop Storage Type
<input type="button" value="Apply"/> <input type="button" value="Delete"/>							

Label	Description
<b>Prop Proxy Name</b>	Enter the unique proxy name that identifies an entry in the proxy table. This value is a string of maximum size 32.
<b>Prop Proxy Type</b>	Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains: <ul style="list-style-type: none"> <li>– Read – Read messages are forwarded to get the request from the manager.</li> <li>– Write – Write messages are forwarded to set configurations.</li> <li>– Inform – Notification messages are forwarded to the agent</li> <li>– Trap – SNMP trap messages are forwarded to the agent</li> </ul>
<b>Prop MibID</b>	Enter the proprietary MIB ID which is used as the root object ID.
<b>Prop Proxy TargetParamIn</b>	Enter the SNMP version that the manager sends as request to the proxy.
<b>Prop Single TargetOut</b>	Enter the SNMP version that the proxy uses to communicate with the agent.
<b>Prop Multiple TargetOut</b>	Enter the SNMP version that the proxy uses to communicate with multiple agents.
<b>Prop Storage Type</b>	Select the type of storage for the proxy. The list contains: <ul style="list-style-type: none"> <li>– Volatile – The configuration is lost after the switch is reboot, even if the entry is saved.</li> <li>– Non-Volatile – The configuration is available even after the switch is reboot, if the entry is saved.</li> </ul>

### 4.1.13.3 SCALARS

This screen allows the user to configure SNMP scalar parameters which are independent of each other

snmpEnableAuthenTraps	Disabled ▾
snmpListenTcpTrapPort	162
snmpTrapOverTcpStatus	Disabled ▾
snmpOverTcpStatus	Disabled ▾
snmpProxyListenTrapPort	162
snmpListenTrapPort	162
snmpListenTcpPort	161

Label	Description
<b>snmpEnableAuthenTraps</b>	Select the status of the authentication failure traps. The list contains: <ul style="list-style-type: none"> <li>– Enabled – Enables the generation of authentication failure traps.</li> <li>– Disabled – Disables the generation of authentication failure traps.</li> </ul>
<b>snmpListenTcpTrapPort</b>	Enter the port number on which SNMP trap message are sent to the manager over TCP. The default value is <b>162</b> .
<b>snmpTrapOverTcpStatus</b>	Select the status of sending SNMP trap messages over TCP. The list contains: <ul style="list-style-type: none"> <li>– Enables – Allows sending of SNMP trap messages over TCP.</li> <li>– Disables – Blocks sending of SNMP trap messages over TCP.</li> </ul>
<b>snmpOverTcpStatus</b>	Select the status of sending SNMP messages over TCP. The list contains: <ul style="list-style-type: none"> <li>– Enables – Allows sending of SNMP messages over TCP. All SNMP messages are send over TCP instead of UDP.</li> <li>– Disables - Blocks sending of SNMP messages over TCP.</li> </ul>

<b>snmpProxyListenTrapPort</b>	Enter the port number on which proxy listens for trap and inform messages from the agent. The default value is <b>162</b> .
<b>snmpListenTrapPort</b>	Enter the port number on which SNMP trap messages are sent to the manager. The default value is <b>162</b> .
<b>snmpListenTcpPort</b>	Enter the port number on which SNMP trap messages are sent to the manager over TCP. The default value is <b>161</b> .

### 4.1.13.4 Agentx

SNMP agentx is a standardized framework for extensible SNMP agents. It defines processing entities called master agents and subagents, a protocol (AgentX) used to communicate between master agents and sub agents, and the elements of procedure by which the extensible agent processes SNMP protocol messages.

Label	Description
<b>Transport Domain</b>	Select the transport domain to be used as TCP. The subagent transport domain must be in sync with the master agents transport domain." The default option is TCP.
<b>IP Address Type</b>	Specifies the IP address type. The default option is <b>IPV4</b> . The list contains: <ul style="list-style-type: none"> <li>- IPv4 – Sets the IP Address type as version 4</li> <li>- IPv6 – Sets the IP Address type as version 6</li> </ul>
<b>Master IP Address</b>	Enter the master agent IP address.
<b>Master PortNo</b>	Enter the master agent port number. The value ranges from 0 to 65535. The default value is <b>705</b> .

## 4.1.14 Syslog

Syslog is a standard for logging program messages. It separates the software that generates and stores messages from the software that reports and analyzes them.

Syslog is a protocol used to capture log information from the devices on a network. This protocol allows a machine to send event notification messages across IP networks to event message collectors, also known as Syslog servers. This protocol is simply designed to transport the event messages.

### 4.1.14.1 Scalars Conf

This screen allows the user to configure the Scalars Syslog settings

Syslog Role	Device	
SyslogFile Status	Disabled	
SyslogMail Status	Disabled	
SMTP Sender Mail Id	<input type="text"/>	<input type="button" value="Reset"/>
Syslog Profile	Raw	
Syslog FileName One	<input type="text"/>	
Syslog FileName Two	<input type="text"/>	
Syslog FileName Three	<input type="text"/>	
Syslog Snmp Trap	Enabled	
Syslog Relay Port	514	
Syslog Relay Transport Type	UDP	
Syslog Authentication Type	No Authentication	

Label	Description
<b>Syslog Role</b>	Select the syslog role. The default option is <b>Device</b> . The list contains: <ul style="list-style-type: none"> <li>– Device - Generates and forwards the syslog message.</li> <li>– 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.</li> </ul>
<b>SyslogFile Status</b>	Select the syslog file storage to log the status in the local storage path. The default option is <b>Disabled</b> . This list contains are:

	<ul style="list-style-type: none"> <li>– Enabled – Sets the syslog local storage as enabled.</li> <li>– Disabled – Sets the syslog local storage as disabled.</li> </ul>
<b>SyslogMail Status</b>	<p>Select the syslog mail storage. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the syslog mail storage.</li> <li>– Disabled – Disables the syslog mail storage.</li> </ul>
<b>SMTP Sender Mail ID</b>	<p>Enter the sender mail ID to which email alerts should be sent using SMTP (Simple Mail Transfer Protocol). The user can customize RGS-PR9000-A to add support for specific event for which email alerts should be sent. This maximum length is 100. The default value is <a href="mailto:support@RGS-PR9000-A.com">support@RGS-PR9000-A.com</a>.</p>
<b>Syslog Profile</b>	<p>Select the syslog profile for beep. The default option is <b>Raw</b>. The list contains.</p> <ul style="list-style-type: none"> <li>– Raw - Raw syslog profile.</li> <li>– Cooked - Cooked syslog profile.</li> </ul>
<b>Syslog FileName One</b>	<p>Enter the first file where the syslog can store the messages locally. This is a string of maximum size 32.</p>
<b>Syslog FileName Two</b>	<p>Enter the second file where the syslog can store the messages locally. This is a string of maximum size 32.</p>
<b>Syslog FileName Three</b>	<p>Enter the third file where the syslog can store the messages locally. This is a string of maximum size 32.</p>
<b>Syslog Snmp Trap</b>	<p>Select the Syslog SNMP server up or down traps to be generated when connectivity fails. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Generates trap whenever connectivity to the external server collecting logs is lost.</li> <li>– Disabled – Does not generate Syslog SNMP server up or down traps.</li> </ul>
<b>Syslog Relay Port</b>	<p>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 from 0 to 65535. The default value is <b>514</b>.</p>
<b>Syslog Relay Transport Type</b>	<p>Select the transport protocol to be used by the relay for receiving syslog messages. The default option is <b>UDP</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– UDP – Receives syslog messages through UDP socket.</li> </ul>



	<ul style="list-style-type: none"> <li>- TCP – Receives syslog messages through TCP socket.</li> </ul>
<p><b>Syslog Authentication Type</b></p>	<p>Select the authentication mode to be used for sending E-mail alerts to the mail server configured. The list contains:</p> <ul style="list-style-type: none"> <li>- No Authentication – E-mail alerts are sent without authentication.</li> <li>- AUTH LOGIN – E-mail alerts are sent after authenticating the user. The authentication is done by sending the BASE64 encoded username and password</li> <li>- 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</li> <li>- 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.</li> <li>- 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 value.</li> </ul>

#### 4.1.14.2 Logging

This screen allows you to modify the settings for logging.

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

Label	Description
<b>Number of Log Buffers</b>	Enter the number of logs and email alert messages that can be stored in a local buffer for the syslog messages. This value ranges from 1 to 200. The default value is <b>50</b> .
<b>Console Log</b>	Select whether the logs and email alert messages should be displayed in the console while being sent to the server. The default option is <b>Enable</b> . The list contains:

	<ul style="list-style-type: none"> <li>- Enable – Sends the log and email alert messages to the server and it will be displayed in the console also.</li> <li>- Disable – Sends the log and email alert messages to the server alone and it will not be displayed in the console.</li> </ul>
<b>Logging Facility</b>	<p>Select the facility level used for storing the logs and email alert messages. The facility refers to different general classification of the messages. The default option is <b>Local0</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Local0 – Reserved local use facility</li> <li>- Local1 – Reserved local use facility</li> <li>- Local2 – Reserved local use facility</li> <li>- Local3 – Reserved local use facility</li> <li>- Local4 – Reserved local use facility</li> <li>- Local5 – Reserved local use facility</li> <li>- Local6 – Reserved local use facility</li> <li>- Local7 – Reserved local use facility</li> </ul>
<b>Logging Severity</b>	<p>Select the severity level for the syslog messages to be logged. The list contains:</p> <ul style="list-style-type: none"> <li>- Emergency – Log messages that represent panic condition.</li> <li>- Alert – Log messages that require immediate attention.</li> <li>- Critical – Log messages that represent critical error.</li> <li>- Error – Log error messages.</li> <li>- Warning – Log warning messages.</li> <li>- Notice – Log messages that represent significant condition but not errors.</li> <li>- Info – Log informational messages.</li> <li>- Debug – Log debug messages</li> </ul>
<b>Syslog Logging</b>	<p>Select whether the syslog service is to be enabled. The default option is <b>Enable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enable – Enables the syslog feature in the system. The syslog messages and email alert messages are logged in the system.</li> <li>- Disable – Disables the syslog feature in the system. The</li> </ul>

	syslog messages and email alert messages are not logged in the system.
<b>Logs</b>	Select the Clear facility to delete the logs buffered in the system. By default, the check box is not selected.

### 4.1.14.3 Mail Table

This screen allows the user to configure the BSD Syslog Mail Table settings.

Note : For Syslog Mail Server, [BSD Syslog Settings](#) Syslog Mail should be enabled and SMTP Sender Mail ID should be configured.

Label	Description
<b>Mail Priority</b>	Enter the priority for the mail-server configuration. This value ranges from 0 to 191.
<b>Server Address Type</b>	Select the mail server address type. The list contains: <ul style="list-style-type: none"> <li>– IPV4 – Sets the Server Address Type as Internet Protocol Version 4</li> <li>– IPV6 – Sets the Server Address Type as Internet Protocol Version 6</li> </ul>
<b>Server Address</b>	Enter the mail server IP.
<b>Mail ID</b>	Enter the receiver mail ID.
<b>User Name</b>	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. This is a string of maximum size 64.
<b>Password</b>	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. This is a string of maximum size 64.

### 4.1.14.4 Fwd Table

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

Forward Priority	<input type="text"/> *
Forward Address Type	IPV4
Server Ip Address	<input type="text"/> *
Forward Port	514
Forward Transition Type	SYSLOG_UDP
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

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

Label	Description
<b>Forward Priority</b>	Enter the priority which is to be forwarded to the desired server. This value ranges from 0 to 191.
<b>Forward Address Type</b>	Select the address type of the server. The list contains: <ul style="list-style-type: none"> <li>– IPV4 – Sets the forward address type as Internet Protocol Version 4</li> <li>– IPV6 – Sets the forward address type as Internet Protocol Version 6.</li> </ul>
<b>Server IP Address</b>	Enter the server IP to which the syslog messages is to be forwarded.
<b>Forward Port</b>	Enter the port through which it can send the syslog message. This value ranges from 0 to 65535. The default value is <b>514</b> .
<b>Forward Transition Type</b>	Select the transport type using which it can send syslog message. The default option is <b>SYSLOG_UDP</b> . The list contains: <ul style="list-style-type: none"> <li>– SYSLOG_UDP – Sets the forward transition type as SYSLOG_UDP</li> <li>– SYSLOG_TCP – Sets the forward transition type as SYSLOG_TCP</li> <li>– SYSLOG_BEEP – Sets the forward transition type as SYSLOG_BEEP</li> </ul>

### 4.1.14.5 SysLog

This page allows you to specify the system log messages you want to view by severity level. You can also choose specific syslog IDs based on your requirement and the number of entries you want to see per page.

Auto-refresh  Refresh |<< << >> >>|

Level **ALERT** ▼

The total number of entries is 9 for the given level.

Start from ID  with  entries per page.

ID	Prior	Date	Time	Host	Message
0	ALERT	Feb 17	15:50:35	ISS	I2C Power_1: ON
1	ALERT	Feb 17	15:50:35	ISS	I2C Power_2: No Module
2	ALERT	Jan 01	00:00:23	ISS	CLI Attempt to login as admin via console Succeeded
3	ALERT	Jan 01	00:05:27	ISS	WEB WEBNM: Successfully logged as User - admin
4	ALERT	Jan 01	00:51:52	ISS	WEB WEBNM: Session logout Idle timer expired for web
5	ALERT	Jan 01	00:51:52	ISS	WEB WEBNM: Session logout Idle timer expired for web
6	ALERT	Jan 01	00:52:03	ISS	WEB WEBNM: Successfully logged as User - admin
7	ALERT	Jan 02	17:07:19	ISS	WEB WEBNM: Successfully logged as User - admin
8	ALERT	Jan 07	16:56:43	ISS	WEB WEBNM: Successfully logged as User - admin

Label	Description
<b>Auto-refresh</b>	Check the box to enable auto-refresh or click refresh button to update the information manually.
<b>Level</b>	<p>You can select from the following levels.</p> <p>emerg: system unstable</p> <p>alert: immediate action needed</p> <p>critical: critical conditions</p> <p>error: error conditions</p> <p>warn: warning conditions</p> <p>notice: normal but significant condition</p> <p>info: informational messages only</p> <p>debugging: debugging messages</p>

### 4.1.15 DDM

ORing's optical Ethernet SFP and BIDI-SFP modules support DDM (digital diagnostics monitoring) technology (as specified by the industry-standard SFF-8472). This technology allows the user to monitor real-time parameters of the SFP or BIDI-SFP modules, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

### 4.1.15.1 SFP Monitor

#### SFP Monitor

Auto-refresh

Enable

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (mW)	(dBm)	RX Power (mW)	(dBm)
1	0	0.000	0.000	0	0	0	0
2	0	0.000	0.000	0	0	0	0
3	0	0.000	0.000	0	0	0	0
4	0	0.000	0.000	0	0	0	0
5	0	0.000	0.000	0	0	0	0
6	0	0.000	0.000	0	0	0	0
7	0	0.000	0.000	0	0	0	0
8	0	0.000	0.000	0	0	0	0
9	0	0.000	0.000	0	0	0	0
10	0	0.000	0.000	0	0	0	0
11	0	0.000	0.000	0	0	0	0
12	0	0.000	0.000	0	0	0	0
13	0	0.000	0.000	0	0	0	0
14	0	0.000	0.000	0	0	0	0
15	0	0.000	0.000	0	0	0	0
16	0	0.000	0.000	0	0	0	0
17	N/A	N/A	N/A	N/A	N/A	N/A	N/A
18	N/A	N/A	N/A	N/A	N/A	N/A	N/A
19	N/A	N/A	N/A	N/A	N/A	N/A	N/A
20	N/A	N/A	N/A	N/A	N/A	N/A	N/A
21	N/A	N/A	N/A	N/A	N/A	N/A	N/A
22	N/A	N/A	N/A	N/A	N/A	N/A	N/A
23	N/A	N/A	N/A	N/A	N/A	N/A	N/A
24	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

°C(0~100)

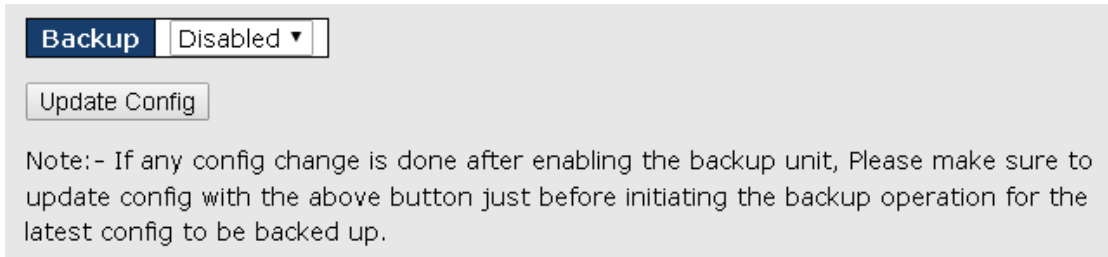
Event Alarm :

Syslog

### 4.1.16 Backup Unit

#### 4.1.16.1 Backup Unit Config

This page enables you to enable or disable backup function. This function allows you to quickly backup/restore configuration.



**Backup** | Disabled ▾

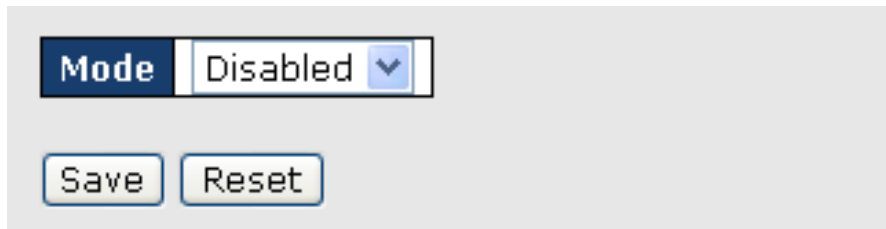
Update Config

Note:- If any config change is done after enabling the backup unit, Please make sure to update config with the above button just before initiating the backup operation for the latest config to be backed up.

## 4.1.17 ModBus

This page enables you to disable or enable ModBus function.

### 4.1.17.1 ModBus Config



**Mode** | Disabled ▾

Save Reset

Label	Description
<b>Mode</b>	Choose to enable or disable Modbus function

## 4.2 Layer 2 Management

This link allows you to configure various Layer 2 features, such as configure port settings, the mirroring feature, the traffic class associated with each priority class, and VLAN settings

### 4.2.1 Port Manager

Port Manager helps to configure parameters of the ports such as MTU, IP specific configuration, and WAN interface specific configuration such as maximum burst size.

#### 4.2.1.1 Basic Settings

This screen 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.

Select	Port	Link Status	Admin State	Bridge Port Type	Default User Priority	SwitchPort Mode	MTU	Link Up/Down Trap	Port Type	Mac Address
<input type="radio"/>	Gi0/1	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:01
<input type="radio"/>	Gi0/2	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:02
<input type="radio"/>	Gi0/3	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:03
<input type="radio"/>	Gi0/4	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:04
<input type="radio"/>	Gi0/5	▲	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:05
<input type="radio"/>	Gi0/6	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:06
<input type="radio"/>	Gi0/7	▼	Up	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:1e:94:00:00:07

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Link Status</b>	<p>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 representation are:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> </ul>
<b>Admin State</b>	<p>Select the desired state of the port. The default option is <b>Up</b>. The state changes to <b>Up</b> or <b>Down</b> state, as a result of either explicit management action or per configuration information retained by the managed system. The list contains:</p> <ul style="list-style-type: none"> <li>– Up – Allows the port to transmit/receive the traffic. The port cannot transmit/receive the traffic, if the Link is not working.</li> <li>– Down – Blocks the port from transmitting/receiving the traffic. The port will not transmit/receive the traffic, even if the Link is working.</li> <li>– LoopBack – Sets the desired admin state as loopback</li> </ul>
<b>Bridge Port Type</b>	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 other than **Customer Bridge** and **Provider Bridge** in the **Bridge Mode selection** screen. The default option is **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

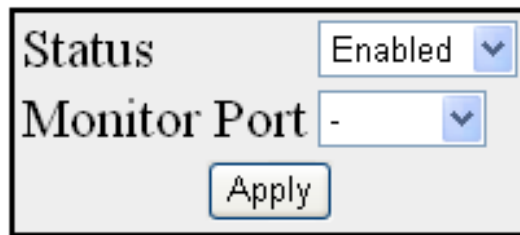
	<p>assigned using other proprietary SVLAN classification tables, where CVLAN is not the index of the table.</p> <ul style="list-style-type: none"> <li>– PropProviderNwPort – Denotes that the port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its ethertype. The packets received with standard Q tag are considered as S-Tagged packets.</li> <li>– CustomerBridgePort – Denotes the port to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs.</li> <li>– None – Denotes that the bridge port type is not set for the port. This is currently not supported.</li> </ul>
<p><b>Default User Priority</b></p>	<p>Select the default ingress user priority for the port. The default value is <b>0</b>. The list contains values from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority.</p>
<p><b>Switch Port Mode</b></p>	<p>Select the mode of operation for the switch port. The mode defines the way of handling of traffic for VLANs. The default option is <b>Hybrid</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> <li>– Hybrid – Configures the port as hybrid port that accepts and sends both tagged and untagged frames.</li> <li>– 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.</li> <li>– If a host port is a member port of an isolated VLAN, traffic</li> </ul>

	<p>from the host port is sent only to the promiscuous port of the private VLAN and the trunk port.</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– Promiscuous – Enables <b>Ingress Filtering</b> 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.</li> </ul>
<b>MTU</b>	<p>Enter the maximum transmission unit frame size 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. This value ranges from 46 to 9216 bytes. The default value is assigned for MTU based on the type/protocol of the interface (as tabulated below), if the MTU value is not configured during creation of interface.</p>
<b>Link Up/Down Trap</b>	<p>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. The default option is <b>Enabled</b> for interfaces that do not operate on top of any other interface. Otherwise, the trap is set as <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the generation of linkUp/linkDown traps for the interface.</li> <li>– Disabled – Disables the generation of linkUp/linkDown traps for the interface.</li> </ul>
<b>Port Type</b>	<p>Select the port type to operate the port as an L2 port or as an L3 port. The default option is <b>Switch Port</b> for the newly enabled physical port. The list contains:</p> <ul style="list-style-type: none"> <li>– Switch Port – Sets the port as an L2 port. The port forwards</li> </ul>

	<p>traffic based on the MAC address and operates in layer 2.</p> <ul style="list-style-type: none"> <li>– 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.</li> </ul>
<b>Mac Address</b>	<p>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.</p>

### 4.2.1.2 Port Monitoring

This screen 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



Label	Description
<b>Status</b>	<p>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. The default option is <b>Disabled</b>.</p> <p>The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables globally the mirroring feature in the switch.</li> <li>– Disabled – Disables globally the mirroring feature in the switch.</li> </ul>
<b>Monitor Port</b>	<p>Select the port to which the mirrored traffic is to be copied. This is a combination of interface type and interface ID. The</p>

	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.).
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Receive Monitoring</b>	Select whether the ingress traffic should be mirrored. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– 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.</li> <li>– Disabled – Disables mirroring of ingress traffic over this interface.</li> </ul>
<b>Transmit Monitoring</b>	Select whether the egress traffic should be mirrored. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled – Enables mirroring of egress traffic over this interface to port that is configured in the field <b>Monitor Port</b>. The mirroring of egress traffic is not performed, if the mirroring feature Status is globally disabled.</li> <li>– Disabled – Disables mirroring of egress traffic over this interface.</li> </ul>

### 4.2.1.3 Traffic Class

This screen allows the user to map evaluated user priority to traffic class, for forwarding by the bridge. RGS-PR9000-A supports eight traffic classes to handle priority traffic. Each traffic is assigned a traffic type based on the time sensitiveness of the traffic. Traffic class is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time-critical traffic compete for the network bandwidth

Select	Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7
Traffic Class									
<input type="radio"/>	Gi0/1	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/2	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/3	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/4	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/5	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/6	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>
<input type="radio"/>	Gi0/7	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Priority</b>	<p>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 <b>Default User Priority</b> value for the ingress port, if the untagged frames are received from Ethernet media. The priority determined is equal to the Regen user priority(configurable only through CLI) value for the ingress port and media- specific user priority, if the untagged frames are received from non-Ethernet media. The default value is 0. The list for the traffic class contains:</p> <ul style="list-style-type: none"> <li>- 0 – Best effort. This represents all kinds of non-detrimental traffic that is not sensitive to QoS metrics such as jitter.</li> <li>- 1 – Background. This represents bulk transfers and other activities that are permitted on the network without impacting the network usage for users and applications.</li> <li>- 2 – Standard (spare traffic). This represents traffic of more importance than background but less importance than excellent load.</li> <li>- 3 – Excellent load. This represents the best effort type</li> </ul>

	<p>service that an information services organization should deliver to its most important customers.</p> <ul style="list-style-type: none"> <li>- 4 – Controlled load. This represents traffic subject to admission control to assure that the traffic is received even when the network is overloaded.</li> <li>- 5 – Interactive voice and video. This represents traffic having delay less than 100 milli-seconds.</li> <li>- 6 – Internetwork control-Layer 3 network control. This represents traffic having delay less than 10 milli-seconds.</li> <li>- 7 – Network control-Layer 2 network control reserved traffic. This represents traffic that demands special treatment based on its</li> </ul>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### 4.2.1.4 Port Control

This screen allows the user to configure the port specific parameters such as negotiation mode of the switch.

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/MDIX Capability
<input type="radio"/>	Gi0/1	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/2	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/3	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/4	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/5	Auto	Full	100MBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/6	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto
<input type="radio"/>	Gi0/7	Auto	Full	1GBPS	Disabled	Disabled	Enabled		0	0	Auto

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Mode</b>	<p>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. The default option is <b>Auto</b>.</p> <p>The list contains:</p> <ul style="list-style-type: none"> <li>- 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</li> </ul>

	<p>connectivity between them. When the mode is set as Auto, the hardware senses the speed and negotiates with the port on the other end of the link for data transfer operation as full-duplex or half-duplex and about flow control.</p> <ul style="list-style-type: none"> <li>– NoNegotiation – 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. When the mode is set as NoNegotiation, the configured values for interface speed, duplex mode and flow control becomes effective.</li> </ul>
<b>Duplex</b>	<p>Select the duplex mode that represents the flow of data through the port. The list contains:</p> <ul style="list-style-type: none"> <li>– Full – Configures interface data transfer mode as full-duplex. Ports can send and receive data at the same time either send or receive data at that specified time.</li> </ul>
<b>Speed</b>	<p>Select the speed of the interface. The list contains:</p> <ul style="list-style-type: none"> <li>– 10 MBPS – Sets the port speed as 10MBPS. This implies that port can transfer data at the rate of 10 Megabits per second.</li> <li>– 100 MBPS – Sets the port speed as 100MBPS. This implies that port can transfer data at the rate of 100 Megabits per second.</li> <li>– 1 GBPS – Sets the port speed as 1GBPS. This implies that port can transfer data at the rate of 1 Giga bits per second.</li> <li>– 10 GBPS – Sets the port speed as 10GBPS. This implies that port can transfer data at the rate of 10 Giga bits per second.</li> <li>– 40 GBPS – Sets the port speed as 40 GBPS. This implies that port can transfer data at the rate of 40 Giga bits per second</li> <li>– 56 GBPS – Sets the port speed as 56 GBPS. This implies that port can transfer data at the rate of 56 Giga bits per second</li> <li>– 2.5 GBPS – Sets the port speed as 2.5 GBPS. This implies that port can transfer data at the rate of 2.5 Giga bits per second.</li> </ul>
<b>FlowControl Admin Status</b>	<p>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</p>



	<p>each unit is equal to 512 bit times. The list contains:</p> <ul style="list-style-type: none"> <li>– Disabled –Disables the flow control mechanism (that is, PAUSE).</li> <li>– Transmit – Enables the transmission of MAC control frames used for PAUSE, to a remote device.</li> <li>– Receive – Enables the reception of MAC control frames used for PAUSE from, a remote device.</li> <li>– Both – Enables both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device</li> </ul>
<p><b>FlowControl Oper Status</b></p>	<p>Displays the PAUSE mode currently used in the interface. If the negotiation <b>Mode</b> is set as <b>Auto</b> for the MAU attached to the interface, then the value is set based on the auto-negotiation function,. The list contains:</p> <ul style="list-style-type: none"> <li>– Invalid -Denotes the flow control operational status is invalid.</li> <li>– 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.</li> <li>– 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 Megabits per second or less.</li> <li>– 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 Megabits per second or less.</li> <li>– Both – Denotes that both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device is enabled.</li> </ul>
<p><b>HOL-Block Prevention</b></p>	<p>Select whether the Head-Of-Line (HOL) blocking should be prevented on a port. HOL blocking happens when HOL packet of a buffer cannot be switched to an output port. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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</li> </ul>

	<p>keeps track of necessity to retransmit discarded packets.</p> <ul style="list-style-type: none"> <li>- Disabled – Does not prevent HOL blocking on the port.</li> </ul>
<b>CPU Controlled Learning</b>	<p>Select the software learning status. This enables or disables the CPU controlled learning on a port. The MAC Address from the packets arriving on the interface are learnt through software instead of hardware. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Disabled – Disables the software learning of MAC Address.</li> <li>- Enabled – Enables the software learning of MAC Address.</li> </ul>
<b>Pause High Water Mark (kbps)</b>	<p>Enter the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges from 1 to 80000000 kbps. The default value is <b>0</b>.</p>
<b>Pause Low Water Mark (kbps)</b>	<p>Enter the ingress rate below which transmission of PAUSE frames are stopped. This value ranges from 1 to 80000000 kbps. The default value is <b>0</b>.</p>
<b>Auto MDI/ MDIX Capability</b>	<p>Select the Auto - MDIX mode for the interface. The default option is <b>Auto</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Auto – Enables MDI/MDIX auto cross over of the interface.</li> <li>- Mdi – Sets the port to mdi mode. This is hardware specific where transmit pair are pins 1,2 and the receive pair are 3,6 pins respectively for the particular port</li> <li>- Mdix – Sets the port to mdix mode. This is hardware specific where transmit pair are pins 3, 6 and the receive pair are 1, 2 pins respectively for the particular port. mdix is the vice versa of mdi.</li> </ul>

### 4.2.1.5 Rate Limiting

Select	Port	Ingress RateLimit			Egress RateLimit	
		DLF Level	Broadcast Level	Multicast Level	Egress-Port Rate-Limit	Port Burst-Size
<input type="radio"/>	Gi0/1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="radio"/>	Gi0/7	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Label	Description
<b>Select</b>	Select a port you want to configure
<b>Port</b>	The ID of the port to be configured
<b>Ingress RateLimit</b>	<p>You can limit the ingress rate so the packets will be dropped at the ingress port when the data rate exceeds the specified rate limit.</p> <p>DLF Level: specify the destination lookup failure packets per second.</p> <p>Broadcast Level: specify the broadcast packets per second</p> <p>Multicast Level: specify the multicast packets per second</p>
<b>Egress RateLimit</b>	<p>This will limit the throughput of each output priority queue.</p> <p>Egress-Port-Rate-Limit: specify the egress limit of packets per second</p> <p>Port Burst-Size: specify the egress limit of packet burst size</p>

## 4.2.2 VLAN

**VLAN (Virtual LAN)** module logically segments the shared media LAN to form virtual workgroups. It fully utilizes the forwarding support available in the switch hardware. It redefines and optimizes the basic transparent bridging functionalities such as learning, forwarding, filtering, flooding and so on.

### 4.2.2.1 Basic Setting

This screen allows the user to configure, for each available virtual contexts, 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

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 Mode	Dynamic Vlan Oper Status	Dynamic Multicast Oper Status	Maximum VLAN ID	Maximum Supported VLANs	Number of VLANs in the System	User Defined TPID
0		IVL	Disabled	Disabled	Enabled	Enabled	IVL	300	16128	DOT_1Q_VLAN_MODE	Disabled	Disabled	4066	4094	1	0

Label	Description
<b>Select</b>	Click to select the context ID to configure the VLAN Basic settings for the virtual context.
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Learning Mode</b>	<p>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. The default option is <b>IVL</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– <b>IVL</b> – 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.</li> <li>– <b>SVL</b> – 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.</li> <li>– <b>HYBRID</b> – 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 <b>L2 Unicast Filter Configuration</b> screen.</li> </ul>
<b>Subnet Based On All Ports</b>	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

	<p>to a VLAN-ID using an administrator configured table, if the subnet based VLAN classification is enabled. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the subnet based VLAN membership classification on all ports of the switch.</li> <li>– Disabled - Disables the subnet based VLAN membership classification on all ports of the switch.</li> </ul>
<b>MAC Based on All Ports</b>	<p>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. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables MAC based VLAN membership classification on all ports of the switch.</li> <li>– Disabled – Disables MAC based VLAN membership classification on all ports of the switch.</li> </ul>
<b>Port and Protocol Based on All Ports</b>	<p>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. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables port and protocol based VLAN membership classification on all ports of the switch.</li> <li>– Disabled – Disables port and protocol based VLAN membership classification on all ports of the switch.</li> </ul>
<b>Global MAC Learning Status</b>	<p>Enable or disable global MAC learning function</p>
<b>Default Vlan Hybrid Type</b>	<p>Select the default Vlan Hybrid Type to be applied for all ports of the switch, if Learning Mode is set as <b>HYBRID</b>. The default option is <b>IVL</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– IVL – Separate forwarding database is created for each VLAN. The information learnt from a VLAN is not shared among other</li> </ul>

	<p>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.</p> <ul style="list-style-type: none"> <li>– 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.</li> </ul>
<b>MAC-Address-Table Aging Time</b>	<p>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 from 10 to 1000000 seconds. The default value is <b>300</b> seconds.</p>
<b>Unicast MAC Learning Limit</b>	<p>Enter the maximum number of unicast MAC addresses that can be learned in the virtual context. This value ranges from 0 to 4294967295. The maximum number of unicast MAC addresses that can be learnt for the different kind of boards are:</p> <ul style="list-style-type: none"> <li>– 950 for BCM and Marvell boards</li> <li>– 16128 for xCAT board.</li> </ul>
<b>Base Bridge Mode</b>	<p>Select the base bridge-mode in which the switch should operate. The list contains:</p> <ul style="list-style-type: none"> <li>– DOT_1D_BRIDGE_MODE – Makes the switch to behave according to IEEE 802.1d implementation.</li> <li>– DOT_1Q_VLAN_MODE – Makes the switch to behave according to IEEE 802.1q implementation</li> </ul>
<b>Dynamic Vlan Oper Status</b>	<p>Displays the operational status of the <b>Dynamic VLAN</b> 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. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Denotes that the GVRP module is enabled in the switch.</li> <li>– Disabled – Denotes that the GVRP module is disabled in the switch.</li> </ul>

<b>Dynamic Multicast Oper Status</b>	<p>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. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Denotes that the GMRP module is enabled in the switch.</li> <li>– Disabled – Denotes that the GMRP module is disabled in the switch.</li> </ul>
<b>Maximum VLAN ID</b>	<p>Displays the largest valid VLAN / VFI ID accepted in the system. This value ranges from 1 to 65535.</p> <ul style="list-style-type: none"> <li>– &lt;vlan -id&gt; - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094</li> <li>– &lt;vfi-id&gt;. - 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 from 4096 to 65535</li> </ul>
<b>Maximum Supported VLANs</b>	<p>Displays the maximum number of VLANs the switch can support.</p>
<b>Number of VLANs in the System</b>	<p>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.</p>
<b>User Defined TPID</b>	<p>Enter the value for the user defined TPID configurable for an Ingress port or for a VLAN Egress Ethertype. The value ranges from 0 to 65535. The default value is <b>0</b>. A value 0(ZERO) deletes the configured entry.</p>

#### 4.2.2.2 Port Setting

This screen allows the user to configure VLAN details such as VLAN membership classification type, for the physical ports available in the device. 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:

- MAC-based VLAN classification
- Subnet-based VLAN classification
- Port and protocol based VLAN classification

Select	Port	MAC Based VLAN	Port and Protocol Based VLAN	Port Protected	Subnet Based VLAN	PVID	Acceptable Frame Types	Ingress Filtering	Ingress EtherType Prefix Hex values by 0x	Egress EtherType Prefix Hex values by 0x	Egress TPID Type	Allowable TPID1	Allowable TPID2	Allowable TPID3
<input type="radio"/>	Gi0/1	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/2	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/3	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/4	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/5	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/6	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0
<input type="radio"/>	Gi0/7	Disabled	Enabled	False	Disabled	1	All	Disabled	8100	8100	Portbased	0	0	0

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>MAC Based VLAN</b>	<p>Select whether the MAC based VLAN membership classification is supported in the port. VLAN membership classification is done based on the source MAC address of the received packets, if the MAC based VLAN classification is supported. By default, the MAC based VLAN classification is set similar as that of the MAC Based on All Ports. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables MAC based VLAN classification in the port.</li> <li>– Disabled – Disables MAC based VLAN classification in the port.</li> </ul>
<b>Port and Protocol Based VLAN</b>	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



	<p>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 on All Ports. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables port and protocol based VLAN classification in the port.</li> <li>– Disabled – Disables port and protocol based VLAN classification in the port.</li> </ul>
<b>Port Protected</b>	<p>Select whether the port should be configured as protected. The default option is <b>False</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– True – Sets the port as protected. The port will not forward frames received from another protected port on the same switch.</li> <li>– False – Does not configure the port as protected. The port operates as a normal port.</li> </ul>
<b>Subnet Based VLAN</b>	<p>Select whether the subnet based VLAN membership classification is supported in the port. 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 supported. By default, the subnet based VLAN classification is set similar as that of the Subnet Based On All Ports. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables subnet based VLAN classification in the port.</li> <li>– Disabled – Disables subnet based VLAN classification in the port.</li> </ul>
<b>PVID</b>	<p>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. The default VLAN ID (that is, 1) is set as the PVID. This value ranges from 1 to 4094.</p>
<b>Acceptable Frame Types</b>	<p>Select the type of VLAN dependent BPDU frames to be accepted by the port during the VLAN membership configuration. The default option is <b>All</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– All – Accepts tagged, untagged and priority tagged</li> </ul>

	<p>frames received on the port and subjects the frames to <b>Ingress Filtering</b> setting.</p> <ul style="list-style-type: none"> <li>– Tagged – Accepts only the tagged frames received on the port. Rejects untagged or priority tagged frames received on the port.</li> <li>– UnTagged and Priority Tagged – Accepts only the untagged or priority tagged frames received on the port. Rejects tagged frames received on the port.</li> </ul>
<b>Ingress Filtering</b>	<p>Select whether the filtering should be applied for the incoming frames received on the port. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Accepts only the incoming frames of the VLANs that have this port in its member list.</li> <li>– Disabled – Accepts all incoming frames received on the port.</li> </ul>
<b>Ingress EtherType Prefix Hex values by 0x</b>	<p>Enter the value for IngressEtherType. The value ranges from 1 to 65535. The default value is <b>33024</b>.</p>
<b>Egress EtherType Prefix Hex values by 0x</b>	<p>Enter the value for IngressEtherType. The value ranges from 1 to 65535. The default value is <b>33024</b>.</p>
<b>Egress TPID Type</b>	<p>Select the egress TPID type for the port. The default option is <b>Portbased</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– <b>Portbased</b> - Specifies the egress TPID type for a port. If the value is portbased the egress TPID of the packet is selected from Egress Port Table.</li> <li>– <b>Vlanbased</b> - Specifies the egress TPID type for a port. When the value is vlanbased the Egress TPID is selected from Egress VLAN Table</li> </ul>
<b>Allowable TPID1</b>	<p>Enter the value for TPID1. This specifies the secondary ether type that is allowable for a port. The configurable value for this object is 0x8100 or 0x8808. This value ranges from 0 to 65535. The default value is <b>0</b>.</p>
<b>Allowable TPID2</b>	<p>Enter the value for TPID2. This specifies the standard ether type that is allowable for a port. The value ranges from 0 to 65535. The configurable value for this object is Q-in-Q EtherType [0x9100]. The default value is <b>0</b>.</p>

<b>Allowable TPID3</b>	Enter the value for TPID3. This specifies the additional user defined ether type that is allowable for a port. This value ranges from 0 to 65535. The default value is <b>0</b> .
------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.2.3 Static VLANs

This screen 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.

VLAN ID  \*

VLAN Name

Member Ports  \*

Untagged Ports

Forbidden Ports

Vlan Type normal ▼

Primary Vlan Id

Vlan Egress Ethertype

VLAN ACTIVE

Select	VLAN ID	VLAN Name	Member Ports	Untagged Ports	Forbidden Ports	Vlan Type	Primary Vlan Id	VLAN ACTIVE	Vlan Egress Ethertype
⊙	1		Gi0/1, Gi0/2, Gi0/3, Gi	Gi0/1, Gi0/2, Gi0/3, Gi		Normal ▼	-	ACTIVE	0x8100
<input type="button" value="Apply"/> <input type="button" value="Delete"/>									

Label	Description
<b>VLAN ID</b>	Enter the VLAN ID that uniquely identifies a specific VLAN. This value ranges from 1 to 4094.
<b>VLAN Name</b>	Enter an administratively assigned string, which is used to identify the VLAN. This value is a string of maximum size 32.
<b>Member Ports</b>	<p>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.</p> <p>The format of this entry is &lt;interface type&gt;&lt;slot number/port number&gt; for gigabitethernet ports. For pseudo wire and attachment circuit interfaces the format is just the interface ID. There is no space needed between these two entries.</p> <p>Example: Gi0/1, Gi0/2, pw1, ac1 (Here Gi is interface type Gigabit Ethernet, Pw is pseudo wire interface and AC is the attachment circuit interface. 0 is slot number and 1 is port number)</p>

<b>Untagged Ports</b>	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 <b>VLAN Member Ports</b> .
<b>Forbidden Ports</b>	Enter port or set of ports which should never receive packets from the VLAN mentioned in the <b>VLAN ID</b> . 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 <b>Member Ports</b> list field.
<b>VLAN Type</b>	Select the private VLAN type to be applied for the specified VLAN ID. The default option is <b>Normal</b> The list contains: <ul style="list-style-type: none"> <li>– Normal – The configured VLAN is not assigned to any private VLAN domain.</li> <li>– Primary – The configured VLAN is set as primary VLAN in a private VLAN domain.</li> <li>– Isolated – The configured VLAN is set as isolated VLAN in a private VLAN domain. The devices connected to host port of this VLAN cannot communicate with each other. One primary VLAN ID should be configured for every isolated VLAN.</li> <li>– 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.</li> </ul>
<b>Primary VLAN ID</b>	Enter the primary VLAN ID that uniquely identifies a primary VLAN associated with the specified VLAN ID. This value ranges from 1 to 4094.
<b>VLAN Egress Ethertype</b>	Enter the value for egress ether type of a packet. The value set for this object is applicable for a port present in this vlan only when the value of vlan PortEgressTPID type is set as vlan based for an egress port. The value ranges from 0 to 65535. The default value is <b>33024</b> .
<b>VLAN Active</b>	Select this check-box to make configured VLAN active.

<b>Select</b>	Click to select the vlan id for which the configuration needs to be modified or deleted.
---------------	------------------------------------------------------------------------------------------

### 4.2.2.4 Protocol Group

This screen 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.

Frame Type \*

Protocol Value \*

Group Identifier \*

Select	Frame Type	Protocol Value	Group Identifier
<input type="button" value="Apply"/> <input type="button" value="Delete"/>			

Label	Description
<b>Frame Type</b>	<p>Select the data-link encapsulation format to be applied in a protocol template. The default option is <b>Ethernet</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Ethernet – Applies the standard IEEE 802.3 frame format. This format contains the following: <ul style="list-style-type: none"> <li>▪ Preamble – 7 byte value that allows the Ethernet card to synchronize with the beginning of a frame.</li> <li>▪ SFD – 1 byte value that indicates the start of a frame.</li> <li>▪ Destination – 6 byte MAC address of the destination.</li> <li>▪ Source – 6 byte MAC address of the source or a broadcast</li> <li>▪ Length – 2 byte value representing the number of bytes in the data Fields.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>▪ Data – 46 to 1500 bytes higher layer information containing protocol information or user data.</li> <li>▪ FCS – 4 byte value representing the cyclic redundancy check used by source and destination to verify a successful transmission.</li> </ul> <p>– 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.</p> <ul style="list-style-type: none"> <li>▪ OUI – 3 byte value representing organizational unique ID assigned to vendors for differentiating protocols from different manufacturers.</li> <li>▪ Type – 2-byte value representing protocol type that defines a specific protocol in the SNAP. This maintains compatibility with Ethernet v2.</li> </ul> <p>– 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.</p> <ul style="list-style-type: none"> <li>▪ 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</li> <li>▪ 2 octet type field – encoding of 802.3 type field in an IEEE 802.2/SNAP header</li> </ul> <p>– 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.</p> <p>– 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.</p> <ul style="list-style-type: none"> <li>▪ DSAP – 1 byte value representing destination</li> </ul>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>service access point to determine the protocol used for the upper layer.</p> <ul style="list-style-type: none"> <li>▪ SSAP – 1 byte value representing source service access point to determine the protocol used for the upper layer.</li> <li>▪ Control – 1 byte value that is used by certain protocols for administration.</li> </ul>
<b>Protocol Value</b>	<p>Select the protocol to be applied above the data-link layer in a protocol template. The default option is <b>IP</b>. The protocol identification is internally handled using octet string. The list contains:</p> <ul style="list-style-type: none"> <li>– IP – Sets the protocol as IP, which is used for communicating data across network using TCP/IP. The corresponding octet string is 08:00.</li> <li>– NOVELL – Sets the protocol as Novell Netware protocol suite, which is developed by Novell Inc. The corresponding octet string is ff:ff.</li> <li>– 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.</li> <li>– APPLETALK – Sets the protocol as AppleTalk, which is a proprietary suite of protocols developed by Apple Inc. The corresponding octet string is 80:9b.</li> <li>– OTHER – Sets the protocol as some other protocol other than IP, NOVELL, NETBIOS and APPLETALK.</li> </ul>
<b>Group Identifier</b>	<p>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 from 0 to 2147483647.</p>
<b>Select</b>	<p>Click to select the Frame Type for which the Group Identifier needs to be modified or deleted.</p>

#### 4.2.2.5 Port Protocol

This screen 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 VLAN ID

which is not yet configured can be assigned for a port. When the VLAN is configured, forwarding will take place according to the VID set for the particular port

Label	Description
<b>Port</b>	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).
<b>Group IP</b>	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 from 0 to 2147483647.
<b>VLAN ID</b>	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 from 1 to 4094.
<b>Select</b>	Click to select the Port for which the Group ID and VLAN ID mapping needs to be modified or deleted.
<b>Status</b>	Displays the status of the respective row / entry. This list contains: <ul style="list-style-type: none"> <li>- Up – Denotes the entry is created and operationally up.</li> <li>- Down – Denotes the entry is created but operationally down.</li> <li>- Under Creation – Denotes the entry is being created and not available for operation / usage.</li> </ul>



### 4.2.2.6 Port MAC Map

Port No	<input type="text"/> *
Port Mac-Map Addr	<input type="text"/> *
Port Mac-Map Vid	<input type="text"/> *
Bcast Option	Allow <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select | Port No. | Port Mac-Map Addr | Port Mac-Map Vid | Bcast option

Label	Description
<b>Port No</b>	Enter the port to which MAC and VLAN 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. The format is <i>&lt;interface type&gt;&lt;slot number/port number&gt;</i> . There is no space between these two entries. Example: Gi0/1 (Here Gi is interface type Gigabit Ethernet interface 0 is slot number and 1 is port number.)
<b>Port Mac-Map Addr</b>	Enter a unique unicast MAC address for the port, which should be mapped to the VLAN and used for MAC based VLAN membership classification.
<b>Port Mac-Map VID</b>	Enter the VLAN ID that uniquely identifies a specific VLAN to which the MAC address of the port should be mapped. This VLAN ID is associated with a specific group of protocols for the specific port. This value ranges from 1 to 4094.
<b>Bcast Option</b>	Select whether the multicast / broadcast untagged frames should be allowed / discarded. The default option is <b>Allow</b> . The list contains : <ul style="list-style-type: none"> <li>- Allow – Drops all multicast / broadcast untagged frames that contain source MAC address belonging to the address configured in the field <b>Port Mac-Map Addr</b>, if the <b>MAC Based VLAN</b> is enabled on the port.</li> <li>- Discard – Processes all multicast / broadcast untagged</li> </ul>

	frames that contain source MAC address belonging to the address configured in the field <b>Port Mac-Map Addr</b> , if the <b>MAC Based VLAN</b> is enabled on the port.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.2.6 Unicast MAC

This screen 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 screen **Static VLAN Configuration** and for the default VLAN, once this screen is accessed. It displays the unicast MAC settings details for the default VLAN alone, if no new VLAN is created in the screen **Static VLAN Configuration**.

Select	Context	Vlan ID	Mac Admin Status	Mac Limit	Mac Operational Status
<input type="radio"/>	0	1	Default <input type="button" value="v"/>	1500	Enable

Label	Description
<b>Select</b>	Click to select the VLAN entry for which the unicast MAC settings should be configured.
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Vlan ID</b>	Displays the VLAN ID that uniquely identifies a specific VLAN. This value ranges from 1 to 4094.
<b>Mac Admin Status</b>	Select the MAC administration status to learn unicast MAC address for the VLAN. The default option is <b>Default</b> . The list contains: <ul style="list-style-type: none"> <li>- Enabled – Learns the unicast MAC address for the VLAN.</li> <li>- Disabled – Does not learn the unicast MAC address for the VLAN.</li> <li>- Default – Sets the default MAC administration status.</li> </ul>
<b>Mac Limit</b>	Enter the maximum number of distinct unicast MAC addresses that can be learnt in the VLAN. This value ranges from 0 to 4294967295. The maximum number of unicast MAC addresses that can be learnt for the different kind of boards are:

	<ul style="list-style-type: none"> <li>- 950 for BCM and Marvell boards</li> <li>- 16128 for xCAT board.</li> </ul>
<b>Mac Operational Status</b>	<p>Displays the operational status of the MAC learning for the VLAN. The list contains:</p> <ul style="list-style-type: none"> <li>- Enable –Denotes that the MAC learning for the VLAN is enabled.</li> <li>- Disable – Denotes that the MAC learning for the VLAN is disabled.</li> </ul>

### 4.2.2.7 Wildcard

This screen allows the user to configure wild card VLAN, which has ID as 0xFFFF. 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** screen

Select	ContextId	MacAddress	Portlist
--------	-----------	------------	----------

Label	Description
<b>Context ID</b>	Select the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Address Selection</b>	<p>Select the type of destination MAC address to which the filtering information of the wild card entry should be applied.</p> <p>The list contains:</p> <ul style="list-style-type: none"> <li>- 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 greyed out and cannot be configured.</li> <li>- Mac Address – Forwards the received frames that contain</li> </ul>

	the MAC address configured in the text box next to this field, through the Ports, if no specific static filtering is configured.
<b>Ports</b>	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 <b>Address-Selection</b> 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)

### 4.2.2.8 Switch Port Filtering

This screen 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.

Select	Vlan Port No	Utility Criteria
<input type="radio"/>	Gi0/1	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/2	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/3	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/4	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/5	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/6	default <input type="button" value="v"/>
<input type="radio"/>	Gi0/7	default <input type="button" value="v"/>

Label	Description
<b>Select</b>	Click to select the port for which filtering utility criteria needs to be configured.
<b>Vlan Port No</b>	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).
<b>Utility Criteria</b>	Select the filtering utility criteria to be applied for the port. The

	<p>learning on a port is decided based on the - Selected filtering utility criteria. The default option is <b>default</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- default – Learning of source MAC from a packet received on the port is done, only if there is at least one member port for a VLAN mentioned in the packet.</li> <li>- enhanced – Learning of source MAC from a packet received on the port is done, only if the following conditions are satisfied.             <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> </ul> </li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.2.9 FDB Flush

This screen allows the user to flush all the dynamically generated MAC address.

Context Id

Interface Id

Vlan Id

Label	Description
<b>Context Id</b>	<p>Select the virtual context ID for which the MAC addresses need to be flushed. This is a uniquely represents a virtual switch created in the system. This value ranges from 0 to 65535. The default value is <b>0</b>.</p> <ul style="list-style-type: none"> <li>- The virtual context feature is not available in the RGS-PR9000-A Workgroup and Enterprise packages.</li> <li>- By default, in all RGS-PR9000-A packages, the basic</li> </ul>

	<p>configuration of the protocols having MI support are mapped to the default context ID (0).</p> <ul style="list-style-type: none"> <li>- The user can create new virtual contexts from the Switch Creation screen. This screen will not be available in Workgroup and Enterprise package.</li> </ul>
<b>Interface Id</b>	<p>Enter the interface ID for which the FDB entries need to be flushed. This is a combination of slot number and the port number. The format is &lt;interface type&gt;&lt;slot number/port number&gt;. There is no space between these two entries</p>
<b>Vlan Id</b>	<p>Enter the VLAN ID for which the FDB entries need to be flushed. This value ranges from 1 and 4094.</p>

### 4.2.3 VLAN Subnet

This screen allows the user to map IP subnet address and VLAN ID to a particular port for subnet-based VLAN membership classification. The source IP-subnet address in the incoming packets is used to classify VLAN membership.

The subnet based VLAN is applied only on IP/ARP packets. The port number is always set as 0 for BCM chipsets, as BCM supports subnet based VLAN globally and not on per port basis

Port No  \*

Subnet Ip  \*

Vlan Id  \*

Arp Bcast Option Allow

Select	Port No.	Subnet Allowed	Mapped Vlan Id	Arp Option
--------	----------	----------------	----------------	------------

Label	Description
<b>Port No</b>	<p>Enter the port number that uniquely identifies the specific port in the switch. 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 &lt;interface type&gt;&lt;slot</p>

	number/port number>. There is no space between these two entries. Example: Gi0/1 (Here Gi is interface type Gigabit Ethernet interface 0 is slot number and 1 is port number.)
<b>Subnet Ip</b>	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.
<b>Vlan Id</b>	Enter the VLAN ID that uniquely identifies a specific VLAN to which the source IP subnet address should be mapped. This value ranges from 1 to 4094.
<b>Arp Bcast Option</b>	Select whether the ARP untagged frames on the VLAN should be discarded or allowed. The default option is <b>Allow</b> . The list contains: <ul style="list-style-type: none"> <li>- Allow – Performs VLAN classification for ARP frames having source IP subnet address matching with the field <b>Subnet IP</b>.</li> <li>- Discard – Does not perform VLAN classification for ARP frames having source IP subnet address matching with the field <b>Subnet IP</b>.</li> </ul>

### 4.2.4 GARP

GARP (Generic Attribute Registration Protocol) is used to synchronize attribute information between the bridges in the LAN. It allows to register and de-register attribute values, which are disseminated into the backbone of the GARP participants.

Select	Context	GARP Status
<input checked="" type="radio"/>	0	Shutdown

Apply

Configure GARP Trace Options

Label	Description
<b>Select</b>	Click to select the context to start or shutdown GARP module.
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>GARP Status</b>	Select the administrative status requested by management for GARP. The default option is <b>Start</b> for the default context ID (0) and <b>Shutdown</b> for other context IDs. The list contains: <ul style="list-style-type: none"> <li>– Start – Enables GARP in the switch on all ports. GMRP and GVRP are enabled explicitly, once the disabled GARP is enabled.</li> <li>– Shutdown – Disables GARP in the switch on all ports and releases all memories.</li> </ul>

## 4.2.5 Dynamic VLAN

Dynamic VLAN feature (GVRP) allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in the topology. It uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in the LAN. GVRP learnt dynamic VLAN memberships are stored in VLAN current database.

The dynamic VLAN feature cannot run in the C-VLAN component of a provider edge bridge.

### 4.2.5.1 Dynamic VLAN

The screen 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



Label	Description
<b>Select</b>	Click to select the context for which the configuration needs to be done.
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0



	to 65535. The default value is <b>0</b> .
<b>Dynamic Vlan Status</b>	<p>Select the administrative status requested by management for GVRP. The default option is <b>Enabled</b> for the default context ID (0) and <b>Disabled</b> for other context IDs. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables GVRP on the switch, on all ports for which GVRP is not specifically disabled in the <b>Dynamic Vlan Port Configuration</b> screen.</li> <li>– Disabled – Disables GVRP on all ports of the switch and transparently forwards all GVRP packets.</li> </ul>

### 4.2.5.2 Port Settings

This screen allows the user to configure the dynamic VLAN feature related parameters for each physical port available in the switch

Select	Port	Dynamic Vlan Status	Restricted VLAN Registration
<input type="radio"/>	Gi0/1	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/2	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/3	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/4	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/5	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/6	Disabled ▼	Disabled ▼
<input type="radio"/>	Gi0/7	Disabled ▼	Disabled ▼

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Dynamic Vlan Status</b>	<p>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 <b>Disabled</b> to <b>Enabled</b>. The default option is <b>Enabled</b> on all physical ports. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables GVRP in the port, only if <b>Dynamic Vlan</b></li> </ul>

	<p><b>Status</b> is globally enabled. Otherwise GVRP is not enabled in the port. Once the <b>Dynamic Vlan Status</b> is globally disabled, GVRP enabled in the port is also disabled.</p> <ul style="list-style-type: none"> <li>– Disabled – Disables GVRP in the port, even if the dynamic VLAN feature (<b>Dynamic Vlan Status</b>) is globally enabled. Silently discards any received GVRP packets and does not propagate GVRP registrations from other ports.</li> </ul>
<p><b>Restricted VLAN Registration</b></p>	<p>Select whether to restrict GVRP from dynamically registering the VLAN. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– Disabled – Disables restricted VLAN registration. That is, the creation or modification of a dynamic VLAN entry is permitted for all VLANs.</li> </ul>

### 4.2.5.3 Garp Timers

This screen 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

Select	Port No	GarpJoinTime (msec)	GarpLeaveTime (msec)	GarpLeaveAllTime (msec)
--------	---------	---------------------	----------------------	-------------------------

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port No</b>	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)
<b>GarpJoinTime(msecs)</b>	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 re-transmitted only once, if the initial message is not acknowledged. This timer is

	<p>started when the initial join message is sent.</p> <p>The join message is sent by a GARP participant to another GARP participant for registering:</p> <ul style="list-style-type: none"> <li>- Its attributes with other participant</li> <li>- Its manually configured attributes</li> <li>- Attributes received from a third GARP participant</li> </ul> <p>This value is represented in milliseconds. The default value is <b>200</b> milliseconds. The value can only be set as multiple of tens (e.g., 210, 220, 230 and so on).</p> <p>This value should satisfy the condition:</p> <p><math>GarpJoinTime &gt; 0</math> and <math>(2 * GarpJoinTime) &lt; GarpLeaveTime</math>.</p>
<p><b>GarpLeaveTime(msecs)</b></p>	<p>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.</p> <p>The leave messages are sent from a GARP participant to another participant in the following scenario:</p> <ul style="list-style-type: none"> <li>- Its attributes should be de-registered</li> <li>- Its attributes are manually de-registered</li> <li>- It receives leave messages from a third GARP participant</li> </ul> <p>This value is represented in milliseconds. The default value is <b>600</b> milliseconds. The value can only be set as multiple of tens (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 join time is 500 milliseconds, then the leave time value can be from 510 milliseconds to 1000 milliseconds only.</p>
<p><b>GarpLeaveAllTime(msecs)</b></p>	<p>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</p>

	<p>participant started or re-registration is done. The leaveall messages are sent from a GARP participant to other participants for:</p> <ul style="list-style-type: none"> <li>- De-registering all registered attributes</li> <li>- Re-registering all attributes with each of the participants</li> </ul> <p>This value is represented in milliseconds. The default value is <b>10000</b> milliseconds. You can set the value as multiple of tens (that is, as 10010, 10020 and so on).</p> <ul style="list-style-type: none"> <li>- The leave all time should be greater than 0 and greater than GarpLeaveTime.</li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.2.6 MSTP

MSTP (Multiple Spanning Tree Protocol) is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It allows the user to build several MST over VLAN trunks, and group or associate VLANs to spanning tree instances, so the topology of one instance is independent of the other instance. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances. The MSTP provides an optional capability for high availability, executing multiple instances of the protocol, and provider bridging.

### 4.2.6.1 Basic Settings

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	Flush Interval	Flush Indication Threshold	BPDU Guard
<input checked="" type="radio"/>	0	Start	Disabled	16	32768	MSTP	00:1e:94:00:00:01	0	False	False	0	0	disable

Label	Description
<b>Select</b>	Click to select the context for which the configuration needs to be done.
<b>Context Id</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>System Control</b>	Select the administrative shutdown status requested by

	<p>management for the MST feature. This status allows the user to set the availability of the MST feature on all ports in the switch. The default option is <b>Start</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Start – Activates the MST feature in the switch on all ports. The required memory is allocated for the feature.</li> <li>– Shutdown – Stops the MST feature in the switch on all ports. The allocated memory is released and made available for other activities.</li> </ul>
<b>MSTP Status</b>	<p>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. The default option is <b>Enabled</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the MST feature in the switch on all ports.</li> <li>– Disabled – Disables the MST feature in the switch on all ports.</li> </ul>
<b>Maximum MST Instances</b>	<p>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 VLANs used by ESPs. This value ranges from 1 to 64. The default value is <b>64</b>.</p>
<b>Bridge Priority</b>	<p>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 from 0 to 61440. The default value is <b>32768</b>. The value should be set in increments of 4096, eg 0, 4096, 8192, 12288 and so on.</p>
<b>Protocol Version</b>	<p>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. The default option is <b>MSTP</b>. The options are::</p> <ul style="list-style-type: none"> <li>– STP – Removes the loop using the STP specified in IEEE 802.1D.</li> <li>– RSTP – Removes the loop using the RSTP specified in IEEE</li> </ul>

	<p>802.1w.</p> <ul style="list-style-type: none"> <li>– MSTP – Removes the loop using the MSTP specified in IEEE 802.1s.</li> </ul>
<b>Region Name</b>	<p>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 d7GS-PR9000-Aeminate STP topology information for other STP instances. The default value is same as that of the Switch Base MAC Address configured in the <b>Factory Default Settings</b> screen. This value is an octet string of maximum size 32.</p>
<b>Region Version</b>	<p>Enter the unique identifier that represents the specific MST region. This value ranges from 0 to 65535.</p>
<b>Dynamic Path Cost Calculation</b>	<p>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. The default option is <b>False</b>. The options are::</p> <ul style="list-style-type: none"> <li>– True – Dynamically calculates path cost based on the speed of the ports whose <b>Admin State</b> is set as <b>Up</b> at that time. The path cost is not changed based on the operational status of the ports, once calculated.</li> <li>– False – Dynamically calculates path cost based on the link speed at the time of port creation.</li> </ul>
<b>Speed Change Path Cost Calculation</b>	<p>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. The default option is <b>False</b>. The options are::</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– False – Does not dynamically calculate the path cost for ports</li> </ul>

	based their speed at that time.
<b>Flush Interval</b>	Enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is <b>0</b> .
<b>Flush Indication Threshold</b>	Enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is <b>0</b>

### 4.2.6.2 Timers

This screen 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

Select	Context Id	Maximum Hop Count	Max Age	Forward Delay	Transmit Hold Count	Hello Time
<input checked="" type="radio"/>	0	20	20	15	6	2

Label	Description
<b>Select</b>	Click to select the context for which the configuration needs to be done.
<b>Context ID</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.
<b>Maximum Hop Count</b>	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. This value ranges from 6 to 40. The default value is <b>20</b> . 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
<b>Max Age</b>	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 BPDU 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 from 6 to 40 seconds. The default value is <b>20</b> seconds.
<b>Forward Delay</b>	Enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state. This value ranges from 4 to 30 seconds. The default value is <b>15</b> seconds
<b>Transmit Hold Count</b>	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 from 1 to 10. The default value is <b>3</b> .
<b>Hello Time</b>	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. The default value is <b>2</b> .

### 4.2.6.3 Port Configuration

This screen 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.

Select	Port	Path Cost	Priority	PointToPoint Status	Edge Port	MSTP Status	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN	BPDU Receive	BPDU Transmit	Layer2-Gateway Port	Loop Guard	Root Guard	Bpdu Guard	Error Recovery
<input type="radio"/>	Gi0/1	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/2	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/3	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/4	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/5	20000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/6	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000
<input type="radio"/>	Gi0/7	2000000	128	ForceTrue	True	Disable	True	200	True	True	True	True	True	True	True	True	None	30000

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Path Cost</b>	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



	<p>cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The default value is <b>20000</b> for all physical ports and <b>199999</b> for port channels.</p>
<b>Priority</b>	<p>Enter the priority value that is assigned to the port. This value is used during the role selection process. The <b>Role</b> is computed for the port for instances to which the port is assigned as member. This value ranges from 0 to 240. The default value is <b>128</b>. This value should be set in increments of 16, eg 0, 16, 32, 48 and so on.</p>
<b>PointToPoint Status</b>	<p>Select the administrative point-to-point status of the LAN segment attached to the port. The default option is <b>Auto</b>. The options are:</p> <ul style="list-style-type: none"> <li>– ForceTrue – Always treats the port as if it is connected to a point-to-point link.</li> <li>– ForceFalse – Always treats the port as if it is having a shared media connection.</li> <li>– Auto – Treats the ports as having a shared media connection or a point- point link based on the prevailing conditions.</li> </ul> <p>Port is considered to have a point-to-point link if,</p> <ul style="list-style-type: none"> <li>– It is an aggregator and all of its members can be aggregated.</li> <li>– The MAC entity is configured for full <b>Duplex</b> operation, either manually or through auto negotiation process (that is, negotiation <b>Mode</b> is set as <b>Auto</b>).</li> </ul> <p>Otherwise port is considered to have a shared media connection</p>
<b>Edge Port</b>	<p>Select the administrative value of the Edge Port parameter. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>– True – Sets the port as an edge port (that is, the <b>Port State</b> is immediately set as <b>forwarding</b>). It is connected directly to a single end station. It allows MSTP to converge faster and does not wait to receive BPDUs.</li> <li>– False – Sets the port as a non-Edge port (that is, the</li> </ul>

	spanning tree process is performed using the MSTP). It is connected to a routing device such as switch.
<b>MSTP Status</b>	<p>Select the MSTP status of the port for all spanning tree instances. This value will override the port's status in the MSTI contexts. The default option is <b>Enable</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Enable – Enables MST in the port. MAC frames are forwarded and their source addresses are learnt.</li> <li>– Disable – Disables MST in the ports. MAC frames are not forwarded and their source addresses are not learnt.</li> </ul>
<b>Protocol Migration</b>	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– False – Does not perform protocol migration mechanism. The port always transmits the standard MSTP BPDUs.</li> </ul>
<b>Hello Time</b>	<p>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. The default value is <b>2</b> seconds.</p>
<b>AutoEdge Status</b>	<p>Select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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 <b>Edge Port</b>, based on the reception of BPDU.</li> <li>– False – Uses the manually configured value for the Edge Port parameter. The value set in the field <b>Edge Port</b> is used for the Edge Port parameter.</li> </ul>
<b>Restricted Role</b>	<p>Select whether the selection of port <b>Role</b> as root can be</p>

	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- False – Includes all available ports of the topology, in the root selection process to select the root for CIST or any MSTI.</li> </ul>
<b>Restricted TCN</b>	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>- True – Blocks the port from propagating the received topology change notifications and topology changes to other ports.</li> <li>- False – Allows the port to propagate the received topology change notifications and topology changes to other ports.</li> </ul>
<b>BPDU Receive</b>	<p>Select the processing status of the received MSTP BPDUs. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>- True – Normally processes the MSTP BPDUs received on the port.</li> <li>- False – Discards the MSTP BPDUs received on the port.</li> </ul>
<b>BPDU Transmit</b>	<p>Select the BPDU transmission status of the port. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>- True – Transmits the MSTP BPDUs from the port.</li> <li>- False – Blocks the transmission of MSTP BPDUs from the port.</li> </ul>
<b>Layer2 Gateway Port</b>	<p>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 <b>Admin State</b> is</p>

	<p>set as <b>Up</b>. The default option is <b>false</b>. The options are:</p> <ul style="list-style-type: none"> <li>– True – Allows the port to operate as a L2GP.</li> <li>– False – Allows the port to operate as a normal port.</li> </ul>
<b>Loop Guard</b>	<p>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. The default option is False. The options are:</p> <ul style="list-style-type: none"> <li>– True – Enables the loop guard feature in the port.</li> <li>– False – Disables the loop guard feature in the port.</li> </ul>
<b>Root Guard</b>	<p>Select <b>True</b> to enable the root guard function and <b>False</b> to disable it. When root guard is enabled on a port, that port cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an “alternate” port role and enters a blocking state if it receives superior STP BPDUs. Select this option to enable root guard for the port.</p>
<b>BPDU Guard</b>	<p>Set the port to none will enable the switch to monitor edge ports and disable them if they receive BPDU packets.</p>
<b>Error Recovery</b>	<p>Set the port to recover from an error-disabled state.</p>

#### 4.2.6.4 VLAN Mapping

This screen 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.

MSTP Instance ID	<input type="text"/> *
Add VLAN	- <input type="button" value="v"/>
Delete VLAN	- <input type="button" value="v"/>
Flush Indication Threshold	<input type="text"/> *
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Instance ID	Mapped VLANs	Flush Indication Threshold
<input type="button" value="Delete"/>			

Label	Description
<b>MSTP Instance ID</b>	Enter an integer value that is used to uniquely identify an instance of the MSTP. This value ranges from 1 to 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.
<b>Add VLAN</b>	Select the VLAN that should be mapped to the MSTP instance. The list contains VLAN Name of all the VLANs available in the switch. The mapping of VLAN to the MSTP instance is not done again, if the VLAN is already mapped to that instance.
<b>Delete VLAN</b>	Select the VLAN that should be unmapped from the MSTP instance. The list contains VLAN Name for the VLANs available in the switch. The unmapping of VLAN from the MSTP instance is not done, if the VLAN is already unmapped from that instance.
<b>Mapped VLANs</b>	Displays the VLAN mapped to the MSTP instance.
<b>Flush Indication Threshold</b>	Enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is <b>0</b> .

### 4.2.6.5 Port Settings

This screen 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.

Select	Port	MSTP Instance ID	Port State	Priority	Cost	PseudoRootId Priority	PseudoRootId Address
<input type="radio"/>	Gi0/1	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05
<input type="radio"/>	Gi0/2	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05
<input type="radio"/>	Gi0/3	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05
<input type="radio"/>	Gi0/4	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05
<input type="radio"/>	Gi0/5	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05
<input checked="" type="radio"/>	Gi0/6	1	Enabled <input type="button" value="v"/>	128	200000	32768	00:01:02:03:04:05

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>MSTP (Instance ID)</b>	Displays an integer value that is used to uniquely identify an instance of the MSTP. This value ranges from 1 to 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.
<b>Port State</b>	Select the status of the MSTP in the port. The options are: <ul style="list-style-type: none"> <li>– Enabled – Enables MSTP in the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data.</li> <li>– 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.</li> </ul>
<b>Priority</b>	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 from 0 to 240. The default value is <b>128</b> . This value should be set in increments of 16, eg, 0, 16, 32, 48 and so on.
<b>Cost</b>	Enter the cost that contributes to the path cost of paths containing the port. The paths' path cost is used during

	<p>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 from 0 to 200000000. The default value is <b>200000</b> for all physical ports and <b>199999</b> for port channels.</p>
<b>PseudoRootID Priority</b>	<p>Enter the priority of the pseudo root. This value is used by port configured as L2GP (that is, the field <b>Layer2-Gateway Port</b> is set as <b>True</b>). This value ranges from 0 to 61440. The default value is <b>32768</b>. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.</p>
<b>PseudoRootId Address</b>	<p>Enter the unicast MAC address of the pseudo root. This value is used by port configured as L2GP (the field <b>Layer2- Gateway Port</b> is set as <b>True</b>). The default value is <b>00:08:02:03:04:01</b>.</p>

#### 4.2.6.6 CIST Port Status

This screen allows the user to view information maintained by every port of the switch for CIST.

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
Gi0/1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled
Gi0/7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	0	Disabled	Disabled

Label	Description
<b>Port</b>	<p>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).</p>
<b>Designated Root</b>	<p>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.</p>
<b>Root priority</b>	<p>Displays the Bridge Priority that represents the priority of the bridge recorded as the CIST root in the configuration BPDUs transmitted. This value ranges from 0 to 61440. The default value is <b>32768</b>.</p>
<b>Designated Bridge</b>	<p>Displays the unique identifier of the bridge, which the port</p>

	<p>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.</p>
<b>Designated Port</b>	<p>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.</p>
<b>Designated Cost</b>	<p>Displays the Path Cost of the Designated Port of the segment connected to the port. This value ranges from 1 to 200000000.</p>
<b>Regional Root</b>	<p>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</p>
<b>Regional Root Priority</b>	<p>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 from 0 to 61440. The default value is <b>32768</b>.</p>
<b>Regional Path Cost</b>	<p>Displays the port's Path Cost that contributes to the cost of paths (including the port) towards the CIST Regional Root. This value ranges from 1 to 200000000.</p>
<b>Type</b>	<p>Displays the operational Point-to-Point Status of the LAN segment attached to the port. The values can be:</p> <ul style="list-style-type: none"> <li>– PointtoPoint – Port is treated as if it is connected to a point-to-point link.</li> <li>– SharedLan – Port is treated as if it is having a shared media connection.</li> </ul>
<b>Role</b>	<p>Displays the current role of the port for the spanning tree instance. The values can be:</p> <ul style="list-style-type: none"> <li>– Disabled – Port is disabled manually (<b>Port State</b>) or automatically (Link status in <b>Layer2 Management &gt; Port Manager &gt; Basic Settings</b>). It does not take part in the spanning tree process.</li> <li>– Alternate – Port acting as an alternate for the root port, is blocked and not used for traffic. It is enabled and declared</li> </ul>



	<p>as the root port, if the current root port is blocked.</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Root – Port is used to forward data to root bridge directly or through an upstream LAN segment.</li> <li>- 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.</li> </ul>
<p><b>Port State</b></p>	<p>Displays the current state of the port as defined by the common STP. The values can be:</p> <ul style="list-style-type: none"> <li>- Disabled – Port is disabled manually (Port State) or automatically (Link). It does not take part in the spanning tree process.</li> <li>- Discarding – Port is included in the STP process and is ready to learn addresses and forward data.</li> <li>- 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.</li> <li>- Forwarding – Port is sending and receiving data based on the formed spanning tree topology which is loop free.</li> </ul>

### 4.2.6.7 Bridge Priority

This screen allows the user to configure the bridge priority to be assigned for the specified VLAN.

Select	MSTP Instance ID	Root	Bridge Priority	Bridge Cost	Root Port
<input type="radio"/>	1	<input type="text" value=""/>	0	0	0
<input type="radio"/>	2	<input type="text" value=""/>	32768	0	0
<input checked="" type="radio"/>	15	<input type="text" value=""/>	32768	0	0

Label	Description
<b>Select</b>	Select the MSTP Instance ID for which the configuration needs to be applied.
<b>MSTP Instance ID</b>	Displays the integer value that uniquely identifies an instance of the MSTP. This value ranges from 1 to 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.
<b>Root</b>	Select the root type for the given vlan interface. The options are; <ul style="list-style-type: none"> <li>– primary - Configures the switch to become root for a given VLAN. The priority of the switch is lowered until it becomes root.</li> <li>– secondary - Configures the switch to become backup root for a given VLAN. The priority of the switch is lowered until it becomes one priority higher than the root, so it can become root if the current root fails.</li> </ul>
<b>Bridge Priority</b>	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 from 0 to 61440. The Default value is <b>32768</b> . The value should be set in increments of 4096, For eg, 0, 4096, 8192, 12288 and so on.
<b>Bridge Cost</b>	Displays the Cost of the path to the MSTI Regional Root seen by this bridge. This is a read-only field.
<b>Root Port</b>	Displays the Port Number of the Port which offers the lowest path cost from this bridge to the CIST Root Bridge. This is a read-only field.

## 4.2.7 RSTP

RSTP (Rapid Spanning Tree Protocol) is a portable implementation of the IEEE 802.1D standard. It provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. It reduces the time to reconfigure the active topology of the network when physical topology or topology configuration parameters changes. It provides increased availability of MAC service when there is a reconfiguration or failure of components in a bridged LAN. It can inter-operate with legacy STP bridges without any change in the configuration.

### 4.2.7.1 Global Settings

Select	Context Id	System Control	Status	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
<input type="radio"/>	0	Shutdown	Disabled	False	False	0	0	

Label	Description
<b>Select</b>	Click to select the context for which the configuration needs to be applied.
<b>Context ID</b>	Specifies the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>System Control</b>	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. The default option is <b>Shutdown</b> . The options are: <ul style="list-style-type: none"> <li>– Start – Activates the RSTP feature in the switch on all ports. The required memory is allocated for the feature.</li> <li>– Shutdown – Stops the RSTP feature in the switch on all ports. The allocated memory is released and made available for other activities.</li> </ul>
<b>Status</b>	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. The default option is <b>Disabled</b> . The options are: <ul style="list-style-type: none"> <li>– Enabled – Enables the RSTP feature in the switch on all ports.</li> <li>– Disabled – Disables the RSTP feature in the switch on all ports.</li> </ul>
<b>Dynamic Path Cost Calculation</b>	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

	<p>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. The default option is <b>False</b>.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>– True – Dynamically calculates path cost based on the speed of the ports whose <b>Admin State</b> is set as <b>Up</b> at that time. The path cost is not changed based on the operational status of the ports, once calculated.</li> <li>– False – Dynamically calculates path cost based on the link speed at the time of port creation.</li> </ul>
<b>Speed Change Path Cost Calculation</b>	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– False – Does not dynamically calculate the path cost for ports based their speed at that time.</li> </ul>
<b>Flush Interval</b>	<p>Enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is <b>0</b>.</p>
<b>Flush Indication Threshold</b>	<p>Enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is <b>0</b>.</p>
<b>BPDU Guard</b>	<p>Set the port to none will enable the switch to monitor edge ports and disable them if they receive BPDU packets.</p>

#### 4.2.7.2 Basic Settings

This screen 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

Select	Context Id	Priority	Version	Tx Hold Count	Max Age	Hello Time	Forward Delay
<input type="radio"/>	0	32768	RSTP Compatible	6	20	2	15
<input checked="" type="radio"/>	1	32768	RSTP Compatible	6	20	2	15

Label	Description
<b>Select</b>	Click to select the context for which the configuration needs to be done.
<b>Context ID</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is <b>0</b> .
<b>Priority</b>	Enter the priority value that is assigned to the switch. This value is used during the election of root. This value ranges from 0 to 61440. The default value is <b>32768</b> . The value should be set in steps of 4096, eg,0, 4096, 8192, 12288 and so on.
<b>Version</b>	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. The default option is <b>RSTP Compatible</b> . The options are: <ul style="list-style-type: none"> <li>– STP Compatible – Removes the loop using the STP specified in IEEE 802.1D.</li> <li>– RSTP Compatible – Removes the loop using the RSTP specified in IEEE 802.1w</li> </ul>
<b>Tx Hold Count</b>	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 from 1 to 10. The default value is <b>6</b> .
<b>Max Age</b>	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 BPDU is valid. This value ranges from 6 to 40 seconds. The default value is <b>20</b> seconds.
<b>Hellow Time</b>	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. The default value is <b>2</b> seconds
<b>Forward Delay</b>	Enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state. This value ranges from 4 to 30 seconds. The default value is <b>15</b> seconds.

### 4.2.7.3 Port Settings

This screen allows the user to configure the port information for RSTP used during computation of loop-free topology

Select	Port	Port Role	Port Priority	RSTP Status	Path Cost	Protocol Migration	Admin Edge Port	Admin Point To Point	Auto Edge Detection	Restricted Role	Restricted TCN	Bpdu Receive	Bpdu Transmit	Layer2 Gateway Port	Loop Guard	Root Guard	Bpdu Guard	Error Recovery
--------	------	-----------	---------------	-------------	-----------	--------------------	-----------------	----------------------	---------------------	-----------------	----------------	--------------	---------------	---------------------	------------	------------	------------	----------------

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Port Role</b>	<p>Displays the current role of the port for the spanning tree. The values can be:</p> <ul style="list-style-type: none"> <li>– Disabled – Port is disabled manually (RSTP Status) or automatically (Link). It does not take part in the spanning tree process.</li> <li>– 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.</li> <li>– 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.</li> <li>– Root – Port is used to forward data to root bridge directly or through an upstream LAN.</li> <li>– Designated – Port is used to send and receive packets to / from a specific downstream LAN segment / device. Only</li> </ul>

	one designated port is assigned for each segment.
<b>Port Priority</b>	Enter the priority value that is assigned to the port. This value is used during the <b>Port Role</b> Selection process. This value ranges from 0 to 240. The default value is <b>128</b> . This value should be set in steps of 16, eg 0, 16, 32, 48 and so on
<b>RSTP Status</b>	Select the RSTP status of the port. The default option is <b>Enable</b> . The options are: <ul style="list-style-type: none"> <li>– Enable – Enables RSTP in the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data.</li> <li>– 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</li> </ul>
<b>Path Cost</b>	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 root. The path cost represents the distance between the root port and designated port. This value ranges from 0 to 200000000. The default value is <b>20000</b> for all physical ports and <b>199999</b> for port channels.
<b>Protocol Migration</b>	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. The default option is <b>False</b> . The options are: <ul style="list-style-type: none"> <li>– 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.</li> <li>– False – Does not perform protocol migration mechanism. The port always transmits the standard RSTP BPDUs.</li> </ul>
<b>Admin Edge Port</b>	Select the administrative value of the Edge Port parameter. The default option is <b>False</b> . The options are: <ul style="list-style-type: none"> <li>– True – Sets the port as an edge port ( that is, the <b>Port State</b> is immediately set as <b>forwarding</b>). It is connected directly to a single end station. It allows RSTP to converge faster and does not wait to receive BPDUs.</li> <li>– False – Sets the port as a non-Edge port (that is, the</li> </ul>

	<p>spanning tree process is performed using the RSTP). It is connected to a routing device such as switch.</p>
<b>Admin Point-to-Point</b>	<p>Select the administrative point-to-point status of the LAN segment attached to the port. The default option is <b>Auto</b>. The options are:</p> <ul style="list-style-type: none"> <li>– ForceTrue – Always treats the port as if it is connected to a point-to-point link.</li> <li>– ForceFalse – Always treats the port as if it is having a shared media connection.</li> <li>– Auto – Treats the ports as having a shared media connection or a point- point link based on the prevailing conditions.</li> </ul> <p>Port is considered to have a point-to-point link if,</p> <ul style="list-style-type: none"> <li>– It is an aggregator and all of its members can be aggregated.</li> <li>– The MAC entity is configured for full Duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as Auto).</li> </ul> <p>Otherwise port is considered to have a shared media connection</p>
<b>Auto Edge Detection</b>	<p>Select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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 <b>Admin Edge Port</b>, based on the reception of BPDU.</li> <li>– False – Uses the manually configured value for the Edge Port parameter. The value set in the field <b>Admin Edge Port</b> is used for the Edge Port parameter.</li> </ul>
<b>Restricted Role</b>	<p>Select whether the selection of port <b>Role</b> 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</p>



	<p>network from influencing the spanning tree active topology. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– False – Includes all available ports of the topology, in the root selection process to select the root.</li> </ul>
<b>Restricted TCN</b>	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>– True – Blocks the port from propagating the received topology change notifications and topology changes to other ports.</li> <li>– False – Allows the port to propagate the received topology change notifications and topology changes to other ports.</li> </ul>
<b>Bpdu Receive</b>	<p>Select the processing status of the received RSTP BPDUs. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>– True – Normally processes the RSTP BPDUs received on the port.</li> <li>– False – Discards the RSTP BPDUs received on the port.</li> </ul>
<b>Bpdu Transmit</b>	<p>Select the BPDU transmission status of the port. The default option is <b>True</b>. The options are:</p> <ul style="list-style-type: none"> <li>– True – Transmits the RSTP BPDUs from the port.</li> <li>– False – Blocks the transmission of RSTP BPDUs from the port.</li> </ul>
<b>Layer2-Gateway Port</b>	<p>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 <b>Admin State</b> is set as <b>Up</b>. The default option is <b>false</b>. The options are:</p>

	<ul style="list-style-type: none"> <li>- True – Allows the port to operate as a L2GP.</li> <li>- False – Allows the port to operate as a normal port.</li> </ul>
<b>Loop Guard</b>	<p>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. The default option is <b>False</b>. The options are:</p> <ul style="list-style-type: none"> <li>- True – Enables the loop guard feature in the port.</li> <li>- False – Disables the loop guard feature in the port.</li> </ul>
<b>Root Guard</b>	<p>Select <b>True</b> to enable the root guard function and <b>False</b> to disable it. When root guard is enabled on a port, that port cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an “alternate” port role and enters a blocking state if it receives superior STP BPDUs. Select this option to enable root guard for the port.</p>
<b>Bpdu Guard</b>	<p>Set the port to none will enable the switch to monitor edge ports and disable them if they receive BPDU packets.</p>
<b>Error Recovery</b>	<p>Set the port to recover from an error-disabled state.</p>

#### 4.2.7.4 Port Status

This screen allows the user to view information maintained by every port of the switch for RSTP

Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
Gi0/1	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Disabled
Gi0/2	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Disabled
Gi0/3	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Disabled
Gi0/4	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Disabled

Label	Description
<b>Port</b>	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).
<b>Designated Root</b>	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.
<b>Designated Cost</b>	Displays the <b>Path Cost</b> of the <b>Designated Port</b> of the segment connected to the port. This value ranges from 1 to 200000000.
<b>Designated Bridge</b>	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.
<b>Designated Port</b>	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.
<b>Type</b>	Displays the operational Admin Point to Point of the LAN segment attached to the port. The values can be: <ul style="list-style-type: none"> <li>– Point-to-Point – Port is treated as if it is connected to a point-to-point link.</li> <li>– SharedLan – Port is treated as if it is having a shared media connection.</li> </ul>
<b>Role</b>	Displays the current role of the port for the spanning tree instance. The values can be: <ul style="list-style-type: none"> <li>– Disabled – Port is disabled manually (<b>RSTP Status</b>) or automatically (Link status in <b>Layer2 Management &gt; Port Manager &gt; Basic Settings</b>). It does not take part in the spanning tree process.</li> <li>– 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.</li> <li>– 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.</li> <li>– Root – Port is used to forward data to root bridge directly or through an upstream LAN segment.</li> <li>– Designated – Port is used to send and receive packets to/from a specific downstream LAN segment/device. Only</li> </ul>

	one designated port is assigned for each segment.
<b>Port State</b>	<p>Displays the current state of the port as defined by the STP.</p> <p>The values can be:</p> <ul style="list-style-type: none"> <li>- Disabled – Port is disabled manually (<b>RSTP Status</b>) or automatically ((Link status in <b>Layer2 Management &gt; Port Manager &gt; Basic Settings</b>). It does not take part in the spanning tree process.</li> <li>- Discarding – Port is included in the STP process and is ready to learn addresses and forward data.</li> <li>- 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.</li> <li>- Forwarding – Port is sending and receiving data based on the formed spanning tree topology which is loop free.</li> </ul>

## 4.2.8 Link Aggregation

LA (Link Aggregation) implements the LA functionality as per the IEEE 802.3ad standard. LA feature allows the user to aggregate individual point- to-point links into a LA group. A MAC client treats the LA group as a single link. The total capacity of the LA group is the sum of the capacities of the individual links present in the group. The LA group provides increased bandwidth for the traffic between the hosts and the server, and does not affect the traffic if any of the links is made down.

LA feature is supported only in point-to-point links, with MACs operating in full Duplex mode. All the links in a LA group should work at the same data rate (that is, Speed should be same).

### 4.2.8.1 Basic Settings

This screen allows the user to configure the LA module parameters that are used globally in the switch for all ports available in the switch

System Control	Start
LA Status	Disabled
System Priority	32768
System ID	00:00:00:00:00:00
LA Independent Mode	Disabled

Label	Description
-------	-------------

<b>System Control</b>	<p>Select the system control status of the LA in the switch. The default option is <b>Start</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Start – Starts the LA module and allocates the resources required by the LA module.</li> <li>– Shutdown – Shuts down the LA module and releases the allocated resources to the system.</li> </ul>
<b>LA Status</b>	<p>Select the administrative status of the LA module. LA feature allows the user to aggregate individual point-to-point links into a LAgroup. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables LA in the switch on all ports. The LA is enabled in the switch, only if the LA <b>System Control</b> is set as <b>start</b>.</li> <li>– Disabled – Disables LA in the switch on all ports.</li> </ul>
<b>System Priority</b>	<p>Enter the priority value associated with the actor’s system ID. This value ranges from 0 to 65535. The default value is <b>32768</b>.</p>
<b>System ID</b>	<p>Enter 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the aggregator. The default value is <b>00:01:02:03:04:01</b>.</p>
<b>LA Independent Mode</b>	<p>Select the independent mode of the LA module.</p> <p>The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables to operate the member ports of the port-channel as independent ports and allows the ports to be visible to higher layers.</li> <li>– Disabled – Disables the ports from visibility to higher layers and sets the member ports of the port-channel operationally up.</li> </ul>

#### 4.2.8.2 Interface Settings

This screen allows the user to create port channel (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.

Port Channel ID	<input type="text"/>	*
Context	<input type="button" value="v"/>	*
Admin Status	Up	<input type="button" value="v"/>
MTU	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Context	PortChannel ID	Admin State	Oper State	MTU
--------	---------	----------------	-------------	------------	-----

Label	Description
<b>Port Channel ID</b>	Enter the identifier that uniquely identifies a port channel to be created in the switch. This value ranges from 1 to 65535.
<b>Context</b>	Select the virtual context ID that uniquely represents a virtual switch created in the physical switch.
<b>Admin Status</b>	Select the desired admin status of the port channel. The default option is <b>Up</b> . The list contains: <ul style="list-style-type: none"> <li>- Up – Allows the port channel to be available for aggregating the ports and to transmit/receive traffic.</li> <li>- Down – Blocks the availability of the port channel for aggregating the ports and the transmission/reception of the traffic.</li> </ul>
<b>MTU</b>	Displays the current operational status of the port channel. This is a read only field. The list contains: <ul style="list-style-type: none"> <li>- Up – Port channel is available for aggregating ports and for transmission/reception traffic.</li> <li>- Down – Port channel availability for aggregating ports and for transmission/reception of traffic is blocked.</li> </ul>
<b>Select</b>	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. The default value is <b>1500</b> . This value ranges from 46 to 9216.

### 4.2.8.3 Port Channel Settings

This screen 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 **Port Channel Interface Basic Settings** screen

Context	Port Channel	Ports	NoOf Ports Per Channel	NoOf HotstandBy Ports	Default Port	Aggregator MAC	Max Ports	D-LAG Distributing Port/Port List	D-LAG System ID	D-LAG System Priority	D-LAG Periodic sync time	D-LAG Master selection wait time	D-LAG Status	D-LAG Redundancy	D-LAG Role Played	D-LAG Max Keep Alive Count	D-LAG Periodic Sync Pdu Tx count	D-LAG Periodic Sync Pdu Rx count	D-LAG Event update Pdu Tx count	D-LAG Event update Pdu Rx count	D-LAG Elected as Master count	D-LAG Elected as Slave count	D-LAG Trap count
---------	--------------	-------	------------------------	-----------------------	--------------	----------------	-----------	-----------------------------------	-----------------	-----------------------	--------------------------	----------------------------------	--------------	------------------	-------------------	----------------------------	----------------------------------	----------------------------------	---------------------------------	---------------------------------	-------------------------------	------------------------------	------------------

Label	Description
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch.
<b>Port Channel ID</b>	Select the port channel identifier from the list already specified in the system, to which the ports should be aggregated or from which aggregated ports should be removed. The list contains the port channels created in the <b>Port Channel Interface Basic Settings</b> screen.
<b>Aggregation Type</b>	Select the type of aggregation to be used in the port channel. The default option is <b>Static</b> for all the ports and <b>Dynamic</b> for the port configured as a default Port of the port channel. The list contains: <ul style="list-style-type: none"> <li>– <b>Static</b> – 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. The port channel should be manually assigned with its member ports.</li> <li>– <b>Dynamic</b> – 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).</li> </ul>
<b>Action Type</b>	Select the action to be performed for the Ports configured in this

	<p>screen. The default option is <b>Add</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Add – Aggregates the mentioned Ports and configures them as a member for the selected Port Channel ID.</li> <li>– Delete – Removes the mentioned Ports from the member list created for the selected Port Channel ID.</li> </ul>
<b>Mode</b>	<p>Select the operating mode to be set for the port channel. The default option is <b>Lacp</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Lacp – Sets the port channel into passive negotiation state, in which the port channel waits for its peer to initiate negotiation.</li> <li>– Manual – Sets/forces the port channel to enable channeling without waiting for its peer to start negotiation.</li> <li>– Disable – Disables the channeling, the LACP feature is disabled in the port channel.</li> </ul>
<b>Ports</b>	<p>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 &lt;interface type&gt;&lt;slot number/port number&gt;. There is no space needed between these two entries.</p>
<b>No Of Ports Per Channel</b>	<p>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 <b>Ports</b> is entered as gi0/4,gi0/7,gi0/8.</p>
<b>No Of HotstandBy Ports</b>	<p>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.</p>
<b>Default Port</b>	<p>Select the port that should be set as default port, which gets attached to the port channel and participates only in dynamic aggregation selection.</p>
<b>Aggregator MAC</b>	<p>Displays the 6-octet MAC address that is assigned to the port channel. This MAC address is automatically assigned to the port channel by RGS-PR9000-A.</p>
<b>Max Ports</b>	<p>Enter the maximum number of ports that can be attached to the port-channel. This value ranges from 2 to 8. The default value is</p>



	<p><b>8.</b> 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 <b>Port Identifier</b> and <b>Port Priority</b>.</p>
<b>D-LAG Distributing Port/Port List</b>	<p>Enter the distributing port/ports on which D-LAG periodic-sync and D-LAG event-update messages will be sent/received for D-LAG internal communication between the D-LAG nodes. Ports which are already part of Port channel should not be configured as Distributing port. D-LAG node should immediately detect and handle distributing port failure with high priority and allow load to be carried on the all the configured ports. 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 &lt;interface type&gt;&lt;slot number/port number&gt;. There is no space between these two entries. For D-LAG Distributing Port and port list, the format is &lt;interface type&gt;&lt;slot number/port number&gt;. There is no space between these two entries.</p>
<b>D-LAG System ID</b>	<p>D-LAG System ID - Enter 6-octet unicast MAC address value to configure the System ID in D-LAG nodes which is used for communicating with the peer node system when D-LAG status is enabled, where the value is used as a unique identifier.</p>
<b>D-LAG System Priority</b>	<p>Enter system priority in D-LAG nodes which is to be used for communicating with the peer node when D-LAG status is enabled. The value of system priority ranges from 0 to 65535. The default value is <b>32768</b>.</p>
<b>D-LAG Periodic Sync Time</b>	<p>Enter the D-LAG periodic sync timer used in Distributed Link Aggregation. Periodic sync timer is used to configure the transmission interval of D-LAG periodic-sync PDUs. Periodic-sync timer will be running individually in each D-LAG node. The configured value of this timer is applicable only from the next start/re-start of the timer. This value ranges from 0 to 90000 ms/(0 to 90 seconds). The default value is <b>1 second (1000 ms)</b>.</p>
<b>D-LAG MS Selection Wait Time</b>	<p>Enter the period for the master slave selection wait timer used in Distributed Link Aggregation. The value of MS selection Wait</p>

	Time ranges between 0 and 90 seconds. The default value is <b>0 second</b> .
<b>D-LAG Status</b>	Select the distributed link aggregation status. The status can be modified irrespective of whether corresponding port-channel is enabled or disabled. The default option is <b>Disabled</b> . The options are: <ul style="list-style-type: none"> <li>– Enabled – Enables load sharing functionality in D-LAG nodes.</li> <li>– Disabled – Disables the D-LAG load sharing functionality in the D-LAG node and will not change/reset the value of this field but configuring this object to disabled</li> </ul>
<b>D-LAG Redundancy</b>	Select the redundancy feature in D-LAG node. The status can be modified irrespective of whether corresponding port-channel is enabled or disabled. The default option is <b>off</b> . The list contains; <ul style="list-style-type: none"> <li>– On: Enables the redundancy feature in D-LAG node. when enabled, master-slave-selection algorithm can be used to select master/slave/backup-master</li> <li>– Off: Disables the redundancy feature in DLAG node.</li> </ul>
<b>DLAG Max Keep Alive Count</b>	Displays the keep alive count of the D- LAG node. D-LAG node will have a Max Keep alive count and each D-LAG node maintains separate keep alive counts for all other remote D-LAG nodes. This value ranges from 0 to 5. The default value is <b>3</b> .
<b>DLAG Periodic Sync Pdu Tx Count</b>	Displays the number of periodic- sync PDUs sent on the distributing port. The default value is <b>0</b> .
<b>DLAG Periodic Sync Pdu Rx Count</b>	Displays the number of periodic- sync PDUs received on the distributing port. The default value is <b>0</b> .
<b>DLAG Event Update Pdu Tx Count</b>	Displays the number of event update PDUs sent on the distributing port. The default value is <b>0</b> .
<b>DLAG Event Update Pdu Rx Count</b>	Displays the number of event update PDUs recieved on the distributing port. The default value is <b>0</b> .
<b>DLAG Elected As Master Count</b>	Displays the number of times the port- channel has been selected as master. The default value is <b>0</b> . This field is used when distributing feature and redundancy feature both are

	enabled in a D-LAG node.
<b>DLAG Elected As Slave Count</b>	Displays the number of times the port-channel has been selected as slave. This object is used when Distributing feature and redundancy feature both are enabled in a D-LAG node. The default value is <b>0</b> .
<b>DLAG Trap count</b>	Displays the number of trap messages sent from the port-channel. The default value is <b>0</b> .

### 4.2.8.4 Protocol Group

This screen 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

Select	Port	Port Priority	Port Identifier	Mode	Activity	Timeout	Wait Time (secs)	Bundle State	Aggregation Selection
<input type="radio"/>	Gi0/1	128	1	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/2	128	2	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/3	128	3	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/4	128	4	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/5	128	5	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/6	128	6	Disable		Short	200	Down	Static
<input type="radio"/>	Gi0/7	128	7	Disable		Short	200	Down	Static

Label	Description
<b>Port</b>	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).
<b>Port Priority</b>	Enter the priority value assigned to the aggregation port. This value is used in combination with <b>Port Identifier</b> during the identification of best ports in the port channel. This value ranges from 0 to 65535. The default value is <b>128</b> .
<b>Port Identifier</b>	Enter the port number that represents the concerned aggregation port. This number is communicated as the Actor_Port in LACPDU. This value ranges from 1 to 65535.
<b>Mode</b>	Select the operating mode to be set for the port. By default, the configuration set in the field <b>Mode</b> in the screen <b>LA Port Channel Basic Settings</b> is displayed. The list contains: <ul style="list-style-type: none"> <li>– LACP – Places the port into passive negotiation state, in which the port waits for its peer to initiate negotiation.</li> </ul>

	<ul style="list-style-type: none"> <li>– On – Forces the port to enable channeling without waiting for its peer to start negotiation.</li> <li>– Disable – Disables the channeling, that is, the LACP feature is disabled in the port.</li> </ul>
<b>Activity</b>	<p>Select the LACP activity for the port. The list contains:</p> <ul style="list-style-type: none"> <li>– Active – Generates LACPDU without waiting for any LACPDU from the partner port.</li> <li>– Passive – Generates LACPDU only when an LACPDU is received from the partner port.</li> </ul>
<b>Timeout</b>	<p>Select the time within which LACPDUs should be received on a port to avoid timing out of the aggregated link. The default option is <b>Long</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Short – Sets the value as 3 seconds for the port to time out of the port channel. LACP PDU is sent every second.</li> <li>– Long – Sets the value as 90 seconds for the port to time out of the port channel. The LACP PDU is sent every 30 seconds.</li> </ul>
<b>Wait Time (secs)</b>	<p>Enter the waiting time for a port after receiving partner information and before entering aggregation (the time taken to attach to the port channel). This value ranges from 0 to 10 seconds. The default value is <b>2</b> seconds.</p>
<b>Bundle State</b>	<p>Displays the current state of the port with respect to LA. This field is read only.</p> <ul style="list-style-type: none"> <li>– Up In Bundle – Specifies that the port is an active member of the port channel. The port is operationally up and actively takes part in aggregation.</li> <li>– Standby – Specifies that 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.</li> <li>– Down – Specifies that 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.</li> </ul>

	<ul style="list-style-type: none"> <li>– Up Individual – Specifies that the port is operating individually and is not taking part in aggregation.</li> </ul>
<b>Aggregation Selection</b>	<p>Displays the type of aggregation in which the port participates. The default option is <b>Static</b> for all the ports and <b>Dynamic</b> for the port configured as a <b>Default Port</b> of the port channel. This field is read only.</p> <ul style="list-style-type: none"> <li>– 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 <b>LA Port Channel Settings</b> screen.</li> <li>– 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 <b>System ID</b> and Admin key (that is, <b>Port Channel ID</b>).</li> </ul>

### 4.2.8.5 Port Settings

This screen allows the user to view the aggregation state of the port channels created in the switch through the Port Channel Interface Basic Settings screen.

Port Channel	Port No	Aggregation State
1	Gi0/1	Aggregation, Sync, Collecting, Distributing, Defaulted

Label	Description
<b>Port Channel</b>	Displays the identifier that uniquely identifies a port channel created in the switch. This value ranges from 1 to 65535.
<b>Port No</b>	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).
<b>Aggregation State</b>	<p>Displays the actor state as transmitted by the actor in LACPDU. The state can be:</p> <ul style="list-style-type: none"> <li>– Aggregation – Sets the port as a potential candidate for aggregation.</li> <li>– Individual – Does not sets the port from aggregation. It can be operated only as an individual link.</li> </ul>

	<ul style="list-style-type: none"> <li>- Sync – Allocates the port to the correct LA group which is associated with a compatible port channel whose identity is consistent with the Actor System ID and Admin key (Port Channel ID). The system ID and admin key are in sync with partner information.</li> <li>- Collecting – Enables the port to collect incoming frames and is not expected to be disabled in the absence of administrative changes or changes in received protocol information.</li> <li>- Distributing – Enables the port to distribute outgoing frames.</li> <li>- Defaulted – Sets the port’s receive machine to use the defaulted operational partner information that is administratively configured for the partner.</li> <li>- Expired – Sets the port’s receive machine in expired state. The receive machine state is changed as expired, if the PDUs are not received from partner for certain time period.</li> </ul>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.8.6 Load Balancing

This screen allows the user to configure the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing.

Select	Port Channel	Selection Policy
<input type="radio"/>	<input type="text" value="1"/>	<input type="checkbox"/> MAC Source <input type="checkbox"/> MAC Destination <input type="checkbox"/> MAC Source and Destination <input type="checkbox"/> IP Source <input type="checkbox"/> IP Destination <input type="checkbox"/> IP Source and Destination <input type="checkbox"/> Vlan ID <input type="checkbox"/> ISID <input type="checkbox"/> MAC Source Vlan ID <input type="checkbox"/> MAC Destination Vlan ID <input type="checkbox"/> MAC Source and Destination Vlan ID <input type="checkbox"/> MPLS VC Label <input checked="" type="checkbox"/> MPLS Tunnel Label <input type="checkbox"/> MPLS VC and Tunnel Label <input type="checkbox"/> Ipv6 Source <input type="checkbox"/> Ipv6 Destination <input type="checkbox"/> L3 Protocol <input type="checkbox"/> Source L4 Port <input type="checkbox"/> Destination L4 Port

Label	Description
<b>Select</b>	Click to select the port channel for which the configuration needs to be done.
<b>Port Channel</b>	Displays the identifier that uniquely identifies a port channel created in the switch. This value ranges from 1 to 65535.
<b>Selection Policy</b>	Select the rule for distributing the Ethernet traffic. The default option is <b>MAC Source and Destination</b> . The options are: <ul style="list-style-type: none"> <li>- MAC Source – Uses the bits of the source MAC address in</li> </ul>

	<p>the packet to select the port in which the traffic should flow.</p> <ul style="list-style-type: none"> <li>– MAC Destination – Uses the bits of the destination MAC address in the packet to select the port in which the traffic should flow.</li> <li>– 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.</li> <li>– IP Source – Uses the bits of the source IP address in the packet to select the port in which the traffic should flow.</li> <li>– IP Destination – Uses the bits of the destination IP address in the packet to select the port in which the traffic should flow.</li> <li>– 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.</li> <li>– VLAN ID – Uses the VLAN ID in the packet to select the port in which the traffic should flow.</li> <li>– ISID – Uses the ISID in the packet to select the port in which the traffic should flow.</li> <li>– 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.</li> <li>– 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.</li> <li>– 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.</li> <li>– MPLS VC Label – Uses the MPLS VC label in the packet to select the port in which the traffic should flow.</li> <li>– MPLS Tunnel Label – Uses the MPLS tunnel label in the packet to select the port in which the traffic should flow.</li> <li>– MPLS VC and Tunnel Label – Uses the MPLS VC and tunnel labels in the packet to select the port in which the</li> </ul>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>traffic should flow.</p> <ul style="list-style-type: none"> <li>- Ipv6 Source – Uses the bits of the source Ipv6 address in the packet to select the port in which the traffic should flow.</li> <li>- Ipv6 Destination – Uses the bits of the destination Ipv6 address in the packet to select the port in which the traffic should flow.</li> <li>- L3 Protocol – Uses the frames of the L3 IP header in the packet to select the port in which the traffic should flow.</li> <li>- Source L4 Port – Uses the bits of L4 source port specified in L4 header (TCP/UDP port) in the packet to select the port in which the traffic should flow.</li> <li>- Destination L4 Port – Uses the bits of L4 destination port specified in L4 header (TCP/UDP port) in the packet to select the port in which the traffic should flow.</li> </ul>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### 4.2.8.7 DLAG Remote Port Channel Settings

This screen allows the user to view the details of all remote port-channels that are part of same D-LAG

Port Channel Index	DLAG SystemID	DLAG System Priority	DLAG Role Played	DLAG Keep Alive Count
65	00:02:02:03:04:01	32768	None	0

Label	Description
<b>Port Channel Index</b>	Displays the index of the remote port-channel( Remote Aggregator's interface index)
<b>DLAG SystemID</b>	Displays the 6-octet MAC address value of each remote D-LAG node, which uniquely identifies the remote and displays the system ID in D-LAG nodes which is used for communicating with the peer node
<b>DLAG System Priority</b>	Displays the stored system priority of each remote D-LAG node
<b>DLAG Role Played</b>	Displays system priority in D-LAG nodes which is to be used for communicating with the peer node when D-LAG status is enabled. The list contains; <ul style="list-style-type: none"> <li>- none – Specifies the role by the remote D-LAG node as</li> </ul>



	<p>none.</p> <ul style="list-style-type: none"> <li>- Master - Specifies the role by the remote D-LAG node as master.</li> <li>- slave - Specifies the role by the remote D-LAG node as slave.</li> <li>- backupmaster - Specifies the role by the remote D-LAG node as backup- master</li> </ul>
<b>DLAG Keep Alive Count</b>	<p>Displays the keep alive count when D-LAG status is enabled. Each D-LAG node will have a Max Keep alive count and each D-LAG node maintains separate keep alive counts for all other remote D-LAG nodes. The default value is <b>3</b>.</p>

#### 4.2.8.8 DLAG Remote Port Settings

This screen is used to access the stored port list information of each remote D-LAG node

Port Channel Index	DLAG SystemID	DLAG Remote Port Index	DLAG Remote Port Bundle State	DLAG Remote Port Sync Status
65	00:02:02:03:04:01	2	upInBndl	In Sync
65	00:02:02:03:04:01	3	upInBndl	In Sync

Label	Description
<b>Port Channel Index</b>	Displays the if Index of the remote port-channel( Remote Aggregator's interface index)
<b>DLAG SystemID</b>	Displays the 6-octet MAC address value of each remote D-LAG node, which uniquely identifies the remote
<b>DLAG Remote Port Index</b>	The remote D-LAG Node contains the ports that are part of the remote port channel. This field displays the index of each port belonging to the remote D-LAG node.
<b>DLAG Remote Port Bundle State</b>	<p>Displays port bundle states of each port belonging to the remote D-LAG node. The list contains;</p> <ul style="list-style-type: none"> <li>- upInBndl - Sets the port operationally up and actively takes part in aggregation.</li> <li>- standby - Sets the port which is capable of joining in aggregation group, when any of the ports in aggregation group goes down.</li> </ul>

	<ul style="list-style-type: none"> <li>- down - Sets the port 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.</li> <li>- upIndividual - Sets the port to operate individually and is not taking part in aggregation.</li> </ul>
<b>DLAG Remote Port Sync Status</b>	Displays the current sync status of each port belonging to the remote D-LAG node. <ul style="list-style-type: none"> <li>- inSync - Sync status of the port belonging to D-LAG node is inSync.</li> <li>- outofSync - Sync status of the port belonging to D-LAG node is out-of- sync</li> </ul>

## 4.2.9 LLDP

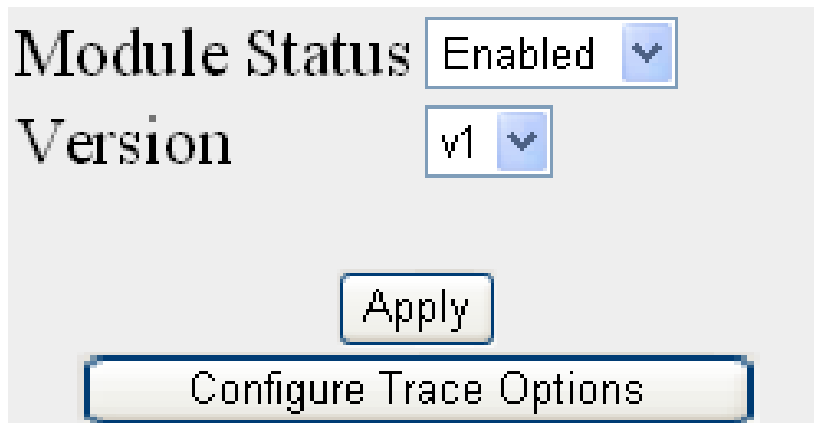
LLDP (Link Layer Discovery Protocol) is a vendor-neutral Data Link Layer protocol used by network devices for advertising their identity, capabilities, and interconnections on an IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document 802.1AB.

LLDP performs functions similar to several proprietary protocols, such as Cisco Discovery Protocol, Extreme Discovery Protocol, Nortel Discovery Protocol (also known as SONMP), and Microsoft's LLTD (Link Layer Topology Discovery).

Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. The topology of an LLDP-enabled network can be discovered by crawling the hosts and querying this database.

### 4.2.9.1 Global Settings

This screen allows the user to enable or disable LLDP module globally and set the LLDP version number.



Label	Description
<b>Module Status</b>	<p>Select the administrative module status of LLDP module. The list contains.</p> <ul style="list-style-type: none"> <li>- Enabled - Indicates that LLDP is enabled in the device and can be enabled port-wise</li> <li>- Disabled - Indicates that LLDP is disabled in the device and also disabled on all ports.</li> </ul>
<b>Version</b>	<p>Select the Version of LLDP to be used on the system. The default option is <b>v1(Version 1)</b>. The list contains;</p> <ul style="list-style-type: none"> <li>- v1 - Enables LLDP version 1 (2005) on the port. When V1 is enabled the port can be assigned with only one MAC address.</li> <li>- 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</li> </ul>

### 4.2.9.2 Port Settings

This screen allows the user to configure the LLDP basic parameters.

Transmit Interval	<input type="text" value="30"/>
Holdtime Multiplier	<input type="text" value="4"/>
Reinitialization Delay	<input type="text" value="2"/>
Tx Delay	<input type="text" value="2"/>
Notification Interval	<input type="text" value="5"/>
Chassis ID Subtype	<input type="text" value="Mac Address"/>
Chassis ID	<input type="text" value="00:1e:94:00:00:01"/>
txCreditMax	<input type="text" value="1"/>
MessageFastTx	<input type="text" value="30"/>
TxFastInit	<input type="text" value="1"/>

Label	Description
<b>Transmit Interval</b>	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. The default value is <b>30</b> seconds.
<b>Holdtime Multiplier</b>	<p>Enter the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. This value ranges from 2 to 10. The default value is <b>4</b>. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula:</p> $TTL = \min (65535, \text{Transmit Interval} * \text{Holdtime Multiplier}).$ <p>For example.</p> <p>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.</p> <p>The value of this object must be restored from non-volatile storage after a re- initialization of the management system.</p>
<b>Reinitialization Delay</b>	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. The default value is <b>2</b> seconds.
<b>Tx Delay</b>	Enter the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems objects. This value ranges from 1 to 8192. The value should be lesser than or equal to (0.25 * Transmit Interval) The default value is <b>2</b> seconds.
<b>Notification Interval</b>	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. The default value is <b>5</b> .
<b>Chassis ID Subtype</b>	<p>Select the source of a chassis identifier. The default option is <b>Mac Address</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Chassis Component - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component</li> <li>– Interface Alias - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.</li> <li>– Port Component - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.</li> <li>– Mac Address - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.</li> <li>– 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.</li> </ul>

	<ul style="list-style-type: none"> <li>Interface Name - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.</li> <li>Local - Represents a chassis identifier based on a locally defined value.</li> </ul>
<b>Chassis ID</b>	Enter the chassis identifier string.
<b>txCreditMax</b>	Enter the maximum number of consecutive LLDPDU's that can be transmitted any time by the port. This value ranges from 1 to 10. The default value is <b>1</b> for LLDP Version v1 and <b>5</b> for LLDP Version v2
<b>MessageFastTX</b>	Enter the interval at which LLDP frames are transmitted on behalf of LLDP agent during fast transmission period. This value ranges from 1 to 3600 seconds. The default value is <b>30</b> for LLDP Version v1 and <b>1</b> for LLDP Version v2.
<b>TxFastInit</b>	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 from 1 to 8. The default value is <b>1</b> for LLDP Version v1 and <b>4</b> for LLDP Version v2.

### 4.2.9.3 Interfaces

This screen allows the user to configure the each ports of the LLDP.

Select	Port	Tx State	Rx State	Tx SEM State	Rx SEM State	Notification Status	Notification Type	Destination MAC
<input type="radio"/>	Gi0/1	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/2	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/3	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/4	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/5	Enabled	Enabled	Idle	Frame Rx	Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/6	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e
<input type="radio"/>	Gi0/7	Enabled	Enabled	Initialize		Disabled	Mis-config	01:80:c2:00:00:0e

Label	Description
<b>Select</b>	Click to select the port for which the LLDP parameters need to be configured.
<b>Port</b>	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).

<b>Tx State</b>	<p>Select the status of the LLDP PDU transmitter. The default option is <b>Enabled</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Enabled: - Enables transmission of LLDPDU from one of the ports of the server to the LLDP module</li> <li>– Disabled – Disables transmission of LLDPDU from one of the ports of the server to the LLDP module</li> </ul>
<b>Rx State</b>	<p>Select the status of the LLDP PDU receiver. The default option is <b>Enabled</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Enabled: - Enables reception of LLDPDU from one of the ports of the server to the LLDP module</li> <li>– Disabled – Enables reception of LLDPDU from one of the ports of the server to the LLDP module</li> </ul>
<b>Tx SEM State</b>	Displays current status of the TX state event machine
<b>Rx SEM State</b>	Displays current status of the RX state event machine.
<b>Notification Status</b>	<p>Select the notification status to be set. The default option is <b>Disabled</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the notification status.</li> <li>– Disabled - Disables the notification status.</li> </ul>
<b>Notification Type</b>	<p>Select the notification type. The default option is <b>Mis- config</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Remote-Table-Change - LLDP agent sends trap notification to NMS whenever remote table change occurs.</li> <li>– Mis-Config - LLDP agent sends trap notification to NMS whenever mis- configuration is identified.</li> <li>– Both - LLDP agent sends trap notification to NMS whenever remote table change occurs or/and whenever mis-configuration is identified</li> </ul>
<b>Destination MAC</b>	Displays the destination mac-address to be used by the LLDP agent for transmission on this port.

#### 4.2.9.4 Neighbors

This screen allows the user to obtain the information of the adjacent server connected with the LLDP.

Chassis ID	Local Interface	Hold Time	Capability	Port ID
00:1e:94:01:3b:33	Gi0/5	120	B	Port.07

Clear LLDP Neighbors

Label	Description
<b>Chassis ID</b>	Displays the Chassis ID of the peer. This value is a string value with a maximum size of 255
<b>Local Interface</b>	Displays the local port on which the peer information is learnt. This value is a string of maximum size 255
<b>Hold Time</b>	Displays the Hold Time advertised by the peer
<b>Capability</b>	Displays the capabilities advertised by the peer
<b>Port ID</b>	Displays the Port ID advertised by the peer

## 4.2.10 802.1x

802.1x or PNAC provides a means of authenticating devices attached to a bridge port. It prevents access to a port when the authentication fails. 802.1X defines (802.1X) port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

Until the authentication is provided, 802.1X access control allows only EAPOL (Extensible Authentication Protocol Over LAN) traffic through the port. When the authentication is provided, normal traffic is allowed through the port.

### 4.2.10.1 Basic Settings

This screen allows the user to configure Authentication status, Authentication mode and Authentication server type



System Control: Shutdown

802.1x Authentication: Disable

Authentication Mode: Local

RemoteAuthenticationServerType: [Empty]

Network Access Server ID: fsNas1

Protocol Version: 2

Buttons: Apply, Configure Trace Options

Label	Description
<p><b>System Control</b></p>	<p>Select the system control status of the PNAC module. The default option is <b>Start</b>. The options are</p> <ul style="list-style-type: none"> <li>- Start – Starts PNAC Module in the system.           <ul style="list-style-type: none"> <li>▪ Memory Resources required by PNAC module are allocated and PNAC module starts running.</li> <li>▪ Creates Memory pool, spawn the PNAC interface task. Initialize all the global data structures</li> <li>▪ Create a hash table for storing the session nodes for MAC based authorization entries.</li> <li>▪ Creates semaphore for controlling concurrent access to critical databases</li> <li>▪ Initialize the timer sub-module and PNAC Local authentication server module.</li> </ul> </li> <li>- Shutdown – Shuts down PNAC Module           <ul style="list-style-type: none"> <li>▪ All resources used by PNAC module are released to the system and the PNAC module is shut down.</li> <li>▪ Initialize all the PNAC state machines.</li> <li>▪ Deactivates the PNAC Local authentication server module, the timer module. Deletes the memory pool for the PNAC module and free its memory.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>▪ Deletes semaphore used for database access-control.</li> </ul>
<b>802.1x Authentication</b>	<p>Select the status of 802.1x based port security feature in the switch. The default option is <b>Enable</b>. The options are::</p> <ul style="list-style-type: none"> <li>– Enable – Enables 802.1x based port security feature in the switch. The switch initiates authentication and sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.</li> <li>– Disable – Disables 802.1x based port security feature in the switch. EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state</li> </ul>
<b>Authentication Mode</b>	<p>Select the Authentication Server Location. The default option is <b>Local</b>. The options are</p> <ul style="list-style-type: none"> <li>– Remote – Radius server based authentication. It calls the AS client functions to communicate with the remote authentication server.</li> <li>– Local – Provides the authentication service requirements in the local database. It maintains a simple database of users who can be permitted on valid proof to access a set of Authenticator's ports. It calls the service functions of the Local AS</li> </ul>
<b>RemoteAuthenticationServerType</b>	<p>Select the Remote Authentication Server Type. The default option is <b>Radius Server</b>. The options are:</p> <ul style="list-style-type: none"> <li>– Radius Server – Sets the remote authentication server as Radius Server. RADIUS server is responsible for authentication, authorization and maintaining its account information with port-based authentication. It is a gateway that controls access to the network. RADIUS uses the User Datagram Protocol (UDP). RADIUS server acts as the centralized authentication server</li> </ul>

	<ul style="list-style-type: none"> <li>Tacacs Server – Sets the remote authentication server as TACACS Server. The remote TACACS+ server is responsible for TACACS+ client communication to authenticate the user, get authorization information and send accounting information to the user. TACACS+ uses the Transmission Control Protocol (TCP). This feature is currently not supported.</li> </ul>
<b>Network Access Server ID</b>	Enter the Network Access Server ID, It is the server ID for which authentication is provided. The Authenticator ID originates from the Access Request packets. The value is of string type.
<b>Protocol Version</b>	Specifies the Version Number of the Protocol. This is a read-only field.

### 4.2.10.2 Port Settings

Select	Port	Authentication Mode/Host Mode	Auth PortStatus	Supp PortStatus	Access Control	Configured Control Direction	Operational Control Direction	AuthSM State	SuppSM State	Restart Authentication	Authentication Retry Count	Reauth	Authentication Max Start	Reauthentication
--------	------	-------------------------------	-----------------	-----------------	----------------	------------------------------	-------------------------------	--------------	--------------	------------------------	----------------------------	--------	--------------------------	------------------

Label	Description
<b>Select</b>	Select the port for which the configuration needs to be done
<b>Port</b>	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).
<b>Port Control</b>	<p>Select the control values of the Authenticator Port. The Default option is <b>ForceAuthorized</b> The options are:</p> <ul style="list-style-type: none"> <li>ForceAuthorized – Allows all the traffic through this port. Disables 802.1X authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client.</li> <li>ForceUnauthorized – Blocks all the traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client</li> </ul>

	<p>through the interface.</p> <ul style="list-style-type: none"> <li>- Auto – Imposes 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server.</li> </ul>
<p><b>Authentication Mode/Host Mode</b></p>	<p>Select the authentication mode to be imposed on the entry. The Default option is Port Based. The list contains:</p> <ul style="list-style-type: none"> <li>- Port Based/Multi-Host – Authenticates and authorizes devices attached to a Bridge port that has point-to-point connection characteristics named as Port based network access control. The following occurs when Port based authentication is selected             <ul style="list-style-type: none"> <li>▪ Receives incoming tagged/untagged data/control frames from the CFA Module (Interface Manager) and checks if the Port is authorized. If authorized, the frame is passed to the higher layer.</li> <li>▪ Receives outgoing data/control frames from the other modules. If authorized, the frame is passed to the CFA module.</li> <li>▪ When an EAPOL frame is received from CFA, it sends the EAP packet to the PNAC Interface Task, which then passes it to the Authenticator Module or Supplicant Module.</li> <li>▪ It forwards all the received EAPOL-Start, EAPOL-Logoff and EAP-Responses to the Authenticator Module via the PNAC Interface Task.</li> <li>▪ It forwards all the received EAP-Requests, EAP-Success and EAP- Failure to the Supplicant Module</li> </ul> </li> </ul>

	<p>via the PNAC Interface Task.</p> <ul style="list-style-type: none"> <li>▪ It forwards all the received EAPOL-Key frames to the Key Handler Module via the PNAC Interface Task.</li> <li>▪ It maintains the physical link status information provided by CFA and informs the Authenticator and Supplicant modules to take the necessary action on physical link UP/DOWN conditions.</li> <li>▪ It forms an EAPOL frame when requested by the Authenticator Module or Supplicant Module or Key Handler Module and transmits it to CFA</li> </ul> <p>– Mac Based/Single-Host – Authenticates and authorizes devices attached to a Bridge port in the shared LAN named as MAC based network access control. The following occurs when Mac based authentication is selected.</p> <ul style="list-style-type: none"> <li>▪ On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized.</li> <li>▪ If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module.</li> <li>▪ If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module.</li> <li>▪ If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module,</li> </ul>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	which then drops the frame
<b>Auth Port Status</b>	<p>Displays the status of the Authenticator Port. The options are:</p> <ul style="list-style-type: none"> <li>– Authorized – Module is ready for transmission or reception of data</li> <li>– Unauthorized - Module is not ready for transmission or reception of data</li> </ul>
<b>Supp Port Status</b>	<p>Displays the status of the Supplicant PAE state machine. The options are:</p> <ul style="list-style-type: none"> <li>– Authorized - Module is ready for transmission or reception of data</li> <li>– Unauthorized - Module is not ready for transmission or reception of data</li> </ul>
<b>Access Control</b>	<p>Select the Access Control status for the port. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator. The default option is <b>INACTIVE</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– INACTIVE – Indicates that the port uses only the Authenticator authorization state to restrict access to the port and not the Supplicant authorization state.</li> <li>– ACTIVE – Indicates that the port applies both the Supplicant authorization state and Authenticator authorization state.</li> </ul>
<b>Configured Control Direction</b>	<p>Select the value of the administrative controlled directions parameter for the port. The options are:</p> <ul style="list-style-type: none"> <li>– Both - Authentication control is imposed on both the incoming and outgoing packets</li> <li>– In - Authentication control is imposed on the incoming packets</li> </ul>
<b>Operational Control Direction</b>	<p>Select the value of the operational controlled directions parameter for the port. The options are:</p> <ul style="list-style-type: none"> <li>– Both - Authentication control is imposed on both the incoming and outgoing packets</li> <li>– In - Authentication control is imposed on the incoming</li> </ul>

	packets
<b>Auth SM State</b>	<p>Select the state of the Authenticator State Machine for the entry. The options are:</p> <ul style="list-style-type: none"> <li>- Initialize –This state occurs when the module is disabled and port is down</li> <li>- Disconnected – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition.</li> <li>- Connecting – This state is the beginning of the PNAC packet exchange</li> <li>- Authenticating – This state occurs whenever authenticator receives response ID from supplicant</li> <li>- Authenticated - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange</li> <li>- Aborting – This state occurs when Authenticator SM receives re- authenticating event or EAP start or supplicant log off</li> <li>- Held - This state occurs when authentication failure occurs due to wrong user name or password</li> <li>- ForceAuth – This state occurs when the port control is changed to force authorized</li> <li>- ForceUnauth - - This state occurs when the port control is changed to force unauthorized</li> </ul>
<b>SuppSMState</b>	<p>Select the state of the Supplicant State Machine. The options are:</p> <ul style="list-style-type: none"> <li>- Disconnected - There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition.</li> <li>- Logoff - State Machine never remains in this state and there will be an immediate transition to the other state</li> <li>- Connecting - This state is the beginning of the PNAC packet exchange</li> <li>- Authenticating – This state occurs whenever supplicant receives a request or challenge from authenticator</li> </ul>

	<ul style="list-style-type: none"> <li>– Authenticated - This state occurs whenever Supplicant SM port transitions to authorized through EAP exchange</li> <li>– Acquired – This state occurs whenever supplicant receives a request ID from authenticator</li> <li>– Held - This state occurs when authentication failure occurs due to wrong user name or password</li> <li>– ForceAuth – This state occurs when the port control is changed to force authorized</li> <li>– ForceUnauth – This state occurs when the port control is changed to force unauthorized</li> </ul>
<b>Restart Authentication</b>	<p>Select the initialization control for the port to restart authentication. The options are:</p> <ul style="list-style-type: none"> <li>– True – Causes the Port to be initialized.</li> <li>– False – Reverts to False once initialization is complete.</li> </ul>
<b>Authentication Retry Count</b>	<p>Enter the maximum number of authentication requests that can be sent from the authenticator before getting response from the supplicant. This value ranges from 1 to 10. The default value is <b>2</b>.</p>
<b>Reauth</b>	<p>Select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. The default option is <b>Disabled</b>.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables reauthentication on the port</li> <li>– Disabled – Disables reauthentication on the port</li> </ul>
<b>Authentication Max Start</b>	<p>Enter the maximum number of successive EAPOL-Start messages that will be sent before the supplicant assumes that there is no authenticator present. This value ranges from 1 to 65535. The default value is <b>3</b>.</p>
<b>Reauthentication</b>	<p>Select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. The default value is <b>False</b>.</p> <p>The list contains:</p>



	<ul style="list-style-type: none"> <li>- True – Enables reauthentication on the port</li> <li>- False – Disables reauthentication on the port</li> </ul>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.10.3 Timers

This screen allows the user to configure the Timer parameters at the individual port level.

Select	Port	Quiet Period (secs)	Transmit Period (secs)	Re-authentication Period (secs)	Supplicant Timeout	Server Timeout	Held Period	Auth Period	Start Period
<input type="radio"/>	Gi0/1	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/2	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/3	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/4	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/5	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/6	60	30	3600	30	30	60	30	30
<input type="radio"/>	Gi0/7	60	30	3600	30	30	60	30	30

Label	Description
<b>Port</b>	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).
<b>Quiet Period (secs)</b>	Enter the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. In this the duration the authenticator remains silent and will not attempt to acquire a supplicant. This value ranges from 0 to 65535 seconds. The default value is <b>60</b> seconds.
<b>Transmit Period (secs)</b>	Enter the Time Period used by the Authenticator State machine to define when the EAP Request ID PDU is to be transmitted. This value ranges from 1 to 65535 seconds. The default value is <b>30</b> seconds.
<b>Re-authentication Period (secs)</b>	Enter the time between periodic re-authentication of the supplicant. Re-authentication period denotes the number of times the switch restarts the authentication process before the port changes to the unauthorized state. This value ranges from 1 to 65535 seconds. The default value is <b>3600</b> seconds.
<b>Supplicant Timeout</b>	Enter the amount of time the switch waits for a response before resending the request to the client, when relaying a request

	from the authentication server to the client. This value ranges from 1 to 65535 seconds. The default value is <b>30</b> seconds.
<b>Server Timeout</b>	Enter the amount of time the switch waits for a reply before resending the response to the server, when relaying a response from the client to the authentication server. This value ranges from 1 to 65535 seconds. The default value is <b>30</b> seconds.
<b>Held Period</b>	Enter the amount of time the client will wait before re-attempting a failed 802.1X authentication. When the Supplicant (in the client) receives an authentication failure indication from the Switch, it remains idle for a period of time which is determined by the value of held-period. After this time, the supplicant initiates authentication again. Authentication failure might occur if supplicant provides a wrong password. This value ranges from 1 to 65535 seconds. The default value is <b>60</b> .
<b>Auth Period</b>	Enter the time interval for resending 802.1X request messages after not receiving a response. This value ranges from 1 to 65535 seconds. The default value is <b>30</b> seconds.
<b>Start Period</b>	Enter the time interval for resending Start messages. Start period denotes the number of seconds between successive EAPOL-Start messages following no response from the authenticator. This value ranges from 1 to 65535 seconds. The default value is <b>30</b> seconds.

#### 4.2.10.4 Local AS

This screen allows the user to configure the Local Authentication Server information. It contains authentication related User configuration information maintained by PNAC local Authentication Server. Each entry contains User name, Password, Authentication protocol used, Authenticated session timeout and Access ports list of the User seeking authentication

User Name	<input type="text"/>	*
Password	<input type="password"/>	*
Permission	Allow <input type="button" value="v"/>	*
Auth-TimeOut	<input type="text"/>	
Port List	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	User Name	Permission	Auth-TimeOut (secs)	Port List
<input checked="" type="radio"/>	Aricent	Allow <input type="button" value="v"/>	0	Gi0/1
<input type="button" value="Apply"/> <input type="button" value="Delete"/>				

Label	Description
<b>User Name</b>	Enter the identity of the user seeking authentication. This field is a string of maximum size 20.
<b>Password</b>	Enter the password specific to the user name. This field is a string of maximum size 20.
<b>Permission</b>	Select the allowance /denial of access for local authentication server. The options are: <ul style="list-style-type: none"> <li>- Allow - Authentication request is allowed over the set of ports in the Port List.</li> <li>- Deny - Authentication request is not allowed over the set of ports in the Port List.</li> </ul>
<b>Auth-TimeOut</b>	Enter the Authentication Timeout in seconds. The time in seconds after which the Authentication offered to the User ceases. When the object value is 0, the ReAuthPeriod of the Authenticator port is used by Authenticator. This value ranges from 1 to 7200 seconds.
<b>Port List</b>	Enter the complete set of ports of the authenticator to which the user is allowed or denied access.

### 4.2.10.5 Radius Settings

This screen allows the user to configure the Radius Server settings. RADIUS is a portable implementation of the RADIUS client protocol. This protocol carries authentication information between the Network Access Server (NAS) that desires to authenticate its links and the RADIUS server that is responsible for authenticating and maintaining the authentication information

Select	IP Address Type	IP Address	Primary	Shared secret	Response Time (secs)	Retry Count	Authentication Port
<input type="radio"/>	IPv4	13.0.0.1	No		10	3	1
<input checked="" type="radio"/>	IPv6	1111::2222	Yes		10	3	1812

Delete    Modify

Configure Trace Options

Label	Description
<b>Server Address Type</b>	Select the Radius server address type. The default option is <b>IPV4</b> . Options are: <ul style="list-style-type: none"> <li>- IPV4 – Radius server address type is set as Internet Protocol Version 4, where a 32 bit address is used.</li> <li>- IPV6 - Radius server address type is set as Internet Protocol Version 6, where a 128 bit address is used.</li> </ul>
<b>IP Address</b>	Enter the IP Address of the Radius Server.
<b>Primary Server</b>	Select server type as a primary server or not. Only one server can be configured as the primary server. The default option is <b>No</b> . Options are: <ul style="list-style-type: none"> <li>- Yes – Indicates the server type as primary server.</li> <li>- No – Indicates the server type is not primary server.</li> </ul>
<b>Shared Secret</b>	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.
<b>Response Time (secs)</b>	Enter the maximum time within which the Radius Server is expected to respond for a request from the Radius Client. This value ranges from 1 to 120 seconds. The default value is <b>10</b> .
<b>Retry Count</b>	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 from 1 to 254. The default value is <b>3</b>
<b>Authentication Port</b>	Enter the port number used for authentication. This value ranges from 1 to 65535

#### 4.2.10.6 MAC Session Info

This screen displays the MAC Session information details. It contains authentication session information associated with each Supplicant while Authenticator operates in MAC based authentication mode. The MAC session entries are deleted from the port whenever it receives the port operational status down information

Select	Supplicant MacAddr	Session Identifier	AuthSM State	Auth-Session Status	Session PortNumber	Session Initialize	Session Reauthenticate
<input checked="" type="checkbox"/>	00:ac:c0:01:05:01	10	AUTHENTICATED	AUTHORIZED	1	False ▾	True ▾

Label	Description
<b>Supplicant MacAddr</b>	Displays the Supplicant MAC Address for the session
<b>Session Identifier</b>	Displays the Session Identifier of the supplicant for the session.
<b>Auth SM State</b>	<p>Select the state of the Authenticator State Machine for the entry. The list contains:</p> <ul style="list-style-type: none"> <li>- Initialize –This state occurs when the module is disabled and port is down</li> <li>- Disconnected – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be a immediate transition.</li> <li>- Connecting – This state is the beginning of the PNAC</li> </ul>

	<p>packet exchange</p> <ul style="list-style-type: none"> <li>- Authenticating – This state occurs whenever authenticator receives response ID from supplicant</li> <li>- Authenticated - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange</li> <li>- Aborting – This state occurs when Authenticator SM receives re- authenticating event or EAP start or supplicant log off</li> <li>- Held - This state occurs when authentication failure occurs due to wrong user name or password</li> <li>- ForceAuth – This state occurs when the port control is changed to force authorised</li> <li>- ForceUnauth - This state occurs when the port control is changed to force unauthorised</li> </ul>
<b>Auth Session Status</b>	<p>Displays the Authentication Session Status.</p> <ul style="list-style-type: none"> <li>- Authorized – Module is ready for transmission or reception of data</li> <li>- Unauthorized - Module is not ready for transmission or reception of data</li> </ul>
<b>Session PortNumber</b>	<p>Displays the port number through which a particular Session MAC address is learnt.</p>
<b>Session Initialize</b>	<p>Select the session initialize status for the supplicant mac address configured. The default value is <b>True</b>. This list contains;</p> <ul style="list-style-type: none"> <li>- True – Indicates session initialize is set</li> <li>- False - Indicates session initialize is reset</li> </ul>
<b>Session Reauthenticate</b>	<p>Select the session reauthentication status for the supplicant mac address configured. The default value is <b>True</b>. This list contains;</p> <ul style="list-style-type: none"> <li>- True – Indicates session re-authentication is initialized</li> <li>- False - Indicates session re-authentication is reset</li> </ul>

### 4.2.11 Mirroring

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. This screen allows the user to configure the mirroring control settings.

Session Index	<input type="text"/> *
Mirror Type	Invalid <input type="button" value="v"/> *
Source Entity	<input type="text"/> *
Destination Entity	<input type="text"/> *
Mode	both <input type="button" value="v"/>
Context Id	<input type="text"/>
Vlan	<input type="text"/>
Rspan Status	Disabled <input type="button" value="v"/>
Rspan VlanId	<input type="text"/>
Rspan Context	<input type="text"/>
<input type="button" value="Add"/>	

Select	Session ID	Mirror Type	Source Entity	Destination Entity	Mode	Context Id	Vlan Id	Rspan Status	Rspan VlanId	Rspan Context	Action	Status
--------	------------	-------------	---------------	--------------------	------	------------	---------	--------------	--------------	---------------	--------	--------

Label	Description
<b>Select</b>	Click to select the session ID for which the configurations have to be modified or the session needs to be deleted.
<b>Session Index</b>	Enter the index of the mirroring session. This value ranges from 1 to 20.
<b>Mirror Type</b>	<p>Select the type of mirroring that the session supports. The default option is <b>Invalid</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- PortBased - Receives / Transmits mirroring packets depending on mirroring mode (ingress/egress/both) on 'source' port(s) to 'destination' port(s)</li> <li>- 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</li> <li>- VlanBased - Receives / Transmits Mirroring data on a</li> </ul>

	<p>particular VLAN to the destination port</p> <ul style="list-style-type: none"> <li>- Invalid - Sets the Mirror Type as Invalid</li> <li>- IpFlowBased - Receives / Transmits Mirroring the packets on the source port for that flow to the destination port</li> </ul>
<b>Source Entity</b>	<p>Enter the source ID which participates in a mirroring session. 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). For MacFlowBased and IPFlowBased Mirroing, this value ranges from 1 to 65535.</p>
<b>Destination Entity</b>	<p>Enter the destination port id from which the packets will be transmitted. 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).</p>
<b>Mode</b>	<p>Select the mode of mirroring. The default option is <b>Both</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- ingress - Mirrors only traffic that is ingressing on the source ports</li> <li>- egress - Mirrors only traffic that is egressing on the source ports</li> <li>- both - Mirrors both traffic that is ingressing on the source ports and egressing out of source ports</li> </ul>
<b>Context Id</b>	<p>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 from 1 to 64.</p>
<b>Vlan</b>	<p>Enter the VLAN identifier from which the packets will be transmitted. This value ranges from 1 to 4094.</p>
<b>Rspan Status</b>	<p>Select whether the session is enabled or disabled for Remote monitoring. The default option is <b>Disabled</b>. The list contains;</p> <ul style="list-style-type: none"> <li>- Source - Enables Session for Remote monitoring and the source entities for the session are remotely monitored.</li> <li>- Destination - Specifies that the session should monitor remote traffic mirrored with RSPAN (Remote Switched Port Analyzer) VLAN ID.</li> <li>- Disabled - Disables Remote monitoring for the mirroring</li> </ul>



	session.
<b>Rspan VlanId</b>	Enter the Remote VLAN identifier used for achieving remote monitoring. This value ranges from 1 to 4094.
<b>Rspan Context</b>	Enter the context identifier to which the Remote VLAN belongs.
<b>Action</b>	Select the Action status for any VLAN entry for a session. The list contains: <ul style="list-style-type: none"> <li>– Add - Creates a VLAN entry for a session</li> <li>– Delete - Deletes a VLAN entry for a session</li> </ul>
<b>Status</b>	Displays the status of the Mirror Control Extension table entries. The list contains: <ul style="list-style-type: none"> <li>– Up - Indicates the status of Mirror Control Extension table entries as enabled.</li> <li>– Down - Indicates the status of Mirror Control Extension table entries as disabled.</li> <li>– Under creation - Indicates that the Mirror Control Extension table entries are under creation.</li> </ul>

## 4.2.12 Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring, O-RSTP, and Open-Ring featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

### 4.2.12.1 O-Ring

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 10 milliseconds and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.



O-Ring supports three ring topologies: Ring Master, Coupling Ring, and Dual Homing. You can configure the settings in the interface below.

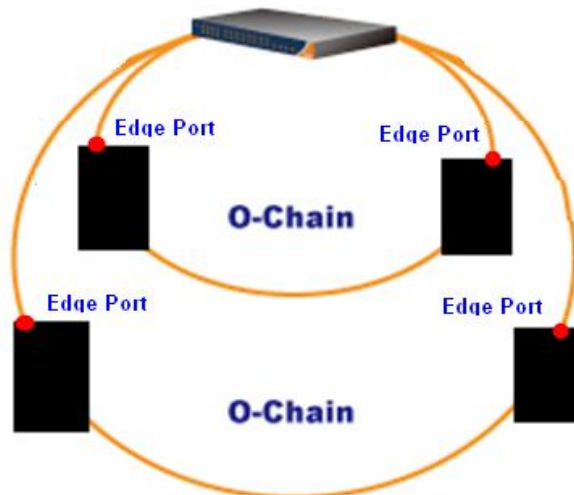


Label	Description
<b>O-Ring</b>	Check to enable O-Ring topology.
<b>Ring Master</b>	Only one ring master is allowed in a ring. However, if more than one switches are set to enable <b>Ring Master</b> , the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
<b>1<sup>st</sup> Ring Port</b>	The primary port when the switch is ring master
<b>2<sup>nd</sup> Ring Port</b>	The backup port when the switch is ring master
<b>Coupling Ring</b>	Check to enable <b>Coupling Ring</b> . <b>Coupling Ring</b> can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
<b>Coupling Port</b>	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup

	mode.
<b>Dual Homing</b>	Check to enable <b>Dual Homing</b> . When <b>Dual Homing</b> is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.

### 4.2.12.2 O-Chain

O-Chain is ORing’s revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 10ms for up to 250 switches if at any time a segment of the chain fails.



O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.

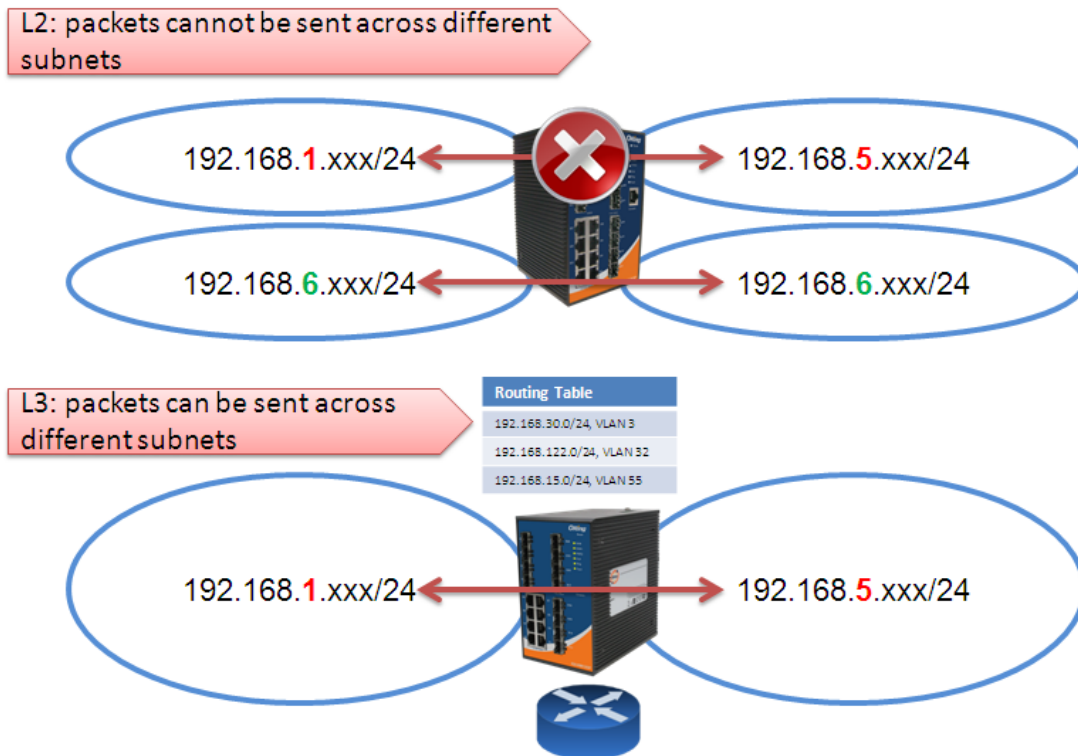
O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.

Enable			
	Uplink Port	Edge Port	State
1st	Port 1	<input checked="" type="checkbox"/>	
2nd	Port 1	<input type="checkbox"/>	

Label	Description
<b>Enable</b>	Check to enable O-Chain function
<b>1<sup>st</sup> Ring Port</b>	The first port connecting to the ring
<b>2<sup>nd</sup> Ring Port</b>	The second port connecting to the ring
<b>Edge Port</b>	An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.

### 4.3 Layer 3 Management

The device provides a variety of Layer 3 functions. Layer 3 switching is hardware-based packet forwarding, hence faster than Layer 2 counterparts which rely on software to forward packets. One of the advantages of Layer 3 switches is that Layer 3 packets can be sent across different subnets while Layer 2 packets cannot.



There are many benefits of using Layer 3 switches other than faster transmission.

#### Security

With more granular routing functions and the implementation of access control lists and subnets, Layer 3 switching provides greater security, control, and bandwidth conservation

than Layer 2 switching.

**Ideal for Large Networks**

Layer 3 switching is an important function for large networks because they are usually divided into multiple sub-networks for management and security purposes. With Layer 3, packets can be routed between the various sub-networks.

**Bandwidth Efficiency**

You can divide networks into smaller segments and restrict broadcasts to only that sub-network with Layer 3 switching, hence reducing overall traffic levels.

**4.3.1 IP**

RGS-PR9000-A IP (Internet Protocol) functions at the network layer. IP delivers/forwards packets to the higher layer and to other hosts/routers. The forwarding table maintained by IP consists of the Static Routers and the Routes learnt from other Routing Protocols.

**4.3.1.1 VLAN Interface**

This screen allows the user to configure the basic settings of the VLAN interface.

Select	VLAN Interface	Switch	Admin State	Ipv4 Enabled State	Oper State	Proxy ARP	MTU
<input checked="" type="radio"/>	1	default	Up	Up	Up	Disabled	1500

Label	Description
<b>Select</b>	Select the VLAN Interface for which the configurations need to be modified or deleted.
<b>VLAN Interface</b>	Enter the VLAN/VFI Id for the Interface to be created. The value

	<p>ranges from 1 to 65535.</p> <ul style="list-style-type: none"> <li>– &lt;vlan -id&gt; - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4094</li> <li>– &lt;vfi-id&gt;. - 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 from 4096 to 65535</li> </ul>
<b>Switch</b>	Select the switch context from the list of configured switches.
<b>Admin State</b>	<p>Select the Admin Status of the VLAN interface. The default option is <b>Down</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Up - Makes the IP interface administratively up. After Configuring the IP address the interface can be made admin UP.</li> <li>– Down - Makes the IP interface administratively down.</li> </ul>
<b>Ipv4 Enabled State</b>	<p>Select the status of IPv4 on the interface. The default option is <b>UP</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– UP - Enables IPv4 on this interface.</li> <li>– Down - Disables IPv4 on this interface.</li> </ul>
<b>Oper State</b>	<p>Displays the current operational status of the VLAN interface. The list contains:</p> <ul style="list-style-type: none"> <li>– Up - Specifies that the interface is operationally up and ready to transmit and receive network traffic.</li> <li>– Down - Specifies that the interface is operationally down.</li> </ul>
<b>Proxy ARP</b>	<p>Select the Proxy ARP admin status for the interface. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables Proxy ARP feature for the interface.</li> <li>– Disabled - Disables Proxy ARP feature for the interface.</li> </ul>
<b>MTU</b>	<p>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. The default value is <b>1500</b>. This value ranges from 46 to 9216.</p>

### 4.3.1.2 IPV4 AddrConf

This screen allows the user to configure the settings of the IPv4 interface.

Interface Id	vlan1 *
Get IP Address Mode	Manual
IP Address	_____ *
Subnet Mask	_____._____._____._____ *
Address Type	Primary
<input type="button" value="Modify"/> <input type="button" value="Reset"/>	

Select	Interface	Switch	IP Address	Subnet Mask	Broadcast Address	Address Type	IP Allocation
<input checked="" type="radio"/>	vlan1	default	192.168.2.96	255.255.0.0	192.168.255.255	Primary	DHCP

Label	Description
<b>Interface Id</b>	Select the index value which uniquely identifies the VLAN interface to which this entry is applicable
<b>Get IP Address Mode</b>	Select the protocol to be used to obtain the IP address from the interface. The default option is <b>RARP</b> . The list contains: <ul style="list-style-type: none"> <li>- Manual - The IP address is configured manually to a specified address by the user or administrator.</li> <li>- RARP - The IP address is assigned to the system by a RARP (Reverse Address Resolution Protocol) server.</li> <li>- 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.</li> </ul>
<b>IP Address</b>	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.
<b>Subnet Mask</b>	Enter the subnet mask for the provided IP address.
<b>Address Type</b>	Select the type of address. The default option is Primary. The list contains: <ul style="list-style-type: none"> <li>- Primary - Primary IP address of the Interface</li> <li>- 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</li> </ul>

### 4.3.1.3 IP Route

Destination Network	<input type="text"/>	*
Subnet Mask	<input type="text"/>	*
Next Hop	Interface <input type="button" value="v"/>	
Gateway	<input type="text"/>	
Interface	vlan1 <input type="button" value="v"/>	*
Switch	default <input type="button" value="v"/>	
Distance (Metric)	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Destination Network	Subnet Mask	Gateway	Interface	Switch	Distance (Metric)	Routing Protocol
<input type="radio"/>	0.0.0.0	0.0.0.0	192.168.2.1	default	default	<input type="text" value="1"/>	192.168.2.1
<input checked="" type="radio"/>	192.168.0.0	255.255.0.0	0.0.0.0	vlan1	default	<input type="text" value="0"/>	Connected

Label	Description
<b>Destination Network</b>	Enter the destination IP address of the route. It denotes the Network Address for which the route is being added.
<b>Subnet Mask</b>	Enter the subnet mask for the Destination Network address.
<b>Gateway</b>	Enter the Next Hop gateway to reach the Destination Network.
<b>Interface</b>	Select the outgoing interface through which the Destination Network is reachable.
<b>Switch</b>	Specifies the name of the switch context.
<b>Distance (Metric)</b>	Enter the Metric value of the destination. The semantics of this metric are determined by the routing-protocol. The value ranges from 1 to 255. The default value is <b>1</b> .
<b>Routing Protocol</b>	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.

### 4.3.1.4 LoopBack Settings

This screen allows the user to configure the basic loopback settings.



LoopBack Interface  \*

Interface type

Interface Status  ▼

Ip Address

Subnet Mask

Select	LoopBack Interface	Interface Status	IP Address	Subnet Mask	Broadcast Address
<input type="button" value="Apply"/> <input type="button" value="Delete"/>					

Label	Description
<b>LoopBack Interface</b>	Enter the Loopback Interface that is to be created.
<b>Interface type</b>	Displays the interface type as Loopback.
<b>Interface Status</b>	Select the Interface Status. The list contains: <ul style="list-style-type: none"> <li>- Up - Allows traffic through the interface.</li> <li>- Down - Does not allow traffic.</li> </ul>
<b>Ip Address</b>	Enter the IP Address for the Loopback interface.
<b>Subnet Mask</b>	Enter the Subnet mask for the given IP Address.
<b>Broadcast Address</b>	Displays the Broadcast address for the specified IP address.

### 4.3.1.5 IVR-VLAN Mapping

This screen allows the user to configure the list of VLANs to be associated for an IVR interface.

VLAN Interface  \*

Switch  ▼

Associated Vlan  \*

Select	VLAN Interface	Context	Associated Vlan
<input type="button" value="Delete"/>			

Label	Description
<b>VLAN Interface</b>	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 <b>VLAN Interface Basic Settings</b> screen. This value ranges from 1 to 4094. The VLAN or list of VLANs can be mapped only to the IVR interfaces already created in the system.
<b>Switch</b>	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.
<b>Associated Vlan</b>	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.

### 4.3.2 IP (contd...)

#### 4.3.2.1 IP

This screen allows the user to configure the IP Information.

IP Routing	Enable <input type="button" value="v"/>
ICMP Send Redirect	Enable <input type="button" value="v"/>
ICMP Send Unreachable	Enable <input type="button" value="v"/>
ICMP Send Echo Reply	Enable <input type="button" value="v"/>
ICMP Send Netmask Reply	Enable <input type="button" value="v"/>
Number of Aggregated Routers	<input type="text" value="50"/>
Number of Multi-Paths	<input type="text" value="2"/>
Load Sharing	Enable <input type="button" value="v"/>
PMTU-D	Enable <input type="button" value="v"/>

Label	Description
<b>IP Routing</b>	Select the IP routing status. The default option is <b>Enable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Enables the IP routing status for configuring IP information.</li> <li>- Disable - Disables the IP routing status for configuring IP information.</li> </ul>
<b>ICMP Send Redirect</b>	Select the ICMP Send redirect status on an interface basis. The default option is <b>Enable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Allows sending ICMP Redirect Message</li> <li>- Disable - Does not allow sending ICMP Redirect Message</li> </ul>
<b>ICMP Send Unreachable</b>	Select the ICMP Send unreachable status. The default option is <b>Enable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Allows sending ICMP unreachable message</li> <li>- Disable - Does not allow sending ICMP unreachable message</li> </ul>
<b>ICMP Send Echo Reply</b>	Select the ICMP send Echo reply status. The default option is <b>Enable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Allows sending ICMP Echo Reply Message</li> <li>- Disable - Does not allow sending ICMP Echo Reply Message</li> </ul>

<b>ICMP Send Netmask Reply</b>	<p>Select the ICMP Send Netmask Reply status. The default option is <b>Enable</b>. The list contains</p> <ul style="list-style-type: none"> <li>– Enable - Allows sending ICMP Net Mask Reply Message</li> <li>– Disable - Does not allow sending ICMP Net Mask Reply Message</li> </ul>
<b>Number of Aggregated Routers</b>	<p>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 from 5 to 4095.</p>
<b>Number of Multi-Paths</b>	<p>Enter the number of multi-paths in the routing table. The value ranges from 1 to 16. The default value is <b>2</b>.</p>
<b>Load Sharing</b>	<p>Enter the load sharing status. The default option is <b>Disable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enable - Allows the distribution of the load available in the equal cost multi-paths</li> <li>– Disable - Does not allow the distribution of the load available in the equal cost multi-paths</li> </ul>
<b>PMTU-D</b>	<p>Select this object to enable or disable the PMTU-D on all paths globally. The default option is <b>Disable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enable - Overrides the route-based and application-level requests for PMTU-D.</li> <li>– Disable –PMTU-D is not done even if the application requests to do so.</li> </ul>

#### 4.3.2.2 IP PMTU

This screen allows the user to configure the IP PMTU.

Destination IP Address	<input type="text"/>	*
Type of service of the path	<input type="text"/>	*
Path MTU value	<input type="text"/>	
PMTU Discovery	Disable	▼
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Destination IP Address	Type of service of the path	Path MTU Value	PMTU Discovery
<input type="button" value="Apply"/> <input type="button" value="Delete"/>				

Label	Description
<b>Destination IP Address</b>	Enter the destination IP address of the path for which the discovery is made.
<b>Type of service of the path</b>	Enter the type of service of the path. The value ranges from 0 to 255.
<b>Path MTU value</b>	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. The default option is <b>255</b> .
<b>PMTU Discovery</b>	Select the status of the PMTU discovery. The list contains: <ul style="list-style-type: none"> <li>- Enable - Enables the PMTU discovery for the given path to override the application request with respect to PMTU-D.</li> <li>- Disable - Disables the PMTU discovery</li> </ul>
<b>Select</b>	Click to select configured destination IP address for which the configuration needs to be re-applied.

### 4.3.2.3 Static ARP

This screen allows the user to configure the static ARP entry settings.

The ARP finds the hardware address of the client and stores them in arp cache. The arp entry can be configured manually by using this command. The entry is stored permanently in the arp cache as a static entry.

Interface vlan1 ▾\*

ipaddress

physicaladdress

Select	Interface	ipaddress	physicaladdress	type	status
<input type="radio"/>	vlan1	192.168.2.1	00:1d:aa:82:94:e0	▾	▾
<input type="radio"/>	vlan1	192.168.2.131	74:d4:35:ca:c9:03	▾	▾
<input checked="" type="radio"/>	vlan1	192.168.2.233	ac:22:0b:7e:8f:33	▾	▾

Label	Description
<b>Interface</b>	Adds a static entry in the ARP cache for the specified interface.
<b>Ipaddress</b>	Enter the IP address or IP alias to map to the specified MAC address.
<b>Physicaladdress</b>	Enter the MAC address to map to the specified IP address or IP alias.
<b>Select</b>	Click to select configured VLAN interface for which the configuration needs to be re-applied.
<b>type</b>	<p>Displays the static entry in the ARP cache for the specified interface. This field is greyed out.</p> <ul style="list-style-type: none"> <li>– fastethernet – Officially referred to as 100BASE-T standard. This is a</li> <li>– version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>– gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>– extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>– i-lan – Internal LAN created on a bridge per IEEE 802.1ap</li> </ul>
<b>Status</b>	Displays the status for the static entry in the ARP cache for the specified interface.

### 4.3.2.4 IP Ping

This screen allows the user to configure the IP PING entry settings. The Packet Internet Groper (Ping) module is built based on the ICMP echo request and ICMP echo response messages. The network administrator uses this ping on a remote device to verify its presence. Ping involves sending ICMP echo messages repeated and measuring the time between transmission and reception of message. The output displays the time taken for each packet to be transmitted, number of packets transmitted, number of packets received and packet loss percentage.

Label	Description
<b>Ping Dest</b>	Enter the destination IP address of the node to be pinged
<b>Ping Timeout</b>	Enter the time in seconds after which the entity waiting for the ping response times out. This value ranges from 1 to 100
<b>Ping Tries</b>	Enter the number of tries in which the data need to be pinged. The value ranges from 1 to 1000.
<b>Ping DataSize</b>	Enter the size of the data need to be pinged. The value ranges from 0 to 2080.
<b>Ping Status</b>	Displays the status of the data that is pinged. This field is greyed out. <ul style="list-style-type: none"> <li>- PROGRESS - Indicates the ping status as in progress.</li> <li>- COMPLETED - Indicates the ping status as completed.</li> </ul>

	– NOT INITIATED - Indicates the ping status as not initiated.
<b>Ping SendCount</b>	Displays the send count of the pinged data.
<b>Ping AvgTime</b>	Displays the average time taken for pinging data.
<b>Ping MaxTime</b>	Displays the maximum time taken for pinging data.
<b>Ping MinTime</b>	Displays the minimum time taken for pinging data.
<b>Ping Success</b>	Displays the success count of the pinged data.

### 4.3.2.5 IPV4 TRACEROUTE

This screen allows the user to configure the IPv4 trace route settings

Index

Destination Ip

Admin State

MaxTTL

MinTTL

TimeOut

MTU

Select	Index	Destination Ip	Admin State	MaxTTL	MinTTL	Oper State	TimeOut	MTU
--------	-------	----------------	-------------	--------	--------	------------	---------	-----

Label	Description
<b>Index</b>	Enter the index value to configure information about a particular IP traceroute operation. This value ranges from 0 to 10.
<b>Destination IP</b>	Enter the destination IP address of the path for which the trace route is made.
<b>Admin State</b>	Select the status for the trace route operation. The default option is on. The list contains: <ul style="list-style-type: none"> <li>– on - Sets the trace operation status as in progress.</li> <li>– Off - Does not sets the trace operation status as in progress.</li> </ul>



<b>MaxTTL</b>	Enter the maximum value of the TTL field to be filled up in the IP packets used for the trace route. The value ranges from 1 to 99. The default value is <b>15</b> .
<b>MinTTL</b>	Enter the minimum value of the TTL field to be filled up in the IP packets used for the trace route. The value ranges from 1 to 99. The default value is <b>1</b> .
<b>TimeOut</b>	Enter the interval in seconds between consecutive trace requests. The value ranges from 1 to 2147483647.
<b>MTU</b>	Enter number of octets of data to be sent in trace packets. The value ranges from 1 to 2147483647.
<b>OperState</b>	Displays the current status for the trace route operation. <ul style="list-style-type: none"> <li>- In progress - Displays the current status for the trace route operation as in progress.</li> <li>- Not in progress - Displays the current status for the trace route operation as not in progress.</li> </ul>
<b>Select</b>	Click to select configured index for which the configuration needs to be re-applied.

### 4.3.3 Layer 3 Tunnel

The Tunnel Interface Configuration page allows the user to configure the tunnels.

Tunnel	<input type="text"/> *
Source	<input type="text"/> *
Destination	<input type="text"/> *
Mode	<input type="text"/> ▼
Config-ID	<input type="text"/> *
Checksum	True ▼
Pmtu Discovery	True ▼
Direction	uni-recvonly ▼
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

select	Phy Alias	TnlAlias	Source	Destination	Mode	ConfigId	Security	CheckSum	PMTU	Direction
--------	-----------	----------	--------	-------------	------	----------	----------	----------	------	-----------

Label	Description
<b>Tunnel</b>	Specifies the Tunnel Interface Alias. The size ranges from 0 to 64
<b>Source</b>	Specifies the address of the local end point of the tunnel (the source address used in the outer IP header).
<b>Destination</b>	Specifies the address of the remote end point of the tunnel (the destination address used in the outer IP header).
<b>Mode</b>	<p>Specifies the encapsulation method used by the tunnel. The options are:</p> <ul style="list-style-type: none"> <li>– Gre - Generic Routing Encapsulation</li> <li>– 6to4 - 6 to 4 encapsulation</li> <li>– isatap - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)</li> <li>– encapsulation</li> <li>– compat - IPv6 Auto-Compatible encapsulation</li> <li>– ipv6ip - IPv6 over IPv4 Configured encapsulation</li> </ul>
<b>Config-ID</b>	<p>Specifies an identifier to distinguish multiple tunnels with the same end points and same encapsulation method. This value ranges from 1 to 2147483647.</p> <ul style="list-style-type: none"> <li>– The identifier must be set as 1 if the encapsulation protocol such as GRE (Generic Routing Encapsulation) or IP-in-IP, which allows one tunnel per set of endpoint addresses, is selected.</li> <li>– The identifier can be set as any random number without conflicting with an existing row if the encapsulation protocol such as L2F (Layer 2 Forwarding), which allows multiple parallel tunnels, is selected.</li> </ul>
<b>Checksum</b>	<p>Specifies whether checksum needs to be set in GRE header for GRE encapsulation method. The default option is <b>False</b> The options are:</p> <ul style="list-style-type: none"> <li>– True - Sets the checksum in GRE header for GRE encapsulation.</li> <li>– False - Does not set the checksum in GRE header for GRE encapsulation.</li> </ul>

<b>Pmtu Discovery</b>	<p>Specifies whether Path MTU discovery needs to be enabled on the tunnel interface. The default option is <b>False</b> The options are:</p> <ul style="list-style-type: none"> <li>- True - Enables Path MTU discovery.</li> <li>- False - Disables Path MTU discovery</li> </ul>
<b>Direction</b>	<p>Specifies whether the configured tunnel is unidirectional or bi-directional. The default option is <b>Bi-directional</b> The options are:</p> <ul style="list-style-type: none"> <li>- uni-recvonly - Configured tunnel is unidirectional.</li> <li>- uni-sendonly - Configured tunnel is unidirectional and send only.</li> <li>- Bi-directional - Configured tunnel is bi-directional</li> </ul>

#### 4.3.4 DHCP Server

DHCP (Dynamic Host Configuration Protocol) is used in a wide variety of devices like ISDN routers, firewalls, etc., for assigning IP addresses to workstations. Besides obtaining IP address, other configuration parameters for a workstation can also be configured in a DHCP server. DHCP clients can retrieve these parameters along with the IP address.

DHCP is based on the client-server architecture. DHCP servers are configured with an IP address and several other configuration parameters. DHCP clients, typically workstations obtain this IP address at start-up. The client obtains the address for a time period termed as the “lease” period. DHCP clients renew the address by sending a request for the IP address before the lease expires.

DHCP uses UDP as its transport protocol and a UDP port for communication. DHCP relay agents connect servers present on one LAN with the client present on another.

DHCP server is responsible for dynamically assigning unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client. The IP address is leased to the interface only for a particular time period as mentioned in the DHCP lease. The interface should renew the DHCP lease once it expires. The DHCP server conta

##### 4.3.4.1 Basic Settings

This screen allows the user to configure the basic DHCP settings.

DHCP Server	Disabled ▾
Blocked IP Address Re-Use Timer (secs)	5 *
ICMP Echo	Disabled ▾
DHCP Next Server	0.0.0.0

Label	Description
<b>DHCP Server</b>	<p>Select the DHCP server status in the router. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables the DHCP server in the router and starts serving the server with the IP addresses. It opens the UDP socket and starts listening for DHCP discover messages from clients.</li> <li>– Disabled - Disables the DHCP server in the router.</li> </ul>
<b>Blocked IP Address Re-Use Time (secs)</b>	<p>Enter the reuse timeout value used by DHCP in seconds. It denotes the amount of time the DHCP server entity waits 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 from 1 to 120 seconds. The default value is <b>5</b> seconds.</p>
<b>ICMP Echo</b>	<p>Select the status of ICMP (Internet Control Message Protocol) Echo feature for the DHCP server. This object controls the server to probe for the IP address before allocating the IP address to a client through the ICMP echo message. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables the ICMP Echo feature. Before allocating an IP Address to client, the server broadcasts ICMP Echo Request (Ping Packet) to check whether any other machine/host is using this IP. If there is no response received, the server allocates the IP to the client.</li> <li>– Disabled - Disables the ICMP Echo feature. The ICMP Echo Request packet mechanism is not used. The IP is directly allocated to the client</li> </ul>
<b>DHCP Next Server</b>	<p>Sets the IP address of the boot server (, 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 default address is</p>

	0.0.0.0 (No boot server is defined. DHCP server is used as the boot server)
--	-----------------------------------------------------------------------------

### 4.3.4.2 Pool Settings

This screen allows the user to configure the DHCP address pool. DHCP address pools are used by the servers to allocate the IP addresses to the clients.

Pool ID	<input type="text"/> *
Pool Name	<input type="text"/> *
Subnet Pool	<input type="text"/> *
Network Mask	<input type="text"/> *
Start IP Address	<input type="text"/> *
End IP Address	<input type="text"/> *
Lease Time (Secs)	<input type="text"/>
Utilization Threshold	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Pool ID	Pool Name	Subnet Pool	Network Mask	Start IP Address	End IP Address	Lease Time (secs)	Threshold	Status
<input type="button" value="Apply"/> <input type="button" value="Delete"/>									

Label	Description
<b>Pool ID</b>	Enter the pool Identifier. This is unique index for each subnet pools. This value ranges from 1 to 2147483647.
<b>Subnet Pool</b>	Enter the subnet of the IP address in the pool.
<b>Network Mask</b>	Enter the network mask. It denotes the client's subnet mask of the IP address in the pool.
<b>Start IP Address</b>	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.
<b>End IP Address</b>	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.
<b>Lease Time (secs)</b>	Enter the time interval for which the IP address is valid. It This specifies the amount of time that the client can use the IP address assigned by the server and 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 from 60 to 2147483647 seconds. The default value is <b>3600 seconds</b> .
<b>Utilization Threshold</b>	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. This value ranges from 0 to 100 in percentage. The default value is <b>75</b> .
<b>Select</b>	Click to select pool id for which the configuration needs to be modified or deleted.
<b>Status</b>	Select the status of the entry. It denotes the status of address pool configuration and allocation of IP address. Options are <ul style="list-style-type: none"> <li>- UP - Configures the address pool successfully for allocating IP address.</li> <li>- Down - Does not configure address pool for allocation IP address.</li> </ul>

### 4.3.4.3 Pool Options

This screen allows the user to set the DHCP server pool options related configuration. The configured options are sent to DHCP client in DHCP offer packet.

Pool Name \*

Option

Option Code \*

Option Value \*

Option Value 2

Select	Pool Name	Option Code	Option Name	Option Value
--------	-----------	-------------	-------------	--------------

Label	Description
<b>Pool Name</b>	Select the pool name from the list of Address Pools created in the system for which DHCP pool options related configuration needs to be applied.
<b>Option</b>	Select the DHCP pool option that is to be set to the selected

	pool name. The default option is <b>NetMask (IP Format)</b> .
<b>Option Code</b>	Displays the corresponding DHCP option code for the DHCP option selected in the field <b>option</b> . The option code represents that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. The default option code is <b>1</b> (the code for the default option – Netmask (IP Format).
<b>Option Value</b>	Enter the value to be set for the DHCP option selected in the field <b>option</b> . This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.
<b>Select</b>	Click to select pool name for which the configuration needs to be modified or deleted.

#### 4.3.4.4 Exclude List

This screen 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.

Pool ID  \*

Start IP Address  \*

End IP Address

Select	Pool ID	Start IP Address	End IP Address
<input type="button" value="Apply"/> <input type="button" value="Delete"/>			

Label	Description
<b>Pool ID</b>	Enter the pool ID for which exclude list is to be created.
<b>Start IP Address</b>	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.

<b>End IP Address</b>	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.
<b>Select</b>	Click to select pool ID for which the configuration needs to be re- applied.

### 4.3.4.5 Host Settings

This screen allows the user to configure the host IP settings.

Select	Host MAC Address	Pool Name	Host IP
--------	------------------	-----------	---------

Label	Description
<b>Host MAC Address</b>	Enter the unicast MAC address for configuring the DHCP host.
<b>Pool Name</b>	Select the pool name from the list of Address Pools created in the system for which DHCP host IP related configuration needs to be applied.
<b>Host IP</b>	Enter the IP address for configuring the DHCP host.
<b>Select</b>	Click to select MAC address for which the configuration needs to be modified or deleted.

### 4.3.4.6 Host Options

This screen allows the user to configure the host option settings.



Host MAC Address	<input type="text"/> *
Pool Name	<input type="button" value="v"/> *
Option	NetMask (IP Format) <input type="button" value="v"/>
Option Code	1 <input type="text"/> *
Option Value	<input type="text"/> *
Option Value 2	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

**Select** Host MAC Address Pool Name Option Code Option Name Option Value

Label	Description
<b>Host MAC Address</b>	Enter the unicast MAC address for configuring the DHCP host.
<b>Pool Name</b>	Select the pool name from the list for which DHCP host IP related configuration needs to be applied.
<b>Option</b>	Select the DHCP pool option that is to be set to the selected pool name. The default option is <b>NetMask (IP Format)</b>
<b>Option Code</b>	Displays the corresponding DHCP option code for the DHCP option selected in the field <b>option</b> . The option code represents that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message The default option code is 1 (the code for the default option – <b>Netmask (IP Format)</b> )
<b>Option Value</b>	Enter the value to be set for the DHCP option selected in the field <b>option</b> . This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.
<b>Select</b>	Click to select Host MAC address for which the configuration needs to be re-applied.

### 4.3.4.7 Bootfile Configuration

This screen allows the user to configure the name of the initial boot file to be loaded in a DHCP client.

Enter the bootfile name <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Label	Description
<b>Enter the bootfile name</b>	Enter the file name to configure the name of the initial boot file to be loaded in a DHCP client. This value is a string of maximum size 64. The boot file contains the boot image that is used as the operating system for the DHCP client.

### 4.3.5 DHCP Relay

DHCP Relay agent is used to forward the DHCP packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information like the network in which the packet is removed and then forwards it to the server. The server identifies the client’s network from this information and allocates IP accordingly, then sends the reply to the relay. The relay strips the information inserted and broadcasts the packets into the client’s network.

#### 4.3.5.1 Basic Settings

This screen allows the user to configure basic DHCP Relay information.

Service DHCP-Relay Disabled ▾

IP DHCP Relay Information Option Disabled ▾

**Note :** To enable DHCP Relay, **DHCP Server** Status should be disabled.

DHCP Server Address  \*

Label	Description
<b>Service DHCP-Relay</b>	<p>Select the DHCP relay status in the switch. The default option is <b>Disabled</b>. Options are:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables the DHCP relay status in the switch. The Relay Agent forwards the packets from the client to a specific DHCP server.</li> <li>– Disabled - Disables the DHCP relay status in the switch.</li> </ul>

<p><b>IP DHCP Relay Information Option</b></p>	<p>Select the controlling status of the processing related to the Relay Agent Information options. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled - Enables the controlling status of the processing related to the</li> <li>- 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.</li> <li>- Disabled - Disables the controlling status of the processing related to the Relay Agent Information options.</li> </ul>
<p><b>DHCP Server Address</b></p>	<p>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.</p>

### 4.3.5.2 Interface Settings

This screen allows the user to configure the interface settings of the DHCP Relay.

Select	Interface	Circuit ID	Remote ID
--------	-----------	------------	-----------

Label	Description
<b>Interface</b>	Select the VLAN Interface.
<b>Circuit ID</b>	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 from 1 to 2147483647. The minimum value configurable for circuit-id is system's maximum default interfaces + 1.

<b>Remote ID</b>	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.
------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.3.6 DHCP Client

DHCP client uses DHCP to temporarily receive a unique IP address for it from the DHCP server. It also receives other network configuration information such as default gateway, from the DHCP server.

#### 4.3.6.1 DHCP Option Type

This screen 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

Interface Name \*

Option Type

Option Code

Option Value

Select	Interface Name	Dhcp Option Type	Dhcp Option Code	Dhcp Option Value
<input type="radio"/>	vlan1	DNS Servers (IP Format)	6	192.168.2.6,168.95.1.1
<input checked="" type="radio"/>	vlan1	NTP Servers (IP Format)	42	

Label	Description
<b>Interface Name</b>	Select an interface for which DHCP option type settings need to be configured from the list of vlan interfaces already created in the system.
<b>Option Type</b>	Select the DHCP Client Option Type for the specified interface created in the system. The list contains; <ul style="list-style-type: none"> <li>- TFTP Server Name (IP Format/String) - Sends the DHCP requests to get the TFTP server's domain name</li> <li>- Bootfile Name (String) - Sends the DHCP requests to get</li> </ul>

	the boot File Name
<b>Option Code</b>	<p>Displays the Option code for the specified interface created in the system. When option code is displayed as;</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- 67 - Indicates Bootfile Name (String) is set. This allows identifying a bootfile when the file field in the DHCP header is used for DHCP options.</li> <li>- 0 - Indicates no option type is set for the interface</li> </ul>
<b>Select</b>	Click to select an interface for which DHCP option type configurations need to be modified or deleted.

### 4.3.6.2 DHCP ClientId

This screen 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

Select	Interface Name	Dhcp Client Identifier
<input checked="" type="radio"/>	vlan1	

Label	Description
<b>Interface Name</b>	Select an interface for which DHCP option type settings need to be configured from the list of VLAN interfaces already created in the system.
<b>Client Identifier</b>	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.
<b>Select</b>	Click to select an interface for which DHCP option type configurations need to be modified or deleted.

### 4.3.7 RIP

**RIP (Routing Information Protocol)** is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

#### 4.3.7.1 RIP VRF Creation

This screen allows the user to enable or disable RIP for default VRF instance or a specific VRF instance

VRF Name	VRF Status
default	Disabled ▾

Label	Description
<b>VRF Name</b>	Select the VRF context name on which RIP has to be enabled or disabled. <b>Virtual Routing and Forwarding (VRF)</b> allows multiple instances of a routing table to co-exist within the same router at the same time.
<b>VRF Status</b>	Select the VRF status in the router. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Disabled - Disables RIP on the VRF instance.</li> <li>– Enabled - Enables RIP on the VRF instance to allow multiple instances of a routing table</li> </ul>

### 4.3.7.2 Basic Setting

This screen allows the user to configure the basic settings of RIP.

Select	Context Id	Context Name	Security	OutputDelay	Trusted Neighbour Feature	Auto-Summary Status	Retransmission Timeout Interval	Maximum Retransmissions	Distance
	0	default	Maximum	Disabled	Disabled	Enabled	5	36	121

Label	Description
<b>Select</b>	Click to select the Context Id for which the RIP configurations need to be modified.
<b>Context ID</b>	Enter a unique value that Identifies the Rip Domain Context.
<b>Context Name</b>	Displays the Context name for the VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
<b>Security</b>	Select the security level of RIP in the system to accept / ignore RIPv1 packets when authentication is in use. The default option is <b>Maximum</b> . The list contains: <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> </ul>

<b>OutputDelay</b>	<p>Select the Output Delay status for the RIP Domain Context.</p> <p>The default option is <b>Disabled</b>. The list contains;</p> <p>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.</p> <p>Disabled - Sets Output delay status in the RIP Domain context as Disabled thereby disabling interpacket delay for RIP packets</p>
<b>Trusted Neighbour Feature</b>	<p>Select the Trusted neighbor feature for the RIP domain context.</p> <p>The default option is <b>Enabled</b>. The list contains:</p> <p>Enabled - Sets the Trusted Neighbor Feature status as enabled. When enabled a list of router's IP address can be configured and RIP Packets from those routers will be processed by RIP and packets from other Routers will be dropped.</p> <p>Disabled - Sets the Trusted Neighbor Feature status as disabled. When disabled RIP Packet from all the routers will be processed.</p>
<b>Auto-Summary Status</b>	<p>Select the Auto Summary status for the RIP domain context.</p> <p>The default option is <b>Enabled</b>. The list contains;</p> <p>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.</p> <p>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.</p>
<b>Retransmission Timeout Interval</b>	<p>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</p>



	a response is received or the maximum retries. The value ranges from 5 to 10. The default value is <b>5</b> .
<b>Maximum Retransmissions</b>	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 from 10 to 40 seconds. The default value is <b>36</b> .
<b>Distance</b>	Enter the distance value for the specified context id. This value ranges from 1 to 255. The default value is <b>121</b> .

### 4.3.7.3 Interface Configuration

This screen allows the user to configure RIP on the specified interface.

Context Id \*

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 Originate
<input type="button" value="Apply"/>	<input type="button" value="Delete"/>										

Label	Description
<b>Context ID</b>	Select the context Id from the list of VRF instances created in the system.
<b>Interface</b>	Select the interface ID for which the RIP parameters need to be configured.
<b>IP Address</b>	Displays the IP address of the RIP interface. This is a read-only field.
<b>Status</b>	Select the administrative status of the RIP-2 in the router. The default option is <b>Enabled</b> . The list contains;: <ul style="list-style-type: none"> <li>- Enabled - Activates RIP2 process throughout the system.</li> <li>- Disabled - Disables RIP2 process in the system.</li> <li>- Passive - Runs RIP2 process as a passive one.</li> </ul>
<b>Split Horizon</b>	Select the operational status of split horizon in the system. The default option is <b>PoRGS-PR9000-Aon Reverse</b> . The list contains: <ul style="list-style-type: none"> <li>- Split Horizon - Enables the split horizon updates for the RIP which prevents the routing loops in distance routing</li> </ul>

	<p>protocol, by prohibiting the router from advertising a route back onto the interface. The split horizon updates are applied in the response packets sent.</p> <ul style="list-style-type: none"> <li>- PoRGS-PR9000-Aon Reverse - Enables the poRGS-PR9000-Aon updates for the RIP which sends route with the metric value 16 on an interface from which route is learnt.</li> <li>- 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.</li> </ul>
<b>Default Route Installation</b>	<p>Select the default route installation status in the RIP Interface. The default option is <b>No</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Yes - Enables default route installation which installs the default route received in updates to the RIP database.</li> <li>- No - Disables default route installation which blocks the installation of default route received in updates to the RIP database.</li> </ul>
<b>Send Version</b>	<p>Select the version of RIP packets that will be sent by the router. The default option is <b>RIP1 Compatible</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Do not send - Stops the IP RIP transmitting advertisements to be sent on a VLAN interface / router port</li> <li>- RIP Version1 - Sends only RIP updates compliant with RFC 1058, on the interface.</li> <li>- RIP1 Compatible - Sends both multicasting RIP updates and RIP updates compliant with RFC 1058, on the interface.</li> <li>- RIP Version2 - Sends only multicasting RIP updates on the interface.</li> </ul>
<b>Receive Version</b>	<p>Select the version of RIP updates to be received. The default option is <b>RIP1 or RIP2</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- RIP1 - Receives only RIP updates compliant with RFC 1058, on the interface.</li> <li>- RIP2 - Receives only multicasting RIP updates on the interface.</li> </ul>

	<ul style="list-style-type: none"> <li>– RIP1 or RIP2 - Receives both multicasting RIP updates and RIP updates compliant with RFC 1058, on the interface.</li> <li>– Do not receive - Sets that no IP RIP transmitting advertisements are received on a VLAN interface / router port.</li> </ul>
<b>Route Age Timer</b>	Enter the time (in seconds) after which the route entry is put into garbage collect (marked as invalid). The value ranges from 30 to 500 seconds. The default value is <b>180 seconds</b> .
<b>Update Timer</b>	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 from 10 to 3600 seconds. The default value is <b>30 seconds</b> .
<b>Garbage Timer</b>	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 from 120 to 180 seconds. The default value is <b>120 seconds</b> .
<b>Rip Default Originate</b>	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 from 0 to 15. The default option is <b>0</b> which implies that origination of default route over the interface is disabled.
<b>Select</b>	Click to select the context Id for which the configuration needs to be modified or deleted.

#### 4.3.7.4 Neighbors List

This screen 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

Select Context Id IP Address

Label	Description
<b>Conext ID</b>	Select the Context ID from the list of VRF instances created in the system to add a trusted neighbor.
<b>IP Address</b>	Enter the IP Address of the neighbor router from which this router can accept RIP packets.
<b>Select</b>	Click to select the Context Id for which the neighbor router needs to be deleted.

### 4.3.7.5 Security Settings

This screen allows the user to configure the type of authentication that is used on the interface

Select Context IP Address Authentication Type Authentication Key Authentication Key ID Start Generate Time Start Accept Time Stop Generate Time Stop Accept Time

Label	Description
<b>ContextID</b>	Select the Context ID from the list of VRF instances created in the system to configure the security settings.
<b>Interface Address</b>	Select the required Interface from the list of interfaces for which crypto authentication parameters are to be configured.
<b>Authentication Type</b>	Select the type of authentication used on the interface. The default option is <b>No Authentication</b> . The list contains: <ul style="list-style-type: none"> <li>No Authentication - Disables authentication when No</li> </ul>

	<p>Authentication is set.</p> <ul style="list-style-type: none"> <li>– Simple Password - Sets the authentication type as simple text.</li> <li>– MD5 - Sets the authentication type as keyed MD5 (Message Digest 5) authentication.</li> <li>– SHA -1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.</li> <li>– SHA-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA 256) authentication. SHA 256 generates Authentication digest of length 32 bytes.</li> <li>– SHA-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.</li> <li>– SHA- 512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.</li> </ul>
<b>Authentication Key</b>	Enter the key - value to be used as the authentication key. This value is a string with a size of 16 octets 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).
<b>Authentication Key ID</b>	Enter the active authentication KeyID currently used in the particular interface for sending RIP updates. This value ranges from 0 to 255.
<b>Start Generate Time</b>	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.
<b>Start Accept Time</b>	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 2136-02-06,06:28:15. For example, Tuesday May 26, 1992 at 1:30:15 PM should be entered as, 1992-5- 26,13:30:15.
<b>Stop Generate Time</b>	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.
<b>Stop Accept Time</b>	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.
<b>Select</b>	Click to select the IP Address for which the configuration needs to be modified or deleted.

### 4.3.7.6 Address Summary

This screen 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

Select	Context Id	Interface	Aggregate Address	Subnet Mask
--------	------------	-----------	-------------------	-------------

Label	Description
<b>Context ID</b>	Select the Context ID from the list of VRF instances created in the system to configure the summary address.
<b>Interface</b>	Select the Interface ID from the list of VLAN interfaces created in the system to configure the summary address.
<b>Aggregate Address</b>	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
<b>Subnet Mas</b>	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
<b>Select</b>	Click to select the Context Id for which the summary address is to be deleted.

### 4.3.8 OSPF

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

#### 4.3.8.1 OSPF VRF Creation

This screen allows the user to enable or disable OSPF for the specified VRF Instance.

VRF Name	VRF Status
default	Disabled

Label	Description
<b>VRF Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF

	instance. VRF name should be created in <b>VRF context manager</b> screen.
<b>VRF Status</b>	Select the admin status of OSPF virtual context. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled - Enables OSPF in the virtual context.</li> <li>– Disabled - Disables OSPF in the virtual context.</li> </ul>

### 4.3.8.2 Basic Settings

This screen allows the user to configure the basic settings of OSPF.

Context Name	default *
Router ID	<input type="text"/>
Autonomous System Border Router	Yes
RFC 1583 Compatibility	Yes
NSSA ASBR-Default-Route Translator	Enabled
ABR-type	Standard
Distance	<input type="text"/>
Default-Information	<input type="text"/>
SPF Delay	1
SPF Hold Time	10
Trace Level	Critical-Trace
GR Trace-Level	Restarting-router
	<input type="button" value="ADD"/>

Select	Context Name	Router Id	Autonomous System	RFC 1583 Compatibility	NSSA ASBR Default-Route	ABR-type	Distance	Default-Information	SPF Delay	SPF Hold Time	Trace Level
<input type="radio"/>	default	0.0.0.0	No	Yes	Disabled	Standard	110	0	1	10	Critical-T

Label	Description
<b>Context Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Router ID/Router Id</b>	Enter a 32-bit integer uniquely identifies the originating router in the Autonomous System.
<b>Autonomous System Border Router/ Autonomous System</b>	Select the status of an ASBR (AS Border Router). The default option is <b>Yes</b> . The list contains: <ul style="list-style-type: none"> <li>– Yes - Configures the router as an ASBR.</li> <li>– No - Configures the router within Autonomous System (AS).</li> </ul>
<b>RFC 1583 Compatibility</b>	Select the compatibility status of RFC 1583 or RFC 2178. This Controls the preference rules, when choosing among multiple AS external LSAs advertising the same destination The default option is Yes. The list contains: <ul style="list-style-type: none"> <li>– Yes – Sets the preference rules specified by the RFC 1583.</li> </ul>



	<ul style="list-style-type: none"> <li>- No - Sets the preference rules specified by the RFC 2178.</li> </ul>
<b>NSSA ASBR Default Route Translator/ NSSA ASBR Default Route</b>	<ul style="list-style-type: none"> <li>- Select the status of the P-Bit setting for the default Type-7 LSA (Link State Advertisement) generated by NSSA internal ASBR. (which is not ABR (Area Border Router)). The default option is Disabled. The list contains: <ul style="list-style-type: none"> <li>- Enabled - Sets the P-Bit in the generated Type-7 default LSA.</li> <li>- Disabled - Clears the P-Bit in the generated default LSA.</li> </ul> </li> </ul>
<b>ABR Type</b>	<p>Select the type of ABRs supported. The default option is Standard. The list contains:</p> <ul style="list-style-type: none"> <li>- Standard - Supports the ABR type as Standard.</li> <li>- CISCO - Supports the ABR type as CISCO.</li> <li>- IBM - Supports the ABR type as IBM.</li> </ul>
<b>Distance</b>	<p>Enter the administrative distance (the metric to reach destination) of the routing protocol. This value ranges from 1 to 255. The default value is <b>0</b>. The value 0 represents the directly connected route.</p>
<b>Default Information</b>	<p>Enter the default information that is to be used for configuring the OSPF basic settings. This value ranges from 0 to 65535.</p>
<b>SPF Delay</b>	<p>Configures the interval by which SPF calculation is delayed after a topology change reception. This value ranges from 0 to 65535 seconds. The default value is <b>1</b>.</p>
<b>SPF Hold Time</b>	<p>Configures the minimum time between two consecutive SPF calculations. This value ranges from 0 to 65535 seconds. The default value is <b>10</b>.</p>
<b>Trace Level</b>	<p>Select the level of trace required for OSPF. The list contains:</p> <ul style="list-style-type: none"> <li>- Packet High Level Dump Trace - Generates debug statements for Packet High Level Dump trace.</li> <li>- Packet Low Level Dump Trace - Generates debug statements for Packet Low Level Dump trace.</li> <li>- Packet Hex Dump Trace - Generates debug statements for Packet Hex Dump trace.</li> <li>- Critical Trace - Generates debug statements for Critical</li> </ul>

	<p>trace.</p> <ul style="list-style-type: none"><li>- Function Entry Trace - Generates debug statements for Function Entry trace.</li><li>- Function Exit Trace - Generates debug statements for Function Exit trace.</li><li>- Memory Allocation Success Trace - Generates debug statements for</li><li>- Memory Allocation Success Trace.</li><li>- Memory Allocation Failure Trace - Generates debug statements for Memory Allocation Failure Trace.</li><li>- Hello packet Trace - Generates debug statements for Hello packet Trace.</li><li>- DDP packet Trace - Generates debug statements for DDP packet Trace.</li><li>- Link State Request Packet Trace - Generates debug statements for Link State Request Packet Trace.</li><li>- Link State Update Packet Trace - Generates debug statements for Link State Update Packet Trace.</li><li>- Link State Acknowledge Packet Trace - Generates debug statements for Link State Acknowledge Packet Trace.</li><li>- Interface State Machine Trace - Generates debug statements for Interface State Machine Trace.</li><li>- Neighbor State Machine Trace - Generates debug statements for Neighbor State Machine Trace.</li><li>- Routing Table Calculation Trace - Generates debug statements for Routing Table Calculation Trace.</li><li>- RTM Module Trace - Generates debug statements for RTM Module Trace.</li><li>- Interface Trace - Generates debug statements for Interface Trace.</li><li>- NSSA Trace - Generates debug statements for NSSA Trace.</li><li>- Route Aggregation Trace - Generates debug statements for Route Aggregation Trace.</li></ul>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> <li>- Configuration Trace - Generates debug statements for Configuration Trace.</li> <li>- Adjacency formation Trace - Generates debug statements for Adjacency formation Trace.</li> <li>- Link State Database Trace - Generates debug statements for Link State Database Trace.</li> <li>- Protocol Packet Processing Trace - Generates debug statements for Protocol Packet Processing Trace.</li> </ul>
<b>GR Trace-Level</b>	<p>Select the graceful restart trace level for OSPF. The list contains:</p> <ul style="list-style-type: none"> <li>- restarting-router - Generates debug statements for messages related to restarting router.</li> <li>- helper - Generates debug statements for messages related to router in helper Mode.</li> <li>- redundancy - Generates debug statements for redundancy messages.</li> </ul>
<b>Select</b>	<p>Click to select the Context Name for which the configurations need to be modified or deleted.</p>

### 4.3.8.3 Area

This screen allows the user to configure the parameters of the router’s attached areas

Context Name	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
<input type="button" value="ADD"/> <input type="button" value="Reset"/>	

Select	Context Name	Area ID	Type	Send Summary Routes	Stub Metric	Stub Metric Type	TOS	Translator Role	Stability Interval	SPF Run Count
<input type="radio"/>	default	0.0.0.0	Normal	No	10	ospfMetric	0	candidate	40	0

Label	Description
<b>Context Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Area ID</b>	Enter the IP Address that uniquely identifies an area that

	associated with the OSPF address range for which authentication is to be enabled.
<b>Type</b>	Select the required type for an area. The default option is <b>Normal</b> . The list contains: <ul style="list-style-type: none"> <li>– Normal - Allows all the external LSAs (Type 5 LSA) to be flooded through the area.</li> <li>– NSSA - Allows only limited number of Type 5 external LSA to be translated into Type 7 LSA and flooded into the area.</li> </ul>
<b>Send Summary Routers</b>	Select 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 default option is <b>NO</b> . The list contains: <ul style="list-style-type: none"> <li>– Yes - Router will summarize and propagate summary LSAs.</li> <li>– No - Router does not originate or propagate summary LSAs.</li> </ul>
<b>Stub Metric</b>	Enter the metric value applied at the indicated type of service. This is applicable to stub and NSSA area. This value ranges from 0 to 16777215. The default value is <b>10</b> .
<b>Stub Metric type</b>	Select the type of metric advertised as a default route. This is applicable to stub and NSSA area. The default option is <b>ospfMetric</b> . The list contains: <ul style="list-style-type: none"> <li>– ospfMetric - Sets the metric type as ospfMetric.</li> <li>– comparableCost - Sets the metric type as comparable cost.</li> <li>– nonComparable - Sets the metric type as non-comparable.</li> </ul>
<b>TOS</b>	Enter the type of service associated with the metric. This is applicable to stub and NSSA area. The default value is <b>zero</b> .
<b>Translator Role</b>	Select an NSSA border router's ability to perform NSSA translation of Type-7 LSAs to Type-5 LSAs. The default option is <b>Candidate</b> . The list contains: <ul style="list-style-type: none"> <li>– Always - Sets the translator role as always to perform NSSA translation of Type-7 LSAs to Type-5 LSAs.</li> <li>– Candidate - Sets the translator role as candidate to perform NSSA translation of Type-7 LSAs to Type-5 LSAs</li> </ul>

<b>Stability Interval</b>	Enter 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 from 0 to 2147483647. The default option is <b>40 seconds</b> .
<b>SPF Run Count</b>	Displays the shortest path first (SPF) run count depends upon the metric type value. This value ranges from 0 to 65535. This field is greyed out.
<b>Select</b>	Click to select the context Name for which the OSPF Area configurations need to be modified or deleted.

### 4.3.8.4 Interface

This screen allows the user to configure OSPF for the specified interface.

Select	Context Name	IP Address	Area ID	Priority	Designated Router	Authentication Type	MD5 Key Id	Authentication Key	Metric	Passive	Demand Circuit	If Type	Transit Delay	Retransmit Delay	Hello Interval	Router Dead Interval
--------	--------------	------------	---------	----------	-------------------	---------------------	------------	--------------------	--------	---------	----------------	---------	---------------	------------------	----------------	----------------------

Label	Description
<b>Context Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Interface</b>	Select the interface index of the port which is already configured.
<b>Area ID</b>	Enter the IP Address that uniquely identifies an area that associated with the OSPF address range for which authentication is to be enabled.
<b>Priority</b>	Enter the priority of the interface, which is used in the DR (Designated Router) election algorithm. When two routers

	<p>attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. This value ranges from 0 to 255. The default value is 1</p>
<b>Authentication Type</b>	<p>Enter the type of authentication used on the interface. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– None - Sets the authentication type as no password authentication.</li> <li>– Simple Password - Sets the authentication type as Simple password type authentication.</li> <li>– MD5 - Sets the authentication type as Message Digest 5 based authentication.</li> <li>– SHA-1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.</li> <li>– SHA-224 - Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.</li> <li>– SHA-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.</li> <li>– SHA-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.</li> <li>– SHA-512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.</li> </ul>
<b>MD5 Key ID/ MD5 Key Id</b>	<p>Enter the secret key used to create the message digest appended to the OSPF packet if the authentication type is MD5. This value ranges from 0 to 255</p>
<b>Authentication Key</b>	<p>Enter the key required for authentication, if authentication is enabled on this interface.</p>
<b>Metric</b>	<p>Enter the metric of using the type of service on the interface. This value ranges from 1 to 65535. The default value is <b>10</b>.</p>

<b>Passive</b>	<p>Select the interface as passive or normal. The default option is <b>No</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Yes - Sets the interface as passive.</li> <li>- No - Sets the interface as normal.</li> </ul>
<b>Demand Circuit</b>	<p>Select the Demand OSPF procedures that should be performed on this interface. The default option is <b>No</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- No - Demand OSPF procedures do not perform on the selected interface.</li> <li>- Yes - Demand OSPF procedures perform on the selected interface.</li> </ul>
<b>If Type</b>	<p>Select the OSPF interface type. The default option is <b>broadcast</b>.</p> <p>The list contains:</p> <ul style="list-style-type: none"> <li>- Broadcast - Specifies that the network supports many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast)</li> <li>- nbma Specifies that the network supports many (more than two) routers, but having no broadcast capability</li> <li>- point-to-point - Sets the network type to point-to-point that joins a single pair of routers.</li> <li>- point-to-multipoint - Sets the network type to point-to-multipoint and treats the non-broadcast network as a collection of point-to-point links.</li> </ul>
<b>Transit Delay</b>	<p>Enter the number of seconds taken to transmit a link state update packet over the interface. This value ranges from 0 to 3600 seconds. The default option is <b>1 second</b>.</p>
<b>Retransmit Interval</b>	<p>Enter the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. The retransmit-interval value is also used while retransmitting database description and link-state request packets. This value ranges from 0 to 3600 seconds. The default option is <b>5 seconds</b>.</p>

<b>Hello Interval</b>	Enter the length of time, in seconds, between the OSPFv3 hello packets on a particular interface (the length of time, in seconds, between the Hello packets that the router sends on the interface). This value ranges from 1 to 65535 seconds. The default option is <b>10 seconds</b> .
<b>Dead Interval</b>	Enter the time period for which the router waits for hello packet from the neighbor before declaring this neighbor down. This value ranges from 0 to 2147483647 seconds. The default option is <b>40 seconds</b> .
<b>IP Address</b>	Displays the IP Address of the OSPF interface. This is a read-only field.
<b>Designated Router</b>	Displays the IP Address of the Designated Router. This is a read-only field.
<b>Select</b>	Click to select the context name for which the OSPF Interface configurations need to be done.

### 4.3.8.5 Virtual Interface

This screen allows the user to configure an OSPF virtual link and its related parameters.

[Select](#)|[Context Name](#)|[Transit Area ID](#)|[Neighbor Router ID](#)|[Authentication Type](#)|[MD5 Key ID](#)|[Authentication Key](#)|[Hello Interval](#)|[Router Dead Interval](#)|[Transit Delay](#)|[Retransmit Interval](#)

Label	Description
<b>Context Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Transit Area ID</b>	Enter the 32-bit integer uniquely identifying an area, which is traversed by the virtual link.
<b>Neighbor Router ID</b>	Enter the router ID of the virtual neighbor.



<b>Authentication Type</b>	<p>Select the type of authentication used on the interface. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– None - Sets the authentication type as no password authentication.</li> <li>– Simple Password - Sets the authentication type as Simple password type authentication.</li> <li>– MD5 - Sets the authentication type as Message Digest 5 based authentication.</li> <li>– SHA-1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.</li> <li>– SHA-224 - Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.</li> <li>– SHA-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.</li> <li>– SHA-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.</li> <li>– SHA-512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.</li> </ul>
<b>MD5 Key ID</b>	<p>Enter the secret key used to create the message digest appended to the OSPF packet if the authentication type is md5. This value ranges from 1 to 255</p>
<b>Authentication Key</b>	<p>Enter the key required for authentication, if authentication is enabled on this interface.</p>
<b>Hello Interval</b>	<p>Enter the length of time, in seconds, between the Hello packets send on the interface. This value ranges from 1 to 65535 seconds. The default option is <b>10 seconds</b>.</p>
<b>Router Dead Interval</b>	<p>Enter the number of seconds that a router's Hello packets have not been seen before it's neighbors declare the router as down. This value ranges from 0 to 2147483647 seconds. The default</p>

	option is <b>60 seconds</b> .
<b>Transit Delay</b>	Enter the number of seconds taken to transmit a link state update packet over the interface. This value ranges from 0 to 3600 seconds. The default option is <b>1 second</b> .
<b>Retransmit Interval</b>	Enter the number of seconds between link-state advertisement retransmissions, for adjacencies belonging to the interface. This value ranges from 0 to 3600 seconds. The default option is <b>5 seconds</b> .
<b>Select</b>	Click to select the Context name for which the Virtual Interface configurations need to be modified or deleted.

### 4.3.8.6 Neighbor

This screen allows the user to configure the neighbor router and its priority.

Context Name \*

Neighbor IP Address \*

Priority

**Note : Neighbor can be configured on NBMA or point-to-multipoint networks**

Select	Context Name	Neighbor IP Address	Neighbor Priority
--------	--------------	---------------------	-------------------

Label	Description
<b>Context Name</b>	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.
<b>Neighbor IP Address</b>	Enter the IP address that is used by the neighbor in the IP source address. Based on the Neighbor router ID the priority of the neighbor is defined.
<b>Priority</b>	Enter the priority of the neighbor in the designated router election algorithm. This value ranges from 0 to 255. The default value is 1. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network
<b>Select</b>	Click to select the Context name for which the priority needs to

	be modified or deleted.
--	-------------------------

### 4.3.8.7 RRD Route

This screen allows the user to configure metric type and route type information to be applied to the routes learnt from the RTM.

Context Name	default <input type="button" value="v"/> *
Destination Network	<input type="text"/> *
Network Mask	<input type="text"/> *
Route Metric	10
Route Metric Type	asexttype2 <input type="button" value="v"/>
Route Tag	0
<input type="button" value="ADD"/> <input type="button" value="Reset"/>	

Select	Context Name	Dest Network	Network Mask	Metric	Metric Type	Route Tag
--------	--------------	--------------	--------------	--------	-------------	-----------

Label	Description
<b>Context Name</b>	Select the VRF name to configure parameters to the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Destination Network</b>	Enter the IP address of the destination route.
<b>Network Mask</b>	Enter the mask for the given destination route.
<b>Metric</b>	Enter the metric value applied to the route before it is advertised into the OSPF domain. This value ranges from 1 to 16777215. The default value is <b>10</b> .
<b>Metric Type</b>	Select the metric type applied to the route before it is advertised into the OSPF domain The default option is <b>asexttype2</b> . The list contains: <ul style="list-style-type: none"> <li>- asexttype1 - Sets the route metric type as AS-External type 1 before it is advertised.</li> <li>- asexttype2 - Sets the route metric type as AS-External type 2 before it is advertised.</li> </ul>
<b>Route Tag</b>	Sets the tag type which describes whether Tags will be

	automatically generated or will be manually configured. This value ranges from 0 to 4294967295. The default value is <b>0</b> .
<b>Select</b>	Click to select the Context Name for which the configurations need to be modified or deleted.

### 4.3.8.8 Aggregation

This screen allows the user to configure the External Tag for configured Type-7 address ranges.

The screenshot shows a configuration form with the following fields and values:

- Context Name: default \*
- Area ID: (empty) \*
- Lsdb Type: summaryLink \*
- Network: (empty) \*
- Mask: (empty) \*
- Advertise: advertiseMatching
- External Tag: 0

Buttons: ADD, Reset

Select	Context Name	Area ID	Lsdb Type	Network	Mask	Advertise	External Tag
--------	--------------	---------	-----------	---------	------	-----------	--------------

Label	Description
<b>Context Name</b>	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.
<b>Area ID</b>	Enter the 32-bit integer uniquely identifying the area in which the address aggregate is to be found.
<b>Lsdb Type</b>	Select the Lsdb type of the address aggregate. The default option is <b>summaryLink</b> . The list contains: <ul style="list-style-type: none"> <li>summaryLink - Sets the LSA type as summary LSA</li> <li>nssaExternalLink - Sets the LSA type as NSSA external Link</li> </ul>
<b>Network</b>	Enter the IP address of the Net that enables the OSPF routing for interfaces defined and to remove the area ID of that

	interface. When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.
<b>Mask</b>	Enter the Subnet Mask that pertains to the Net or Subnet for the given destination IPv4 address.
<b>Advertise</b>	Select whether the subnets are advertised outside the area or not. The default option is <b>advertiseMatching</b> . The list contains: <ul style="list-style-type: none"> <li>- advertiseMatching - Allows the subnets subsumed by ranges to trigger the advertisement of the indicated aggregate.</li> <li>- doNotAdvertiseMatching - Does not advertise subnets outside the area.</li> </ul>
<b>External Tag</b>	Enter the external tag attached to the external route. This tag is used to communicate information between AS boundary routers. The default value is <b>zero</b> .
<b>Select</b>	Click to select the context Name for which the configurations need to be modified or deleted.

#### 4.3.8.9 AsExAggregation

Context Name \*

Network \*

Mask \*

Area ID \*

Aggregation Effect

Translation

Select | Context Name | Network | Network Mask | Area ID | Advertise | Translation

Label	Description
<b>Context Name</b>	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.
<b>Network</b>	Enter the IP address of the Net that enables the OSPF routing for interfaces defined and to remove the area ID of that interface. When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.
<b>Mask</b>	Enter the Subnet mask for the given destination IPv4 address.
<b>Area ID</b>	Enter the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
<b>Aggregation Effect</b>	<p>Select whether Type-5/Type-7 will be aggregated or not. The default option is <b>advertise</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– advertise - Generates aggregated Type-5 if the associated Area ID is</li> <li>– 0.0.0.0. Generates aggregated Type-7 in the corresponding NSSA area if Area ID is other than 0.0.0.0.</li> <li>– 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.</li> <li>– 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.</li> <li>– 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</li> </ul>
<b>Translation</b>	<p>Select the P Bit setting in the generated Type-7 LSA. The default option is <b>enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– enabled - Sets P Bit in the generated Type-7 LSA.</li> <li>– disabled - Clears the P Bit in the generated Type-7 LSA.</li> </ul>
<b>Select</b>	Click to select the context name for which the configurations need to be modified or deleted.

### 4.3.8.10 GraceRestart

This screen allows the user to configure graceful restart feature for OSPF. The graceful restart mechanism allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over.

Context Name	default *
Opaque Option	Enable
Restart Support	None
Restart Grace LSA Ack	Enable
Grace LSA Retransmit Count	2
Restart Interval	120
Restart Reason	Unknown
Helper Support:	<input type="checkbox"/> UnKnown <input type="checkbox"/> S/W Restart <input type="checkbox"/> S/W Reload UpGrade <input type="checkbox"/> Switch to Redundant
Helper Strict LSA Checking	False
Helper Grace Time Limit	0

Label	Description
<b>Context Name</b>	Select the VRF name to configure the graceful restart feature for the specified VRF instance. This value represents a unique name of the VRF instance.
<b>Opaque Option</b>	Select the opaque-capable option. The default option is <b>Disable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Enables the opaque-capable option.</li> <li>- Disable - Disables the opaque-capable option.</li> </ul>
<b>Restart Support</b>	Select the router support for the OSPF graceful restart feature. The default option is <b>None</b> . The list contains: <ul style="list-style-type: none"> <li>- None - Does not restart support for the OSPF graceful restart feature.</li> <li>- Planned Only - Restarts support for the OSPF graceful restart feature only in planned state.</li> <li>- Planned and Unplanned - Restarts for the OSPF graceful</li> </ul>

	restart feature both in planned and unplanned state.
<b>Restart Grace LSA Ack</b>	<p>Select whether the Grace LSAs sent by the router are expected to be acknowledged by the peers, if the Grace Ack Required state is enabled. The default option is <b>Enable</b>. The list contains::</p> <ul style="list-style-type: none"> <li>– Enable - Grace LSAs sent by the router are acknowledged by the peers.</li> <li>– Disable - Grace LSAs sent by the router are not acknowledged.</li> </ul>
<b>Grace LSA Retransmit Count</b>	<p>Enter the number of retransmissions for unacknowledged Grace LSAs. This value ranges from 0 to 180. The default value is <b>2</b>.</p>
<b>Restart Interval</b>	<p>Enter the OSPF graceful restart timeout interval. This value Specifies the graceful restart interval, in seconds, during which the restarting router has to reacquire OSPF neighbors that are fully operational prior to the graceful restart. This value ranges from 1 to 1800. The default value is <b>120</b>.</p>
<b>Restart Reason</b>	<p>Select the router restart reason code of the OSPF graceful restart feature. The default option is <b>Unknown</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– UnKnown - Restarts the system due to unplanned events (such as restarting after a crash).</li> <li>– S/W Restart - Restarts the system due to software restart.</li> <li>– S/W Reload UpGrade - Restarts system due to reloading / upgrading of software.</li> <li>– Switch to Redundant - Restarts system due to switch over to a redundant support processor.</li> </ul>
<b>Helper Support</b>	<p>Select the router helper support for the OSPF graceful restart feature. The default option is <b>set</b>. The options are:</p> <ul style="list-style-type: none"> <li>– UnKnown - Sets the helper support for restarting of system due to unplanned events (such as restarting after a crash).</li> <li>– S/W Restart - Sets the helper support for restarting of system due to restart of software.</li> <li>– S/W Reload UpGrade - Sets the helper support for</li> </ul>



	restarting of system due to reload or upgrade of software. <ul style="list-style-type: none"> <li>- Switch to Redundant - Sets the helper support for restarting of system due to switch over to a redundant support processor.</li> </ul>
<b>Helper Strict LSA Check</b>	Select whether strict LSA checking is enabled for the graceful restart. The default option is <b>False</b> . The list contains: <ul style="list-style-type: none"> <li>- True - Strict LSA checking is enabled for the graceful restart.</li> <li>- False - Strict LSA checking is disabled for the graceful restart.</li> </ul>
<b>Helper Grace Time Limit</b>	Enter the OSPF graceful restart interval limit, in seconds, in the helper side. During this period, the router advertises that the restarting router is active and is in FULL state. This value ranges from 0 to 1800 seconds. The default option is <b>0 seconds</b> .

### 4.3.9 PRD

RRD (Route Redistribution) allows different routing protocols to exchange routing information. Using a routing protocol to advertise routes that are learnt by other means, such as, another routing protocol, static routes, or directly connected routes, is called redistribution. While running a single routing protocol throughout an entire IP internetwork is desirable, multi-protocol routing is widespread for a number of reasons, for example, company mergers, multiple departments managed by multiple network administrators, and multi-vendor environments. If a single routing protocol cannot be used, route redistribution is the only solution. Running different routing protocols is often part of a network design.

Each routing protocol on a network is separated into an Autonomous System (AS). All routers in the same autonomous system (running the same routing protocol) have complete knowledge of the entire AS. A router that connects two (or more) autonomous systems is known as a Border Router. A border router advertises routing information from one AS to the other AS(s). It is only possible to redistribute routing information for like routed protocols. Different routing protocols have different and often incompatible algorithms and metrics.

BGP Status	Disabled ▾
Import Routes	Direct ▾
RouteMap Name	<input type="text"/>
Metric Value	<input type="text" value="0"/>
Match Type	<input type="text"/>
VRF Name	<input type="text"/> *
<input type="button" value="ADD"/>	

Select	BGP Status	Imported Route Type	RouteMap Name	Metric Value	Match Type	Context Name
--------	------------	---------------------	---------------	--------------	------------	--------------

Label	Description
<b>BGP Status</b>	Select the route redistribution status for BGP. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled – Imports the specified routes 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</li> <li>– Disabled – Removes the specified routes from BGP and does not distribute or import routes from IGP (RIP and OSPF).</li> </ul>
<b>Import Routes</b>	Select the routes to import and control the redistribution of routes. The default option is <b>Direct Routes</b> . The list contains; <ul style="list-style-type: none"> <li>– Direct routes – Enables import of directly connected routes into BGP</li> <li>– Static routes – Enables import of static routes into BGP.</li> <li>– RIP routes – Enables import of RIP routes into BGP.</li> <li>– OSPF routes – Enables import of OSPF routes into BGP.</li> </ul>
<b>RouteMap Name</b>	Enter the route map name that identifies the specified route-map in the list of route-maps. This value is a string of maximum size 20.
<b>Metric Value</b>	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 from 0 to 4294967295.
<b>Match Type</b>	Select the Metric type applied to the route before it is advertised into the OSPF domain <ul style="list-style-type: none"> <li>- External – Redistributes OSPF external routes</li> <li>- internal - Redistributes OSPF internal routes</li> <li>- NSSA-External – Redistributes OSPF NSSA external routes</li> </ul>
<b>VRF Name</b>	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 of maximum size 32.
<b>Select</b>	Click to select the BGP routes for which RRD status needs to be deleted.

## 4.3.10 VRRP

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP routers(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment.

### 4.3.10.1 VRRP Global Settings

This screen allows the user to set the global status of VRRP in the switch.

VRRP Version

VRRP Status

Auth Deprecate Status

Notification Control

VRRP Version	VRRP Status	Auth Deprecate	Notification Control
VRRP_VE	VRRP_ST.	AUTH_DE	NOTIF_CN

Label	Description
<b>VRRP Version</b>	Select which VRRP version to use.
<b>VRRP Status</b>	Select the global status of the VRRP in the switch. The default option is <b>Disabled</b> Options are: <ul style="list-style-type: none"> <li>- Enabled - Enables the VRRP in the switch.</li> <li>- Disabled - Disables VRRP.in the switch</li> </ul>
<b>Auth Deprecate Status</b>	Select the option to enable or disable authentication status. The default option is <b>Enabled</b> . Options are: <ul style="list-style-type: none"> <li>- Enabled - Sets the authentication to Type 0 alone.</li> <li>- Disabled - Sets the authentication to any one of the values Type 0-2 and the authentication feature is compatible with RFC 2338.</li> </ul>
<b>Notification Control</b>	Enable or disable notification control function.

### 4.3.10.2 Track Settings

Group Number

No. of Link

Interface

Select	Group No	No of Links	Interface
--------	----------	-------------	-----------

Label	Description
<b>Group Number</b>	Identifies the VRRP group. It can be a value from 0 through 255.
<b>No. of Link</b>	Specify the number of links to be tracked
<b>Interface</b>	Specify the interface to be tracked.

### 4.3.10.3 VRRP Virtual Router Settings

This screen allows the user to configure the VRRP parameters.

Select	Virtual Router ID	Interface	Address Type	Primary IP	Priority	Authentication Type	Authentication Key	Advertisement Interval (msecs)	Pre-emption	Accept Mode	Group No	Decrement Priority	Virtual MAC	Master Ip Addr	Oper State	Admin Status
--------	-------------------	-----------	--------------	------------	----------	---------------------	--------------------	--------------------------------	-------------	-------------	----------	--------------------	-------------	----------------	------------	--------------

Label	Description
<b>Virtual Router ID</b>	Enter the virtual ID associated with each virtual router. This value ranges from 1 to 255.
<b>Interface</b>	Select the interface from the list of available vlan interfaces to configure the virtual router.
<b>Primary IP Address</b>	Enter the Primary IP Address for the virtual router. This is the IP address listed as the source in VRRP advertisement last received by this virtual router. The default value is <b>0.0.0.0</b> .
<b>Secondary IP Address</b>	Enter the Secondary IP Address for the virtual router.
<b>Priority</b>	Enter the priority to be used for the virtual router master election process. This value ranges from 1 to 254. The default value is <b>100</b>
<b>Authentication Type</b>	Select the authentication type for the VRRP Protocol exchanges. The default option is <b>no Authentication</b> . Options are: <ul style="list-style-type: none"> <li>no Authentication – Configures the authentication type as</li> </ul>

	No Authentication. This implies that the VRRP protocol exchanges are not authenticated.
<b>Authentication Key</b>	Enter the authentication key for the virtual router. This field is an octet string of maximum size 16.
<b>Advertisement Interval (Secs)</b>	Enter the time interval, in seconds, for sending the advertisement packets. Only the master router sends the VRRP Advertisements, This value ranges from 1 to 255 seconds. The default value is <b>1</b> second.
<b>Pre-emption</b>	Select the option to enable or disable pre-emption of state change from either Backup to Master or vice versa based on the election process. This controls whether a higher priority virtual router will preempt a lower priority master. The default option is <b>Enable</b> . Options are: <ul style="list-style-type: none"> <li>– Enable - Enables pre-emption of state change from either Backup to Master or vice versa based on the election process.</li> <li>– Disable - Disables pre-emption of state change from either Backup to Master or vice versa based on the election process.</li> </ul>
<b>State</b>	Displays the current state of the virtual router. This is a read-only field. The list contains: <ul style="list-style-type: none"> <li>– Initialize – Specifies that the virtual router is waiting for a startup event.</li> <li>– Backup – Specifies that the virtual router is monitoring the availability of the master router.</li> <li>– Master – Specifies that the virtual router is forwarding packets for IP addresses that are associated with the router.</li> </ul>
<b>Status</b>	Select the option to enable/disable the virtual router function. The default value is <b>Down</b> . Options are: <ul style="list-style-type: none"> <li>– Up – Transits the state of the virtual router from initialize to backup or master based on the priority value.</li> <li>– Down – Transits the state of the virtual router from master or backup to initialize.</li> </ul>

### 4.3.10.4 Associated IP

Virtual Router ID	<input type="text"/> *
Interface	<input type="text"/> ▼ *
Address-Type	<input type="text"/> ▼ *
Secondary IP Address	<input type="text"/> *
<input type="button" value="ADD"/>	

Select	Virtual Router ID	Interface	Address Type	Assoc IP
--------	-------------------	-----------	--------------	----------

Label	Description
<b>Virtual Router ID</b>	Enter the virtual ID associated with each virtual router. This value ranges from 1 to 255.
<b>Interface</b>	Select the interface from the list of available vlan interfaces to configure the virtual router.
<b>Secondary IP Address</b>	Enter the Secondary IP Address for the virtual router.

## 4.4 Multicast

### 4.4.1 IGMP Snooping

IGMP (Internet Group Management Protocol) is the protocol, a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGS (IGMP Snooping) is a feature that allows the switch to listen in on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, the other computer can learn the multicast sessions to which the computers on the local network are listening. IGS significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

#### 4.4.1.1 Basic Settings

This screen allows the user to configure basic settings such as IGMP snooping status, operational status, Snooping Mode, Proxy Reporting and Snoop Leave level.

System Control Start

Select	IGMP Snooping Status	Operational Status	Snooping Mode	Proxy Reporting	Snoop Leave Level	Snoop Report process config-level	Enhanced Mode	Sparse Mode
<input checked="" type="radio"/>	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Mac Based <input type="button" value="v"/>	Enabled <input type="button" value="v"/>	Vlan Based <input type="button" value="v"/>	Non-RouterPorts <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>
Select	Proxy Status	Filter Status	Multicast Vlan	Report Forwarding	Query Forwarding	Retry Count	Query Transmit On TC	
<input type="radio"/>	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Router Ports <input type="button" value="v"/>	Non-Router Ports <input type="button" value="v"/>	2	Disabled <input type="button" value="v"/>	

Label	Description
<b>System Control</b>	<p>Select the System Control status of IGS in the switch. The default option is <b>Start</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> </ul>
<b>Select</b>	Select the option button to configure the selected parameters
<b>IGMP Snooping Status</b>	<p>Select the Global status of IGS in the switch. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Starts the IGMP snooping protocol operations.</li> <li>– Disabled – Stops performing the IGMP snooping protocol operations.</li> </ul>
<b>Operational Status</b>	<p>Displays the Operational status of the IGS in the switch. The default option is <b>disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Indicates that IGS protocol is currently enabled in the system.</li> <li>– Disabled - Indicates that IGS protocol is currently disabled in the system</li> </ul>
<b>Snooping Mode</b>	<p>Select the IGMP snooping mode. Modes are provided with redundancy support. The default option is <b>MAC Based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– IP based – IGS protocol operation is based on the IP address and group address. This mode is chosen if the</li> </ul>



	<p>hardware supports programming of S, G and *, and G entries</p> <ul style="list-style-type: none"> <li>– MAC based - Hardware supports only MAC based multicast tables and the snooping protocol operation is based only on the group address.</li> </ul>
<b>Proxy Reporting</b>	<p>Select the Proxy Reporting status in the switch. IGS network traffic gets reduced. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Switch generates reports and forwards them to the router, based on the available host information.</li> <li>– Disabled – Switch acts as transparent snooping bridge. The switch forwards all v3 reports and a single v2 report to the router.</li> </ul>
<b>Snoop Leave Level</b>	<p>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. The default option is <b>Vlan Based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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 an interface can be used for processing the leave messages.</li> </ul>
<b>Snoop Report process config-level</b>	<p>Select the report processing mechanism to be used for handling the incoming report messages to be processed. The default option is <b>Non-RouterPorts</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Non-RouterPorts – The incoming report messages are</li> </ul>

	<p>processed only in the non-router ports. Report message received on the router ports are not processed.</p> <ul style="list-style-type: none"> <li>– All-Ports – The incoming report messages are processed in all the ports inclusive of router ports.</li> </ul>
<b>Enhanced Mode</b>	<p>Select the operating status of snooping module. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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 &amp; 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.</li> <li>– 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.</li> </ul>
<b>Sparse Mode</b>	<p>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. The default option is <b>disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – The IGS module drops the unknown multicast traffic when there is no listener for the multicast data</li> <li>– Disabled – The IGS module forwards the unknown</li> </ul>

	<p>multicast traffic. The multicast data gets flooded to the member port of VLAN.</p>
<b>Proxy Status</b>	<p>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:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables proxy in the system. The switch act as querier for all downstream interfaces and act as host for all upstream interfaces.</li> <li>– Disabled – Disables proxy in the system.</li> </ul>
<b>Filter Status</b>	<p>Select the filter status. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– Disabled – Disables 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.</li> </ul>
<b>Multicast Vlan</b>	<p>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. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the multicast 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.</li> </ul>

	<ul style="list-style-type: none"> <li>– 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.</li> </ul>
<b>Report Forwarding</b>	<p>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. The default option is <b>Router Ports</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Router Ports – Forwards reports only on the router ports</li> <li>– All Ports – Forwards reports on all ports of the VLAN</li> <li>– Non-edge - Forwards the reports on non-edge ports detected by spanning tree protocol</li> </ul>
<b>Query Forwarding</b>	<p>Select whether the query to be forwarded to the entire member ports of the VLAN or to Non-router Ports. The default option is <b>Non- Router Ports</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– All Ports – The query messages are forwarded to all the member ports of the VLAN.</li> <li>– Non-Router Ports – The query messages are forwarded only to the non- router ports.</li> </ul>
<b>Retry Count</b>	<p>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. The default value is <b>2</b>.</p>
<b>Query Transmit On TC</b>	<p>Select path redundancy for IGMP Snooping queries transmission to be enabled or disabled whenever topology changes. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– Disabled- Path redundancy is disabled and it leads to flooding of data.</li> </ul>

#### 4.4.1.2 Timer

This screen allows the user to set Router port purge interval, Group-Member Port Purge

Interval, Report Forward Interval and Group Query Interval.

Router Port PurgeInterval (Secs)	<input type="text" value="60"/>
Group-Member Port Purge Interval (Secs)	<input type="text" value="130"/>
Report Forward Interval (Secs)	<input type="text" value="25"/>
Group Query Interval (Secs)	<input type="text" value="5"/>

Label	Description
<b>Router Port Purge Interval (Secs)</b>	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 from 60 to 600 seconds. The default value is <b>125</b> seconds.
<b>Group-Member Port Purge Interval (Secs)</b>	Enter the time interval after which a learnt port entry is purged, if IGMP reports are not received on a port. This value ranges from 130 to 1225 seconds. The default value is <b>260</b> seconds.
<b>Report Forward Interval (Secs)</b>	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 from 1 to 25 seconds. The default value is <b>5</b> seconds.
<b>Group Query Interval (Secs)</b>	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 from 2 to 5 seconds. The default value is <b>2</b> seconds.

### 4.4.1.3 VlanConfiguration

This screen allows the user to configure IGMP Snooping on specific VLANs.

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	
Multicast Vlan Profile	
Max Response Code	
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

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	Multicast Vlan Profile	Max Response Code
--------	---------	----------------------	--------------------	-----------------	------------	---------------------------	------------------------	---------------------	------------------------------	------------------------	--------------------------------------	------------------	--------------------------	------------------------	-------------------

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN from the list specified already in the system. The IGMP snooping configuration is performed for this specific VLAN ID.
<b>IGMP Snooping Status</b>	Select the status of IGMP snooping on the specified VLAN. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– 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.</li> <li>– Disabled - IGS is disabled on the specified VLAN.</li> </ul>
<b>Operating Version</b>	Select the Operating Version of IGS for the specified VLAN. The default option is <b>Version 3</b> . The list contains: <ul style="list-style-type: none"> <li>– Version 1 – The port list connected to listeners of Multicast groups is built based on IGMP membership Reports, Query and Leave messages</li> <li>– 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.</li> </ul>

	<ul style="list-style-type: none"> <li>- 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.</li> </ul>
<b>Fast Leave</b>	<p>Select the Fast Leave status of IGS. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>
<b>Querier Status</b>	<p>Select whether the switch is configured as a querier in a VLAN. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Disabled – The switch is configured as non-querier, does not propagate any general query messages and does not take part in querier election.</li> </ul>
<b>Startup Query Count</b>	<p>Enter the number of queries to be sent during startup of querier election process at the interval of startup query interval. This value ranges from 2 to 5. The default value is <b>2</b>.</p>
<b>Startup Query Interval(secs)</b>	<p>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 from 15 to 150</p>

	seconds. The default value is <b>32</b> seconds.
<b>Querier Interval(secs)</b>	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 6 and 600 seconds. The default value is <b>125</b> seconds.
<b>Other Querier Present Interval(secs)</b>	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 from 120 to 1215 seconds. The default value is <b>255</b> seconds.
<b>Router Port List</b>	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. The default option is <b>None</b> .
<b>Blocked Router Port List</b>	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. The default option is <b>None</b> .
<b>Multicast Vlan Profile</b>	Select the multicast profile identification configured for a particular VLAN and is used for multicast VLAN classification. When any untagged report or leave message is received and the Group & Source address in the received packet matches any rule in this profile, the received packet is classified to be associated with the VLAN to which this profile is mapped.
<b>Max Response Code</b>	Enter the maximum response code advertised in queries which are sent over this VLAN. This value ranges from 0 to 255 tenths of a second. The default value is <b>100</b> .



### 4.4.1.4 Interface Configuration

This screen allows the user to configure IGMP Snooping on specific interface.

Interface Index	Ex0/4
Leave Mode	
Threshold Limit Type	-
Threshold Limit	
Rate Limit	
Filter Profile	
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	

Interface Index	Leave Mode	Threshold Limit Type	Threshold Limit	Rate Limit	Filter Profile Id
Gi0/4	Normal Leave	None	0	4294967295	0

Label	Description
<b>Interface Index</b>	Select the interface index of the port from the list specified already in the system
<b>Leave Mode</b>	<p>Select the mechanism to be used for processing leave messages in the down stream interface. The default option is <b>Normal Leave</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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</li> <li>- Normal Leave – A group or group specific query is sent on the interface when a leave message is received. Once</li> </ul>

	<p>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</p>
<b>Threshold Limit Type</b>	<p>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. The default option is <b>None</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– None – No limiting is done.</li> <li>– Groups – Limits the IGMP report message based on the group registration allowed per downstream interface.</li> <li>– Channels – Limit is applied only for IGMPv3 Include and Allow reports based on the S, G registration that are allowed per downstream interface.</li> </ul>
<b>Threshold Limit</b>	<p>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. This value ranges from 0 to 4294967295. The default value is <b>0</b>.</p>
<b>Rate Limit</b>	<p>Enter the rate limit for a down stream 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. This value ranges from 0 to 4294967295. The default value is <b>4294967295</b>.</p>
<b>Filter Profile</b>	<p>Select the Filter Profile Identifier. A unique identifier configured by the administrator for a particular Internet address type identifies each of the profile entries. The profile ID is configured for the downstream interface. The default value is <b>0</b>.</p>

### 4.4.1.5 RouterPortConf

This screen allows the user to configure the details of the router port.

VLAN ID	vlan1
Router Port List *	<input type="text"/>
V1/V2 Rtr Port Purge Interval	<input type="text"/>
Static Router Port Version	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>	

VLAN ID	Router Port	Router Port Config Version	Router Port Version	V1/V2 Router Port Purge Interval	V3 Router Port Purge Interval
---------	-------------	----------------------------	---------------------	----------------------------------	-------------------------------

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN from the list already specified in the system. The IGMP snooping configuration is performed for the entered VLAN ID.
<b>Router Port List</b>	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.
<b>V1/V2 Rtr Port Purge Interval</b>	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. This value ranges from 60 to 600. The default value is <b>125</b>
<b>Static Router Port Version</b>	Select the operating version of the IGMP proxy on the upstream router port from the list already specified in the system. The default option is <b>Version 3</b> . The list contains: <ul style="list-style-type: none"> <li>- Version1 – Indicates that the operating version of IGMP</li> </ul>

	<p>proxy is version 1</p> <ul style="list-style-type: none"> <li>- Version2 - Indicates that the operating version of IGMP proxy is version 2</li> <li>- Version3 - Indicates that the operating version of IGMP proxy is version 3</li> </ul>
<b>Router Port Config Version</b>	Displays the configured version of the IGMP Proxy on the upstream router port. The default value is <b>Version 3</b>
<b>Router Port</b>	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.
<b>Router Port Version</b>	Displays the operating version of the IGMP proxy on the upstream router port. The default value is <b>Version 3</b> .
<b>V3 Router Port Purge Interval</b>	Displays the time interval after which the switch assumes that there are no IGMP v3 routers present on the upstream port. 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. This value ranges from 60 to 600. The default value is <b>125</b> .

#### 4.4.1.6 RouterPorts

This screen displays the Router Port List table. The dynamic and static ports are listed in the screen.

<b>VLAN ID</b>	<b>Dynamic Port List</b>	<b>Static Port List</b>
----------------	--------------------------	-------------------------

Label	Description
<b>VLAN ID</b>	Displays the VLAN Identifier that uniquely identifies a specific VLAN on which router ports are learnt / configured.
<b>Dynamic Port List</b>	Displays the lists of ports on which routers are present.
<b>Static Port List</b>	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.
--	----------------------------------------------------------------------------------------------------------------

### 4.4.1.7 Static Entry

This screen allows the user to configure the IGMP snooping on static interface.

Select | VLAN ID | Group Address | Port List

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN from the list specified already in the system. The MAC based multicast forwarding entry is displayed for the requested VLAN ID.
<b>Group Address</b>	Enter the Group MAC Multicast address that is learnt.
<b>Port List</b>	Enter the learnt ports list for which the multicast data packets for the group will be forwarded.

### 4.4.1.8 FwdInformation

This screen displays the IGMP group information such as MAC based or IP based Multicast Forwarding Table and Multicast Forwarding table is populated with list of ports interested in receiving multicast traffic to avoid flooding of multicast data traffic.

VLAN ID | Group MAC Address | Port List

Label	Description
<b>VLAN ID</b>	Displays the VLAN Identifier that uniquely identifies a specific VLAN. The MAC based multicast forwarding entry is displayed

	for the requested VLAN ID.
<b>Group MAC Address</b>	Displays the Group MAC Multicast address that is learnt.
<b>Port List</b>	Displays the learnt ports list for which the multicast data packets for the group will be forwarded.

### 4.4.1.9 McastReceiverInfo

This screen displays multicast report sent by each host in a multicast group requesting data from a specific source.

<b>Vlan Id</b>	<b>Group IP</b>	<b>Port</b>	<b>Host IP</b>	<b>Source IP</b>	<b>Filter Mode</b>
----------------	-----------------	-------------	----------------	------------------	--------------------

Label	Description
<b>Vlan Id</b>	Displays the VLAN ID pertaining to the multicast receiver table.
<b>Group IP</b>	Displays the multicast group address for which the receiver has sent a request to join the group.
<b>Port</b>	Displays the port on which the multicast receiver has sent a join request.
<b>Host IP</b>	Displays the IP address of the multicast receiver that has sent a request to join the multicast group
<b>Source IP</b>	Displays the unicast source IP address of the data source that sends multicast data to the group.
<b>Filter Mode</b>	<p>Displays the mode that has been registered by the multicast receiver, for the unicast source IP address specified. The list contains:</p> <ul style="list-style-type: none"> <li>- Include - Reception of packets sent to the specified multicast address, is requested <i>*only*</i> from those IP source addresses listed in the source-list parameter.</li> <li>- Exclude - Reception of packets sent to the given multicast address, is requested from all IP source addresses <i>*except*</i> those listed in the source- list parameter</li> </ul>

### 4.4.2 MLD Snooping

MLDS (Multicast Listener Discovery Snooping) is a protocol used by an IPv6 router to

discover the presence of multicast listeners (that is, nodes willing to receive multicast packets) on its directly attached links, and to discover specifically which multicast address is of interest to the neighboring nodes. It can also be used by applications to listen to some multicast group. When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic from flooding the Layer 2 segment of the network.

### 4.4.2.1 Basic Settings

This screen allows the user to configure basic settings such as MLD snooping status, operational status, Snooping Mode, Proxy Reporting and Snoop Leave level.

System Control Start

Select	MLD Snooping Status	Operational Status	Snooping Mode	Proxy Reporting	Snoop Leave Level
<input checked="" type="radio"/>	Enabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Mac Based <input type="button" value="v"/>	Enabled <input type="button" value="v"/>	Vlan Based <input type="button" value="v"/>
Select	Enhanced Mode	Proxy Status	Report Forwarding	Retry Count	Query Transmit On TC
<input type="radio"/>	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Router Ports <input type="button" value="v"/>	2	Disabled <input type="button" value="v"/>

Label	Description
<b>System Control</b>	Select the System Control status of MLDS in the switch. The default option is <b>Start</b> . The list contains: <ul style="list-style-type: none"> <li>– Start – Memory resources required by the MLDS module are allocated and the module starts running. It also initializes semaphore creation, timer task RBTree, hash table, RBT Tree nodes.</li> <li>– Shutdown - All the resources are released back to the system and the module stops running. When the module is shutdown, all the timers are stopped. The RBTree, hash Table and the allocated memory pools are deleted.</li> </ul>
<b>Select</b>	Select the option button to configure the MLD Snooping related parameters
<b>MLD Snooping Status</b>	Select the Global status of MLDS in the switch. The default option is <b>Disabled</b> . The list contains:

	<ul style="list-style-type: none"> <li>– Enabled - MLDS is enabled globally in a system. When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic and it forwards that traffic only to ports on the VLAN that have MLD hosts for that address</li> <li>– Disabled - MLDS is disabled globally in a system. When MLDS is disabled and a switch receives a packet with a multicast destination address, it floods the packet to all ports in the same VLAN</li> </ul>
<b>Operational Status</b>	<p>Displays the Operational status of MLDS in the switch. It is displayed based on the configuration status. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Indicates that the MLDS module operation is currently enabled in the system. The status gets enabled when the system control status is start and the snooping status is enabled.</li> <li>– Disable - Indicates that the MLDS module operations is currently disabled in the system.</li> </ul>
<b>Snooping Mode</b>	<p>Select the MLDS snooping mode. Modes are provided with redundancy support. The default option is <b>MAC based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– IP based - Hardware supports programming of S, G and *, G entries. MLDS snooping is based on the IP address and group address.</li> <li>– MAC based - Hardware supports only MAC based multicast tables and the snooping is based only on the group address.</li> </ul>
<b>Proxy Reporting</b>	<p>Select the Proxy Reporting status in the switch. MLD network traffic is reduced. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - On reception of query, switch generates reports as consolidated bitmaps in the table and forwards them to the router, based on the available host information.</li> <li>– Disabled – On reception of query, group consolidation table will be formed but will not be used for reporting to the upstream. Switch forwards all SSM (MLDv2) and a single</li> </ul>



	<p>ASM (MLDv1) report to the router.</p>
<p><b>Snoop Leave Level</b></p>	<p>Select the leave processing mechanism to be configured 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 back on 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. The default option is <b>Vlan Based</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Vlan Based – Configures the leave mechanism at the vlan level. In Vlan based leave processing mode, the fast leave functionality configurable per vlan is available for processing leave messages.</li> <li>– Port Based – Configures the leave mechanism at port level. In Port based leave processing mode, the explicit host tracking functionality or the fast leave functionality configurable on a logical interface can be used for processing the leave messages.</li> </ul>
<p><b>Enhanced Mode</b></p>	<p>Select the operating status of snooping module. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – The snooping module operates in enhanced mode. It is a mode of operation provided to enhance the operation of MLD 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 &amp; 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.</li> <li>– 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</li> </ul>

	<p>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.</p>
<p><b>Proxy Status</b></p>	<p>Select the Proxy status in the system. In proxy mode all the reports and queries generated by the switch will have the switch IP as the source IP. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled – Enables proxy in the system. By default all the ports will be down stream ports.</li> <li>- Disabled – Disables proxy in the system. By default all the ports will be up stream.</li> </ul>
<p><b>Report Forwarding</b></p>	<p>Select whether the report must be forwarded on all ports or only on router ports. The port which receives the query from the router is the Router port. The default option is <b>Router Ports</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Router Ports – Reports will be forwarded only on the router ports</li> <li>- All Ports – Reports will be forwarded on all ports</li> </ul>
<p><b>Retry Count</b></p>	<p>Enter the maximum number of group specific queries sent on a port on reception of an MLDv1 leave message. This values ranges from 1 to 5. The default value is <b>2</b>.</p>
<p><b>Query Transmit On TC</b></p>	<p>Select path redundancy for MLDS Snooping queries transmission to be enabled or disabled whenever topology changes. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Disabled- Disables path redundancy and it leads to flooding of data.</li> </ul>

### 4.4.2.2 Timer

This screen allows the user to set Router port purge interval, Group-Member Port Purge Interval, Report Forward Interval and Group Query Interval

Router Port PurgeInterval (Secs)	<input type="text" value="125"/>
Group-Member Port Purge Interval (Secs)	<input type="text" value="260"/>
Report Forward Interval (Secs)	<input type="text" value="5"/>
Group Query Interval (Secs)	<input type="text" value="2"/>

Label	Description
<b>Router Port PurgeInterval (Secs)</b>	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 from 60 to 600 seconds. The default value is <b>125</b> seconds.
<b>Group-Member Port Purge Interval (Secs)</b>	Enter the time interval after which a port gets deleted, if MLD reports are not received on a port. This value ranges from 130 to 1225 seconds. The default value is <b>260</b> seconds.
<b>Report Forward Interval (Secs)</b>	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 MLD membership report. This value ranges from 1 to 25 seconds. The default value is <b>5</b> seconds.
<b>Group Query Interval (Secs)</b>	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 from 2 to 5 seconds. The default value is <b>2</b> seconds.

### 4.4.2.3 VlanConfiguration

This screen allows the user to configure MLD Snooping on specific VLANs.

VLAN ID	vlan1
MLDS Status	Enabled
Operating Version	Version 2
Fast Leave	Disabled
Querier Status	Disabled
Querier Interval(secs)	
Router Port List	
Blocked Router Port List	
Max Response Code	
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	VLAN ID	MLDS Status	Configured Version	Current Version	Fast Leave	Configured Querier Status	Current Querier Status	Querier Interval(secs)	Router Port List	Blocked Router Port List	Max Response Code
<input checked="" type="radio"/>	1	Enabled	Version 2	v2	Disabled	Disabled	Disabled	125			0

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN. The MLD snooping configuration is performed for this specific VLAN ID.
<b>MLDS Status</b>	Select the Global status of MLDS on the specified VLAN. The default option is <b>Enabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled – Enables MLDS on the specified VLAN. The switch will watch for MLD messages from the host connected to those interfaces and build the software. This ensures that only the ports that require a given multicast stream actually receive it.</li> <li>– Disabled – Disables MLDS on the specified VLAN.</li> </ul>
<b>Operating Version</b>	Select the Operating Version of MLDS for the specified VLAN. The default option is <b>Version 2</b> . The list contains: <ul style="list-style-type: none"> <li>– Version 1 – Sets the MLDS Operating version as version 1. MLDS report is accessed only with group address. It is provided with leave request option</li> <li>– Version 2 –. Sets the MLDS Operating version as version 2. MLDS report is accessed with source and group address.</li> </ul>
<b>Fast Leave</b>	Select the Fast Leave status of MLDS. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled – Enables Fast Leave status of MLDS. 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</li> </ul>

	<p>functionality does not verify if other interested receivers are still present for the multicast group on the same port.</p> <ul style="list-style-type: none"> <li>– Disabled – Enables normal leave functionality. 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.</li> </ul>
<b>Querier Status</b>	<ul style="list-style-type: none"> <li>– Select whether the switch is configured as a querier in a VLAN. The default option is <b>Disabled</b>. The list contains:</li> <li>– Enabled – Configures the switch as Querier. The switch starts sending general queries at regular time intervals.</li> <li>– Disabled – Does not configure the switch as Querier. The switch starts receiving queries from any other router and the functionality gets disabled.</li> </ul>
<b>Querier Interval(secs)</b>	<p>Enter the time period during which the general queries are sent by MLDS, when the switch is configured as querier on a VLAN. This value ranges from 60 to 600 seconds. The default value is <b>125</b> seconds.</p>
<b>Router Port List</b>	<p>Enter the 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.</p>
<b>Blocked Router Port List</b>	<p>Enter the list of ports which are configured as blocked router ports. On a blocked router port the software discards queries, PIM/DVMRP and Data Messages and prevents such a port from ever becoming a router port. The blocked router port feature does not involve any hardware programming. Multicast data will be dropped on a blocked router port. Reports will not be forwarded on blocked router port. Reports coming from blocked router port are not processed.</p>
<b>Max Response Code</b>	<p>Enter the maximum response code advertised in queries which are sent over this VLAN. This value ranges from 0 to 255 milliseconds. The default value is <b>0</b>.</p>
<b>Configured Version</b>	<p>Displays the working MLD Version on the given VLAN. This value can be version 1 or version 2.</p>
<b>Current Version</b>	<p>Displays the current querier status in the VLAN. This value can</p>

	be enabled or disabled.
--	-------------------------

#### 4.4.2.4 RouterPortConf

This screen allows the user to configure the details of the VLAN Router Port.

VLAN ID	vlan1 <input type="button" value="v"/>
Router Port List	<input type="text"/>
V1/V2 Rtr Port Purge Interval	<input type="text"/>
Static Router Port Version	<input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	

VLAN ID	Router Port	Router Port Config Version	Router Port Version	V1/V2 Router Port Purge Interval	V3 Router Port Purge Interval
---------	-------------	----------------------------	---------------------	----------------------------------	-------------------------------

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN. The MLD snooping configuration is performed for the entered VLAN ID.
<b>Router Port List</b>	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.
<b>V1/V2 Rtr Port Purge Interval</b>	Enter the time interval after which proxy 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. However if control messages are received from the router before the timer expiry, then the timer is restarted. This value ranges from 60 to 600. The default value is <b>125</b> .
<b>Static Router Port Version</b>	Select the operating version of the IGMP proxy on the upstream router port. The default option is <b>Version 2</b> . The list contains:

	<ul style="list-style-type: none"> <li>- Version1 – Indicates that the operating version of MLDS proxy is version 1</li> <li>- Version2 - Indicates that the operating version of MLDS proxy is version 2</li> </ul>
<b>Router Port</b>	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.
<b>Router Port Config Version</b>	Displays the configured version of the MLDS Proxy on the upstream router port. The static router port version gets displayed in the configured version. The default value is <b>Version 2</b> .
<b>Router Port Version</b>	Displays the operating version of the MLDS proxy on the upstream router port. The default value is <b>Version 2</b> .
<b>V3 Router Port Purge Interval</b>	Displays the time interval (seconds) after which the switch assumes that there are no IGMP v3 routers present on the upstream port. When the timer expires, the learnt router port entry is purged. However if control messages are received from the router before the timer expiry, then the timer is restarted. This value ranges from 60 to 600. The default value is <b>125</b> .

#### 4.4.2.5 RouterPorts

<b>VLAN ID</b>	<b>Dynamic Port List</b>	<b>Static Port List</b>
----------------	--------------------------	-------------------------

Label	Description
<b>VLAN ID</b>	Select the VLAN Identifier that uniquely identifies a specific VLAN. The MLD snooping configuration is performed for the entered VLAN ID.
<b>Dynamic Port List</b>	Displays the lists of ports on which routers are present.
<b>Static Port List</b>	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 MLDv2, based on the address type.

### 4.4.2.6 FwdInformation

This screen displays the MLDS group information such as MAC/ IP 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.

VLAN ID	Group MAC Address	Port List
---------	-------------------	-----------

Label	Description
<b>VLAN ID</b>	Displays the VLAN Identifier that uniquely identifies a specific VLAN. The MAC based multicast forwarding entry is displayed for the entered VLAN ID
<b>Group MAC Address</b>	Displays the Group MAC Multicast address that is learnt.
<b>Port List</b>	Displays the learnt ports list to which the multicast data packets for the group will be forwarded.

### 4.4.3 GMRP

GMRP (GARP Multicast Registration Protocol) link permits to enable/disable GMRP on a global basis and also at the per-port level. This gives more control over the switch to the users. Once you enable the protocol on the switch, you can decide on the ports on which the protocol needs to run. GMRP does not support multiple instances. GMRP registers and de-registers the group membership information and group service requirement information with the GARP

#### 4.4.3.1 GMRP

This screen allows the user to configure GMRP globally.

Select	Context	GMRP Status
<input type="radio"/>	0	Disabled <input type="button" value="v"/>

Label	Description
<b>Context</b>	Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This value ranges from 0 to 65535. The default value is 0
<b>GMRP Status</b>	Select the global status of GMRP protocol in the system. GMRP uses the services of GARP to propagate multicast



	<p>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. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- 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.</li> </ul>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.4.3.2 Port Settings

This screen allows the user to configure the GMRP control and restricted group registration details for every bridge port.



Label	Description
<b>Port</b>	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).
<b>GMRP Status</b>	<p>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. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- 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.</li> </ul>

	When disabled any GMRP packets received will be silently discarded and no GMRP registrations will be propagated from other ports
<b>Registration</b>	<p>Select the Restricted Group Registration status. Restricted Group Registration enables you to restrict the multicast groups learnt through GMRP learning. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- Disabled - Disables Restricted Group Registration.</li> </ul>

## 4.4.4 IGMP

IGMP (Internet Group Management Protocol) is a group membership management protocol used to report group memberships to any immediate neighboring multicast switch. A host uses the IGMP to inform a switch when it joins or leaves an Internet Multicast group.

### 4.4.4.1 Basic Settings

This screen allows the user to configure the IGMP Status.

Label	Description
<b>Global Status</b>	<p>Specifies the global status of the IGMP protocol in the switch. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled - Enables the IGMP globally.</li> <li>- Disabled – Removes all dynamic multicast entries, stops all timers for route entries and disables IGMP on all IGMP enabled interfaces.</li> </ul>

<b>Global limit</b>	Enter the total number of multicast groups that are allowed globally. The default value is <b>0</b> . The value ranges from 0 to 255.
<b>Current GroupCount</b>	Displays the current count of groups that are added. The value ranges from 0 to 255.

### 4.4.4.2 Interface Configuration

This screen allows the user to configure the IGMP interfaces.

Select|Interface|IGMP Admin Status|Operating Version|Fast Leave|Channel Tracking|Query Interval|Query Response Time|Robustness Value|Interface GroupLimit|GroupList ID|GroupCurrent Count|Join RateLimit

Label	Description
<b>Interface</b>	Select the interface for which IGMP is enabled.
<b>IGMP Admin Status</b>	Select the IGMP admin Status for the interface. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled - Enables IGMP on the interface.</li> <li>– Disabled - Disables IGMP on the interface.</li> </ul>
<b>Operating Version</b>	Select the version of IGMP which is running on the interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. The default option is <b>Version 2</b> . The list contains: <ul style="list-style-type: none"> <li>– Version 1 - Sets the IGMP version as version 1.</li> <li>– Version 2 - Sets the IGMP version as version 2.</li> <li>– Version 3 - Sets the IGMP version as version 3.</li> </ul>
<b>Fast Leave</b>	Select the status of the fast leave feature of the IGMPv3 protocol. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled – Supports immediate intimation to the Multicast Routing Protocol on the last member leaving the Group.</li> </ul>

	<ul style="list-style-type: none"> <li>– Disabled – Does not support fast leave feature.</li> </ul>
<b>Channel Tracking</b>	<p>Select the status of channel tracking feature of the IGMPv3 protocol. Channel tracking is the ability of a system to keep track of each individual host that is joined to a particular multicast group or channel. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables the router to keep track of each individual host that is joined to a particular multicast group or channel</li> <li>– Disabled - Disables explicit channel tracking feature support.</li> </ul>
<b>Query Interval</b>	<p>Enter the frequency at which IGMP Host-Query packets are transmitted on the interface. This value ranges from 1 to 65535 seconds. The default value is <b>125</b> seconds.</p>
<b>Query Response Time</b>	<p>Enter the maximum response time for IGMP queries. This value ranges from 1 to 255. The default value is <b>100</b> seconds.</p>
<b>Robustness Value</b>	<p>Enter the Robustness value on this interface. The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be loss, the Robustness Variable may be increased. IGMP is robust to packet losses. This value ranges from 1 to 255. The default value is <b>2</b>.</p>
<b>Interface GroupLimit</b>	<p>Enter the total number of multicast groups that can be allowed for this interface. If IGMP interface current group count reaches this Interface Limit value then no membership reports is honored on this interface except the group list mapped to this interface. This value ranges from 0 to 255.</p>
<b>GroupList ID</b>	<p>Enter the except group list id for an interface. This group list is exempted for limiting on this interface. This value ranges from 0 to 4294967295.</p>
<b>GroupCurrent Count</b>	<p>Displays the current count of groups that are added to the interface, This counter is incremented for each valid membership report on this interface and decremented for leave report if Interface Limit is configured for this interface. This value ranges from 0 to 255.</p>

#### 4.4.4.3 Group Information

This screen allows the user to configure IGMP Multicast groups.

Interface	vlan1 <input type="button" value="v"/> *
Group Address	<input type="text"/> *
Source Address	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Interface	Group Address	Filter Mode
<input type="button" value="Delete"/>			

Label	Description
<b>Interface</b>	Select the interface from the list of interfaces for which the entry contains information for an IP multicast group address.
<b>Group Address</b>	Enter the IP multicast group address.
<b>Source Address</b>	Enter the IP Source address where multicast data packets originate.
<b>Select</b>	Select the interface for which the configurations need to be deleted.
<b>Filter Mode</b>	Specifies the state in which the interface is currently set. This indicates the relevance of the corresponding source list entries for IGMPv3 interfaces This is a read-only field. The default option is <b>Exclude</b> , The list contains: <ul style="list-style-type: none"> <li>- Include - Specifies the filter mode as Include.</li> <li>- Exclude - - Specifies the filter mode as Exclude.</li> </ul>

#### 4.4.4.4 Source Information

This screen displays the source list entries corresponding to each Interface filter mode record.

Interface	Group Address	Source Address	Reporter Address
vlan2	225.0.0.0	11.0.0.10	12.0.0.10
vlan2	225.0.0.0	11.0.0.10	12.0.0.20
vlan2	225.0.0.0	11.0.0.20	12.0.0.40
vlan2	225.0.0.0	11.0.0.30	12.0.0.10
vlan2	225.0.0.0	11.0.0.30	12.0.0.30

Label	Description
-------	-------------

<b>Interface</b>	Displays the interface for which the entry contains information for an IP multicast group address.
<b>Group Address</b>	Displays the IP multicast group address.
<b>Source Address</b>	Displays the IP Source address.
<b>Reporter Address</b>	Displays the IP Address of the Host requesting for the Multicast Group Information. When tracking is enabled it displays the IP address of the host for Individual membership entry.

### 4.4.4.5 GroupList Configuration

This screen allows the user to configure the IGMP group list information.

Select	GroupList ID	Group IP Address	Mask
<input checked="" type="radio"/>	50	239.255.255.2	239.255.255.2

Label	Description
<b>GroupList ID</b>	Enter the global group list Identifier. The value ranges from 1 to 4294967295.
<b>Group IP Address</b>	Enter the multicast Group IP address.
<b>Mask</b>	Enter the subnet mask address of the IGMP group.

### 4.4.5 MLD

MLD (Multicast Listener Discovery) implements the router part of MLD conforming to the RFC 3810. IPv6 systems (hosts and routers) use MLD to report their multicast group memberships to any neighboring multicast routers. MLD registers with IPv6 for packet flow and interface

change notifications.

### 4.4.5.1 Basic Settings

This screen allows the user to set the global status of the MLD feature in the router.

Label	Description
<b>Global Status</b>	<p>Select the global status of the MLD protocol in the router. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the MLD protocol in the router on all interfaces.</li> <li>– Disabled – Disables the MLD on all interfaces, removes all dynamic multicast entries and stops all timers for route entries.</li> </ul>

### 4.4.5.2 Interface Configuration

This screen allows the user to configure the MLD related information for the interfaces in which MLD is enabled.

Select | Interface | MLD Admin Status | Operating Version | Fast Leave | Query Interval | Query Response Time | Robustness Value | Join RateLimit

Label	Description
<b>Interface</b>	<p>Select the VLAN or router port interface for which the MLD interface related information should be configured. 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). The interface type is displayed as VLAN</p>

	for the VLAN interface and as slot for other interfaces.
<b>MLD Admin Status</b>	<p>Select the administrative MLD status for the interface. The default option is <b>Enabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the MLD module in the selected interface.</li> <li>– Disabled – Disables the MLD module in the selected interface.</li> </ul>
<b>Operating Version</b>	<p>Select the MLD version to be run on the selected interface. The default option is <b>Version 1</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Version 1 – Implements MLD version 1 on the - Selected interface. MLD version 1 does not support source filtering, but supports host suppression.</li> <li>– Version 2 – Implements MLD version 2 on the - Selected interface. MLD version 2 supports source filtering, but does not support host suppression.</li> </ul>
<b>Fast Leave</b>	<p>Select the fast leave feature status of MLD on the selected interface. The fast leave feature. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – The router blocks a source list for a host for a multicast group as specified by the host for that group. The router stops forwarding the multicast group traffic to the host, if the source list received in the leave message is same as the blocked source list.</li> <li>– Disabled – The router removes an interface from a forwarding table for a multicast group based on request from a host connected to that interface, only if other hosts of that interface are also not interested in receiving traffic for that multicast group.</li> </ul>
<b>Query Interval</b>	<p>Enter the time interval (in seconds) between MLD host- query packets. This determines the number of host-query packets transmitted on the interface. These packets contain group membership information. This value ranges from 1 to 31744 seconds. The default value is <b>125</b> seconds.</p>
<b>Query Response Time</b>	<p>Enter the maximum query response time (in tenths of a second) advertised in MLD queries on the interface. This represents the</p>



	maximum time interval before which the host is expected to respond to an MLD query. You have to enter the response time in tenths of a second, while the software converts it into seconds. For example, to set the response time as 45 seconds, you have to enter 450 in this field. This value ranges from 1 to 31744 tenths of a second. The default value is <b>100</b> tenths of a second (10 seconds).
<b>Robustness Value</b>	Enter the robustness value that allows tuning for the expected packet loss on a link. Increase in robust count allows more packet loss but increases the leave latency of the network. The MLD robustness to packet losses is calculated based on the formula Robustness value – 1. For example, if robust value is set as 3, then MLD is robust to 2 (3-1) packet losses. This value ranges from 1 to 255. The default value is <b>2</b>

### 4.4.5.3 MLD Source Information

This screen allows the user to view the source list entries of each interface and multicast group pair on the router

Address Type	Group Address	Interface	Source Address
--------------	---------------	-----------	----------------

Label	Description
<b>Address Type</b>	Displays the address format of the group and source address. This value can be: – 2 – Group and source address are set as per IPv6 format.
<b>Group Address</b>	Displays the IPv6 multicast group address for which the host wants to join.
<b>Interface</b>	Displays the CFA interface index for which multicast group and source address are displayed.
<b>Source Address</b>	Displays the source address from which the host wants to listen the traffic.

### 4.4.6 IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of the discovered hosts. IGMP proxy provides queue interface and socket interface options to receive and transmit the IGMP control packets and multicast data packets.

IGMP proxy device performs router portion of IGMP on the downstream interfaces and host portion of IGMP on the upstream interfaces. IGMP proxy device consolidates the reports received in the downstream interfaces, and sends a summarized report on to the upstream interface.

### 4.4.6.1 Basic Settings

This screen allows the user to configure the IGMP Proxy Status.

Label	Description
<b>Proxy Status</b>	<p>Enables/ Disables IGMP Proxy in the Switch. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Starts IGMP proxy module</li> <li>– Disabled – Stops IGMP proxy module</li> </ul>

### 4.4.6.2 Upstream Interface

This screen allows the user to configure IGMP Proxy upstream interfaces.

Select	Interface Index	Operating Version	Configured Version	Version Purge Interval
<input checked="" type="radio"/>	vlan1	Version 3	Version 3	125

Label	Description
<b>Interface</b>	Specifies the Layer 3 VLAN Interface, which is defined as an upstream interface.
<b>Configured Version</b>	Specifies the configured version of the IGMP Proxy device on the upstream interface. The options are

	<ul style="list-style-type: none"> <li>- Version 1</li> <li>- Version 2</li> <li>- Version 3</li> </ul> <p>The default option is <b>Version 3</b>.</p>
<b>Version Purge Interval</b>	Specifies the interval (in seconds) after which the upstream interface IGMP operating version will be changed to configured IGMP version. This value ranges from 60 to 600 seconds.
<b>Interface Index</b>	Specifies the index value of the Layer 3 VLAN Interface, which is defined as an upstream interface. This is a read-only field. This value ranges from 1 to 65535.
<b>Operating Version</b>	<p>Indicates the operating version of the IGMP Proxy device on the upstream interface. This is a read-only field. The options are</p> <ul style="list-style-type: none"> <li>- Version 1</li> <li>- Version 2</li> <li>- Version 3</li> </ul>

### 4.4.6.3 MRoute Information

This screen allows the user to view the multicast routing information for the registered group members.

Source	Group	Uplface Index
--------	-------	---------------

Label	Description
<b>Source</b>	Indicates the Unicast Source IP address of the data
<b>Group</b>	Indicates the IP multicast group address for which multicast registrations are received.
<b>Uplface Index</b>	Indicates the index value of the upstream interface on which IP multicast datagrams are received for the registered group address.

### 4.4.6.4 NextHop Information

This screen allows the user to view the list of outgoing interfaces for the multicast forwarding entries.

<b>Source Address</b>	<b>Group Address</b>	<b>NextHop Iface Index</b>	<b>NextHop State</b>
-----------------------	----------------------	----------------------------	----------------------

Label	Description
<b>Source Address</b>	Indicates the Unicast source IP address of the data source that sends multicast data for registered groups.
<b>Group Address</b>	Indicates the IP Multicast group address for which multicast registrations are received.
<b>NextHop Iface Index</b>	Indicates the Index value of the interface on which multicast registrations for the group are received.
<b>NextHop State</b>	Indicates the state of the outgoing interface on which the multicast registrations have been received. The options are <ul style="list-style-type: none"> <li>- Forwarding – Denotes that the entry is created.</li> <li>- Prune</li> </ul>

## 4.4.7 PIM

PIM (Protocol Independent Multicast) is a multicast routing protocol designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to a router that runs the IP protocol along with IGMP. PIM supports a plane-separated architecture for the Control and Forwarding planes. PIM is independent of the underlying unicast routing protocol and uses the information from the unicast routing protocol.

### 4.4.7.1 Basic Settings

This screen allows the user to configure the PIM basic settings.

PIM Status  ▾  
 PIMv6 Status  ▾

PIM PMBR Status  ▾  
 PIM Router Mode  ▾  
 PIM Static RP Status  ▾  
 PIM Bidir Status  ▾  
 PIM RPF Status  ▾

Label	Description
<b>PIM Status</b>	Select the PIM status in the switch. The default value is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled - Enables PIM globally in the switch.</li> <li>– Disabled - Disables PIM globally in the switch.</li> </ul>
<b>PIMv6 Status</b>	Select the PIMv6 status in the switch. The default value is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled - Enables PIMv6 globally in the switch.</li> <li>– Disabled - Disables PIMv6 globally in the switch</li> </ul>
<b>PIM PMBR Status</b>	Select the PIM Multicast Border Router (PMBR) Status. A PMBR integrates two different PIM domains (either PIM -SM or PIM-DM) and also connects a PIM domain to other multicast routing domain(s). The default value is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>– Enabled - Enables PIM PMBR in the switch.</li> <li>– Disabled - Disables PIM PMBR in the switch.</li> </ul>
<b>PIM Router Mode</b>	Select the mode of the PIM-SM router. The list contains: <ul style="list-style-type: none"> <li>– SSM Only - The SSM Only mode of the PIM-SM router.</li> <li>– SM, SSM - The SM_SSM mode of the PIM-SM router.</li> </ul>
<b>PIM Static RP Status</b>	Select the static configuration of RP status. Static configuration

	<p>allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled - Enables PIM Static RP Status in the switch.</li> <li>- Disabled - Disables PIM Static RP Status in the switch.</li> </ul>
<b>PIM Bidir Status</b>	<p>Select the PIM Bidir status in the router. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potentially receivers also. The default value is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled - Enables PIM Bidir Status in the switch.</li> <li>- Disabled - Disables PIM Bidir Status in the switch</li> </ul>
<b>PIM RPF Status</b>	<p>Select the PIM RPF status in the router. The list contains:</p> <ul style="list-style-type: none"> <li>- Enabled - Enables PIM RPF Status in the switch.</li> <li>- Disabled - Disables PIM RPF Status in the switch.</li> </ul>

### 4.4.7.2 Component

This screen allows the user to configure PIM component parameters.

Component ID

Mode \*

Candidate CRP Hold Time

Scope Zone Name

Select	Component Id	BSR Expiry Time	Mode	CRP Hold Time	Scope Zone Name
<input type="button" value="Apply"/> <input type="button" value="Delete"/>					

Label	Description
<b>Component ID</b>	Enter a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255.
<b>Mode</b>	Select the operating mode for the component id configured.

	<p>The default option is <b>Sparse</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Dense - Indicates the component is running in <b>Dense</b> mode, implicitly building shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present.</li> <li>– Sparse - Indicates the component is running in <b>Sparse</b> mode, explicitly building unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source.</li> </ul>
<b>Candidate CRP Hold Time</b>	Enter the hold time of the component when it is a candidate RP (Rendezvous Point) in the local domain. This value ranges from 0 to 255. The default value is <b>0</b> .
<b>Scope Zone Name</b>	Enter the scope-zone-name. The maximum length of the string is 64.
<b>BSR Expiry Time</b>	Displays the minimum time remaining before the bootstrap router in the local domain is declared down. This is a read-only field.

### 4.4.7.3 Interface

This screen allows the user to configure PIM interfaces.

Select	Interface	AddrType	Address	MaskLen	DR Addr	Hello Int	JP Int	C-BSR Pref	Comp Id
<input type="radio"/>	vlan1	IPv4	12.0.0.1	8	12.0.0.1	30	60	-1	1
<input checked="" type="radio"/>	vlan1	IPv6	fe80:0000:0000:0000:020	16	fe80:0000:0000:0000:020	30	60	-1	1

Label	Description
<b>Interface</b>	Select the index value of the PIM interface.
<b>Address Type</b>	Specifies the address type of the PIM interface. The default option is IPv4. The list contains: <ul style="list-style-type: none"> <li>– <b>IPv4</b> - Specifies the IPv4 address type.</li> </ul>

	– IPv6 - Specifies the IPv6 address type.
<b>Hello Interval</b>	Enter the frequency at which PIM Hello messages are transmitted on the interface. This value ranges from 1 to 255 seconds. The default value is <b>30</b> seconds.
<b>Join Prune Interval</b>	Enter the frequency at which PIM Join/Prune messages are transmitted on the PIM interface. This value ranges from 1 to 255 seconds. The default value is <b>60</b> seconds.
<b>C-BSR Preference</b>	Enter the preference value for the local interface as a candidate bootstrap router. This value ranges from -1 to 255. The default value is <b>-1</b> .
<b>Component Id</b>	Enter a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as <b>Sparse</b> or <b>Dense</b> mode. This value ranges from 1 to 255.
<b>Select</b>	Click to the interface for which PIM interface parameters to be reapplied.
<b>Address</b>	Displays the IP address.
<b>Mask Len</b>	Displays the IP mask length for the configured IP address. This value ranges from 0 to 32 for an IPv4 address and 0 to 128 for IPv6 address.
<b>DR Addr</b>	Displays the DR address.

#### 4.4.7.4 CandidateRP

This screen allows the user to configure PIM information for candidate RP for IP multicast groups. A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as RP.



Component Id	<input type="text" value="1"/> *
Address Type	<input type="button" value="v"/>
Group Address	<input type="text"/> *
Group Mask length	<input type="text"/> *
RP Address	<input type="text"/> *
Priority	<input type="text" value="192"/>
PIM Mode	<input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Component Id	Address Type	Group Address	Group Mask Length	RP Address	Priority	PIM Mode
<input type="button" value="Delete"/>							

Label	Description
<b>Component Id</b>	Enter a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255.
<b>Address Type</b>	Select the address type of the PIM interface. The default option is IPv4. The list contains: <ul style="list-style-type: none"> <li>- <b>IPv4</b> - Sets the address type as Internet protocol version 4.</li> <li>- <b>IPv6</b> - Sets the address type as Internet protocol version 6.</li> </ul>
<b>Group Address</b>	Enter the IP multicast group address, for which the switch advertises itself as the candidate RP (Rendezvous Point) which contains the multicast routing information.
<b>Group Mask length</b>	Enter the subnet mask, which when combined with the group address gives the group prefix. This value ranges from 0 to 32 for IPv4 address and 0 to 128 for IPv6 address.
<b>RP Address</b>	Enter the IP address of the Candidate-RP.
<b>Priority</b>	Enter the priority of the Candidate-RP. The priority value ranges from 0 to 255. The default value is <b>192</b> .
<b>PIM Mode</b>	Select PIM mode of the group for which candidate RP is configured. The list contains: <ul style="list-style-type: none"> <li>- Sparse - Specifies the component is running in Sparse mode.</li> <li>- Bidir - Specifies the component is running in Bidir mode.</li> </ul>

### 4.4.7.5 StaticRP

This screen allows the user to configure PIM information for static RP for IP multicast groups.

Component Id	<input type="text" value="1"/>	*
Address Type	<input type="button" value="v"/>	
Group Address	<input type="text"/>	*
Group Mask Length	<input type="text"/>	*
RP Address	<input type="text"/>	*
Embedded RP	<input type="button" value="v"/>	
PIM Mode	<input type="button" value="v"/>	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Select	Component Id	Address Type	Group Address	Group Mask Length	RP Address	Embedded RP	PIM Mode
<input type="button" value="Apply"/> <input type="button" value="Delete"/>							

Label	Description
<b>Component Id</b>	Enter a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255.
<b>Address Type</b>	Select the address type of the PIM interface. The default option is <b>IPv4</b> . The list contains: <ul style="list-style-type: none"> <li>- <b>IPv4</b> - Sets the address type as Internet protocol version 4.</li> <li>- <b>IPv6</b> - Sets the address type as Internet protocol version 6.</li> </ul>
<b>Group Address</b>	Enter the IP multicast group address, for which the switch advertises itself as the static RP (Rendezvous Point).
<b>Group Mask Length</b>	Enter the subnet mask, which when combined with the group address gives the group prefix. This value ranges from 0 to 32 for IPv4 address and 0 to 128 for IPv6 address.
<b>RP Address</b>	Enter the IP address of the Static-RP.
<b>Embedded RP</b>	Select the status of the embedded RP. The default option is <b>Disable</b> . The list contains: <ul style="list-style-type: none"> <li>- Enable - Enables the Embedded RP.feature.</li> <li>- Disable - Disables the Embedded RP.feature.</li> </ul>

<b>PIM Mode</b>	<p>Select the PIM mode of the group for which candidate RP is configured. The list contains:</p> <ul style="list-style-type: none"> <li>- Sparse - Specifies the component is running in Sparse mode.</li> <li>- Bidir - Specifies the component is running in Bidir mode.</li> </ul>
-----------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### 4.4.7.6 Global

This screen allows the user to configure PIM Reverse Path Forwarding (RPF) Status and Shortest Path Tree Group Threshold, Source Threshold, Switching period, RP threshold and RP Switching Period.

**Bidirectional PIM Configurations**

Offer Interval

Offer Limit

**Shortest Path Tree**

Group Threshold

Source Threshold

Switching Period

RP Threshold

RP Switching Period

Label	Description
<b>Offer Interval</b>	Enter the time interval between the Distance Forwarder (DF) election Offer messages to be sent. The default value is <b>100</b> milli-seconds. This value ranges from 1 to 20000000.milliseconds.
<b>Offer Limit</b>	Enter the Bidir-PIM offer limit, the number of unanswered offers before the router changes as the designated forwarder (DF). The default value is <b>3</b> . This value ranges from 3 to 100.
<b>Group Threshold</b>	Enter a BPS (Bits-per-second) value, which initiates the source specific counters for a particular group when the threshold of data rate for any group exceeds. It is based on number of packets. The default value is <b>0</b> . This value ranges from 0 to 2147483647

<b>Source Threshold</b>	Enter a BPS value, which initiates the switching to shortest path tree when the threshold of data rate for any source exceeds. It is based on number of packets. This value ranges from 0 to 2147483647. The default value is <b>0</b> .
<b>Switching Period</b>	Enter the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. The default value is <b>0</b> . This value ranges from 0 to 2147483647. The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured. The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.
<b>RP Threshold</b>	Enter the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree. This value ranges from 0 to 2147483647. This value ranges from 0 to 2147483647. The default value is <b>0</b> . To switch to SPT, this threshold must be configured and the switching is based on the number of registered packets received.
<b>RP Switching Period</b>	Enter the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree. The default value is <b>0</b> . This value ranges from 0 to 2147483647. RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP to switch to SPT, this period must be configured.

#### 4.4.7.7 DM

This screen allows the user to configure the parameters related to dense mode.

SR Origination Status	Disabled <input type="button" value="v"/>
Refresh Interval	<input type="text"/>
SR Processing Status	Enable <input type="button" value="v"/>
Source Active Interval	210 <input type="text"/>

Label	Description
<b>SR Origination Status</b>	Select the generation status of the state refresh message. The default option is <b>Disabled</b> . The list contains:

	<ul style="list-style-type: none"> <li>- <b>Disabled</b> – Does not generate the state refresh message.</li> <li>- <b>Enabled</b> – Generates the state refresh message.</li> </ul>
<b>Refresh Interval</b>	Enter configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router. This value ranges from 4 to 100.
<b>SR Processing Status</b>	<p>Select the processing status state refresh message. The default value is <b>Disable</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- <b>Disable</b> – Disables the SRM processing and forwarding, that is, the router drops the State Refresh Messages, if received and also the router will not advertise the SR Capability in Hello messages</li> <li>- <b>Enable</b> – Enables the SRM processing and forwarding. On enabling, this router advertises itself as SR Capable in Hello Messages</li> </ul>
<b>Source Active Interval</b>	Enter the time period (in seconds) after which the SRM control messages is generated by the router after a data packet is received. The default value is <b>210</b> seconds This value ranges from 120 to 210 seconds.

#### 4.4.7.8 RoutelInfo

This screen displays the PIM multicast routing information.

ComponentID	AddrType	Group	Source	Mask	Vector	Upstream Neighbour	Incoming Interface	Pim Mode
-------------	----------	-------	--------	------	--------	--------------------	--------------------	----------

Label	Description
<b>ComponentID</b>	Enter a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255.
<b>AddrType</b>	<p>Select the address type of the PIM interface. The default option is <b>IPv4</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- <b>IPv4</b> - Specifies the IPv4 address type.</li> <li>- <b>IPv6</b> - Specifies the IPv6 address type.</li> </ul>

<b>Group</b>	Displays the IP multicast group address for which the multicast routing information is displayed.
<b>Source</b>	Displays the network address of the source.
<b>Mask</b>	Displays the network mask of the source
<b>Vector</b>	Displays PIM Reverse Path Forwarding vector (RPF) value
<b>Upstream Neighbour</b>	Displays the address of the upstream neighbor from which IP datagram sent to the multicast address are received.
<b>Incoming Interface</b>	Specifies the value of If Index for the interface on which IP datagram sent to the multicast address are received. This is a read- only field.
<b>Pim Mode</b>	Displays the PIM mode of the group for which candidate RP is configured. The list contains: <ul style="list-style-type: none"> <li>- Sparse - Indicates the component is running in Sparse mode.</li> <li>- Bidir - Indicates the component is running in Bidir mode.</li> </ul>

#### 4.4.7.9 RPinfo

This screen displays the PIM information for candidate RPs for IP multicast groups.

The PIM information is obtained from received candidate RP advertisements, if the local router is BSR. The PIM information is obtained from received RP set messages if the local router is not BSR.

Component	AddrType	Group	MaskLen	Candidate RP	Hold Time	Expiry Time	Pim Mode
-----------	----------	-------	---------	--------------	-----------	-------------	----------

#### Note : Pim Mode values

**2: Sparse**

**4: Bidir**

Label	Description
<b>Component</b>	Displays a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode.

	This value ranges from 1 to 255.
<b>AddrType</b>	Displays the address type of the PIM interface. The default option is <b>IPv4</b> . The list contains: <ul style="list-style-type: none"> <li>– <b>IPv4</b> - Indicates the address type as Internet protocol version 4.</li> <li>– <b>IPv6</b> - Indicates the address type as Internet protocol version 6.</li> </ul>
<b>Group</b>	Displays the IP multicast group address for which the information about the candidate RP is displayed
<b>MaskLen</b>	Displays the multicast group address mask.
<b>Candidate RP</b>	Displays the IP address of the candidate RP
<b>Hold Time</b>	Displays the time remaining for the advertisement of a candidate RP to be aged out. This value ranges from 0 to 255 seconds. This value is 0 for the local router that is not configured as BSR.
<b>Expiry Time</b>	Displays the minimum time remaining for the candidate RP to be declared as down. This value is 0 for the local router that is not configured as BSR.
<b>Pim Mode</b>	Displays PIM mode of the group for which candidate RP is configured <ul style="list-style-type: none"> <li>– Sparse - Specifies the component is running in Sparse mode.</li> <li>– Bidir - Specifies the component is running in Bidir mode.</li> </ul>

#### 4.4.7.10 PimHA

This screen displays the PIM High Availability information for IP multicast groups.

Pim HotStandby AdminStatus	Disabled
Pim HotStandby Status	Init
Pim HotStandby BulkUpdate Status	NotStarted
Forwarding Table EntryCount	0

Label	Description
<b>Pim HotStandby AdminStatus</b>	Displays the status of the Hot standby feature. The list contains

	<ul style="list-style-type: none"> <li>- Enabled - Indicates the admin status is enabled</li> <li>- Disabled - Indicates the admin status is disabled</li> </ul>
<b>Pim HotStandby Status</b>	<p>Displays the status of the PEER node. The list contains</p> <ul style="list-style-type: none"> <li>- ActiveNodePeerUp – Indicates standby-node is up</li> <li>- ActiveNodePeerDown – Indicates standby-node is down</li> </ul>
<b>Pim HotStandby BulkUpdate Status</b>	<p>Displays the synchronization status between the Active node and Stand-by node. The list contains</p> <ul style="list-style-type: none"> <li>- InProgress - Active Node is updating the info to standby</li> <li>- Completed - Active and standby node have synchronized the data</li> <li>- NotStarted - Active Node doesn't start the synchronization yet</li> <li>- Aborted - Bulk update stopped while in progress</li> </ul>
<b>Forwarding Table EntryCount</b>	<p>Displays the number of entries available in Forwarding Path (Data Plane).</p>

#### 4.4.7.11 ElectedRP

This screen displays the PIM Elected RP Information for IP multicast groups.

ComponentID	AddrType	Group	Mask	RP	Priority	Hold Time
-------------	----------	-------	------	----	----------	-----------

Label	Description
<b>ComponentID</b>	<p>Displays a Unique number to configure the PIM component in the router. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode. This value ranges from 1 to 255.</p>
<b>AddrType</b>	<p>Displays the address type of the PIM interface. The default option is IPv4. The list contains:</p> <ul style="list-style-type: none"> <li>- <b>IPv4</b> - Indicates the address type as Internet protocol version 4.</li> <li>- <b>IPv6</b> - Indicates the address type as Internet protocol version 6.</li> </ul>
<b>Group</b>	<p>Displays the IP multicast group address for which the information about the candidate RP is displayed.</p>



<b>Mask</b>	Displays the multicast group address mask.
<b>RP</b>	Displays the RP Address of the DF Election row
<b>Priority</b>	Displays the priority of the interface which will be advertised as a Candidate-RP. The priority value ranges from 0 to 255. The default value is <b>192</b> .
<b>Hold Time</b>	Displays the time remaining for the advertisement of a candidate RP to be aged out. This value ranges from 0 to 255 seconds. This value is 0 for the local router that is not configured as BSR.

#### 4.4.7.12 DFInfo

This screen displays the PIM DF information for IP multicast groups.

<b>AddrType</b>	<b>RP</b>	<b>Interface</b>	<b>State</b>	<b>Winner</b>	<b>Uptime</b>	<b>WinMetric</b>	<b>WinMetricPref</b>	<b>MsgCount</b>
-----------------	-----------	------------------	--------------	---------------	---------------	------------------	----------------------	-----------------

Label	Description
<b>AddrType</b>	Specifies the address type of the PIM interface. The default option is IPv4. The list contains: <ul style="list-style-type: none"> <li>– <b>IPv4</b> - Indicates the address type as Internet protocol version 4.</li> <li>– <b>IPv6</b> - Indicates the address type as Internet protocol version 6.</li> </ul>
<b>RP</b>	Displays the RP Address of the DF Election row.
<b>Interface</b>	Displays the index value of the PIM interface.
<b>State</b>	Displays the election state of the router for the specified RP address and interface: The options are offer, win, lose or backoff.
<b>Winner</b>	Displays the address of the DF election winner for the specified RP address and interface.
<b>Uptime</b>	Displays the uptime of the DF election winner for the specified RP address and interface.
<b>WinMetric</b>	Displays the metric of the DF election winner for the specified RP to reach the RP.
<b>WinMetricPref</b>	Displays the metric preference of the DF election winner for the

	specified RP to reach the RP.
<b>MsgCount</b>	Displays the number of DF messages sent by the router for the specified RP and interface.

## 4.5 Ethernet OAM

Ethernet Operations, Administration and Maintenance (EOAM) is implemented as per the IEEE standard 802.3ah-Clause 57. The EOAM sub- layer provides mechanisms useful for monitoring link operation such as link monitoring, remote fault indication and remote loopback control. In general, OAM provides network operators, the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions. The EOAM optional sub-layer provides data link layer mechanisms that complement the application that may reside in higher layers.

The EOAM information is conveyed in Slow Protocol frames called OAMPDUs. The OAMPDUs contain the appropriate control and status information used to monitor, test and troubleshoot EOAM-enabled links. The OAMPDUs (untagged frames) traverse a single link, being passed between peer OAM entities, and as such, are not forwarded by MAC clients (bridges or switches).

### 4.5.1 Basic Settings

This screen allows the user to configure the EOAM related parameters used globally for all the ports available in the switch.

System Control	Shutdown
EOAM Status	Disabled
EOAM Link-Monitor event resend Count	10
EOAM OUI	00:01:02

Label	Description
<b>System Control</b>	<p>Select the administrative system control status of EOAM module. The default option is <b>Start</b>. The list contains:</p> <ul style="list-style-type: none"> <li>- Start – Allocates resources required by EOAM module and starts EOAM on all ports.</li> <li>- Shutdown – Releases allocated resources and shuts down</li> </ul>

	the EOAM on all ports.
<b>EOAM Status</b>	Select the administrative module status of EOAM module. EOAM feature allows the user to monitor and troubleshoot Ethernet point-to-point links. EOAM is used when Ethernet is deployed as the broadband access technology between carrier and customer networks. The default option is <b>Disabled</b> . The list contains: <ul style="list-style-type: none"> <li>- Enabled – Enables the EOAM in the switch.</li> <li>- Disabled – Disables the EOAM in the switch and also on all the ports in the switch.</li> </ul>
<b>EOAM Link-Monitor event resend Count</b>	Enter the number of times an error event OAMPDU can be sent repeatedly. The events such as symbol period, frame-period, frame, frame-secs-summary and organization specific event are sent repeatedly, to avoid loss of OAMPDUs on faulty links. This value ranges from 1 to 10. The default value is <b>10</b> .
<b>EOAM OUI</b>	Enter the Organizational Unique Identifier (OUI) of the local EOAM client. This value is sent in the information OAMPDU in local information TLV. The OUI is a 24-bit identifier that is purchased from IEEE to uniquely identify a vendor, manufacturer, or assignee. This value is an octet string of size 3 bytes. The default value is the first three bytes of the switch base MAC address

### 4.5.2 Port Settings

This screen allows the user to enable / disable EOAM on an interface. It also allows the user to configure the OAM capabilities and loopback status of an EOAM interface.

Select	Port	Status	Mode	LB Permit/Deny	Operational Status	Remote LB	Link Event	Uni Directional	Variable Retrieval
--------	------	--------	------	----------------	--------------------	-----------	------------	-----------------	--------------------

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be applied.
<b>Port</b>	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).
<b>Status</b>	<p>Select the desired administrative OAM mode for the interface. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled – Enables the operation of EOAM over the interface.</li> <li>– Disabled – Disables the operation of EOAM over the interface.</li> </ul>
<b>Mode</b>	<p>Select the mode of OAM operation for the Ethernet-like interface. The default option is <b>Active</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Active – Sets the remote OAM entity in a loopback state and initiates monitoring activities with the remote OAM peer entity. The remote OAM entity echoes back every received frame (except OAMPDUs) over the same interface on which the frame is received. The normal traffic is disabled and the looped back frames are transmitted on the interface.</li> <li>– Passive – Does not set the remote OAM entity in the loopback state and waits for the peer to initiate OAM actions.</li> </ul>
<b>LB Permit/Deny</b>	<p>Select a mechanism to provide control over processing of received OAM loopback commands, as the OAM loopback is a disruptive operation ( user traffic does not pass). The default option is <b>Deny</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Permit – Processes the OAM loopback commands that are used to monitor the health of the link.</li> <li>– Deny – Ignores the received loopback commands that are used to monitor the health of the link.</li> </ul>
<b>Operational Status</b>	<p>Displays the operational status of EOAM. This status is useful for the OAM entities that are placed on the same full-duplex Ethernet link and begin a discovery phase to determine the OAM capabilities to be used on an Ethernet link, at initialization and failure conditions. The values can be:</p> <ul style="list-style-type: none"> <li>– Disabled – OAM is disabled on the interface (EOAM Status is set as Disabled for the interface).</li> </ul>

	<ul style="list-style-type: none"> <li>- LinkFault – Link is transmitting OAMPDUs with a link fault indication. The fault indication is transmitted, when the link detects a fault or interface Admin State is set as Down or port Link is down.</li> <li>- PassiveWait – The OAM entity is waiting to see if the peer device is OAM capable. The EOAM Mode for the interface is set as Passive.</li> <li>- ActiveSendLocal – The OAM entity is actively trying to discover whether the peer has OAM capability, but the decision is not yet made. The EOAM Mode for the interface is set as Active.</li> <li>- SendLocalAndRemote – The local OAM entity has discovered the peer, but the configuration of the peer is not yet accepted or rejected.</li> <li>- SendLocalAndRemoteOk – The local OAM entity has discovered the peer and the configuration of the peer is accepted (OAM peering is allowed).</li> <li>- OamPeeringLocallyRejected – The local OAM entity has discovered the peer, but the configuration of the peer is rejected (OAM peering is declined).</li> <li>- OamPeeringRemotelyRejected – The remote OAM entity have rejected the OAM peering.</li> <li>- Operational – The local OAM entity learns that both it and the remote OAM entity have accepted the peering.</li> <li>- nonOperationalHalfDuplex – EOAM is enabled, but the interface is in half Duplex operation.</li> </ul>
<p><b>Remote LB</b></p>	<p>Displays the status of the EOAM remote loopback functionality in the interface. This value is communicated to the peer through the local configuration field of information OAMPDUs. The values can be:</p> <ul style="list-style-type: none"> <li>- Enable – EOAM remote loopback functionality is enabled. The OAM entity can initiate and respond to loopback commands.</li> <li>- Disable - EOAM remote loopback functionality is disabled.</li> </ul>

<b>Link Event</b>	<p>Displays the status of the EOAM link event(s) monitoring functionality in the interface. This value is communicated to the peer through the local configuration field of information OAMPDUs. The values can be:</p> <ul style="list-style-type: none"> <li>– Enable – EOAM link event(s) monitoring functionality is enabled. The OAM entity can send and receive event notification OAMPDUs.</li> <li>– Disable – EOAM link event(s) monitoring functionality is disabled.</li> </ul>
<b>Uni Directional</b>	<p>Displays the status of the Uni-Directional support in the interface. This value is communicated to the peer through the local configuration field of information OAMPDUs. The values can be:</p> <ul style="list-style-type: none"> <li>– Enable – Uni-Directional support is enabled. The OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only)</li> <li>– Disable – Uni-Directional support is disabled). The OAM entity does not support the transmission of OAMPDUs on links that are operating in unidirectional mode.</li> </ul>
<b>Variable Retrieval</b>	<p>Displays the status of the EOAM Variable Retrieval support in the interface. This value is communicated to the peer through the local configuration field of information OAMPDUs. The values can be:</p> <ul style="list-style-type: none"> <li>– Enable – EOAM Variable Retrieval support is enabled. The OAM entity can send and receive variable request and response OAMPDUs.</li> <li>– Disable – EOAM Variable Retrieval support is disabled.</li> </ul>

### 4.5.3 LinkEvent Settings

This screen allows the user to configure the event notification and thresholds to generate the standard EOAM events. EOAM generates and receives event notification OAMPDUs to indicate various link problems.

Select	Port	Symbol Period			Frame			Frame Period			Frame Seconds			Critical Event	Dying Gasp
		Enabled/Disabled	Window (millions)	Threshold	Enabled/Disabled	Window (100 msec)	Threshold	Enabled/Disabled	Window	Threshold	Enabled/Disabled	Window (100 msec)	Threshold		

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be applied
<b>Port</b>	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).
<b>Symbol Period</b>	<p>Select the symbol period status;</p> <ul style="list-style-type: none"> <li>– <b>Enabled/Disabled</b> - Select whether the OAM entity should send an Event Notification OAMPDU when an Error Symbol Period Event occurs. The Error Symbol Period Event is generated when the number of symbol errors exceeds a threshold within a configured window defined by a number of symbols. The default option is <b>Enabled</b>. The options are:           <ul style="list-style-type: none"> <li>▪ <b>Enabled</b> – Sends an Event Notification OAMPDU when an Error Symbol Period Event occurs. The OAMPDU is not sent even when the Error Symbol Period Event occurs, if the Link Event is set as Disable (EOAM link event(s) monitoring functionality not supported in the switch).</li> <li>▪ <b>Disabled</b> – Does not send an Event Notification OAMPDU even when an Error Symbol Period Event occurs.</li> </ul> </li> <li>– <b>Window (millions)</b> - Enter the number of symbols (millions) over which the <b>Threshold</b> event is defined. This value ranges from 1 to 18446744073709. The default value is the number of symbols in one second for the underlying physical layer.</li> </ul>

	<ul style="list-style-type: none"> <li>- <b>Threshold</b> - Enter the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU with an Error Symbol Period Event TLV. The default value is 1 symbol error. The Event Notification OAMPDU is sent periodically at the end of every window, if the threshold value is set as 0. In this case, the Event Notification OAMPDU is used as an asynchronous notification about the statistics related to the threshold crossing alarm, to the peer OAM entity.</li> </ul>
<p><b>Frame</b></p>	<p>Select the frame setting;</p> <ul style="list-style-type: none"> <li>- <b>Enabled/Disabled</b> - Select whether the OAM entity should send an Event Notification OAMPDU when an Error Frame Event occurs. The Error Frame Event is generated when the number of frame errors exceeds a Threshold within a configured Window defined by a period of time. The default option is <b>Enabled</b>. The list contains:             <ul style="list-style-type: none"> <li>▪ <b>Enabled</b> – Sends an Event Notification OAMPDU when an Error Frame Event occurs. The OAMPDU is not sent even when the Error Frame Event occurs, if the Link Event is set as Disable (that is, EOAM link event(s) monitoring functionality not supported in the switch).</li> <li>▪ <b>Disabled</b> – Does not send an Event Notification OAMPDU even when an Error Frame Event occurs.</li> </ul> </li> <li>- <b>Window (100 msec)</b> - Enter the amount of time (milli-seconds) over which the Threshold is defined. This value ranges from 10 to 600 milli- seconds. The default value is <b>10</b> milli-seconds (1 second).</li> <li>- <b>Threshold</b> - Enter the number of frame errors that must occur within a window for generating an Event notification OAMPDU with an Error Frame Event TLV. This value ranges from 1 to 4294967295. The default value is <b>1</b> frame error.</li> </ul>



<p><b>Frame Period</b></p>	<p>Select the frame period;</p> <ul style="list-style-type: none"> <li>- <b>Enabled/Disabled</b> - Select whether the OAM entity should send an Event Notification OAMPDU when an Error Frame Period Event occurs. The Error Frame Period Event is generated when the number of frame errors exceeds a Threshold within a configured Window defined by a number of frames. The default option is <b>Enabled</b>. The list contains: <ul style="list-style-type: none"> <li>▪ <b>Enabled</b> – Sends an Event Notification OAMPDU when an Error Frame Period Event occurs. The OAMPDU is not sent even when the Error Frame Period Event occurs, if the Link Event is set as Disable (EOAM link event(s) monitoring functionality not supported in the switch).</li> <li>▪ <b>Disabled</b> – Does not send an Event Notification OAMPDU even when an Error Frame Period Event occurs.</li> </ul> </li> <li>- <b>Window</b> - Enter the number of frames over which the threshold is defined. This value ranges from 1 to 4294967295. The default value is the number of minimum size Ethernet frames that can be received over the physical layer in one second.</li> <li>- <b>Threshold</b> - Enter the number of frame errors that must occur within the configured Window for generating an Event notification OAMPDU with an Error Frame Period Event TLV. This value ranges from 0 to 4294967294. The default value is 1 frame error. The Event Notification OAMPDU is sent periodically at the end of every Window, if the threshold value is set as 0. In this case, the Event Notification OAMPDU is used as an asynchronous notification about the statistics related to the threshold crossing alarm, to the peer OAM entity.</li> </ul>
<p><b>Frame Seconds</b></p>	<p>Select the frame seconds value;</p>

	<ul style="list-style-type: none"> <li>- <b>Enabled/Disabled</b> - Select whether the OAM entity should send an Event Notification OAMPDU when an Error Frame Seconds Event occurs. The Error Frame Seconds Event is generated when the number of errored frame seconds exceeds a Threshold within a configured Window defined by time period. The errored frame second is defined as a one second interval that has at least one frame error. The default option is <b>Enabled</b>. The list contains:             <ul style="list-style-type: none"> <li>▪ <b>Enabled</b> – Sends an Event Notification OAMPDU when an Error Frame Seconds Event occurs. The OAMPDU is not sent even when the Error Frame Seconds Event occurs, if the Link Eventy is set as Disable (EOAM link event(s) monitoring functionality not supported in the switch).</li> <li>▪ <b>Disabled</b> – Does not send an Event Notification OAMPDU even when an Error Frame Seconds Event occurs.</li> </ul> </li> <li>- <b>Window (100 msec)</b> - Enter the amount of time (milli-seconds) over which the threshold is defined. This value ranges from 100 to 9000 milli- seconds. The default value is <b>100</b> milli-seconds (10 seconds).</li> <li>- <b>Threshold</b> - Enter the number of errored frame seconds that must occur within the configured window for generating an Event notification OAMPDU with an Error Frame Seconds Summary Event TLV. This value ranges from 1 to 900. The default value is <b>1</b> errored frame second. The Event Notification OAMPDU is sent periodically at the end of every window, if the threshold value is set as 0. In this case, the Event Notification OAMPDU is used as an asynchronous notification about the statistics related to the threshold crossing alarm, to the peer OAM entity.</li> </ul>
<p><b>Critical Event</b></p>	<p>Select whether the local OAM entity should attempt to indicate a critical event through the OAMPDU flags to its peer OAM</p>

	<p>entity when a critical event (defined by the switch) occurs. The default option is <b>Enabled</b> for the Ethernet-like interfaces that support OAM. The list contains:</p> <ul style="list-style-type: none"> <li>– <b>Enabled</b> – Indicates the critical event to the peer OAM entity.</li> <li>– <b>Disabled</b> – Does not indicate the critical event to the peer OAM entity.</li> </ul>
<b>Dying Gasp</b>	<p>Select whether the local OAM entity should attempt to indicate a dying gasp through the OAMPDU flags field to its peer OAM entity when a dying gasp event (defined by the switch) occurs. The default option is <b>Enabled</b> for the Ethernet-like interfaces that support OAM. The list contains:</p> <ul style="list-style-type: none"> <li>– <b>Enabled</b> – Indicates the dying gasp to the peer OAM entity.</li> <li>– <b>Disabled</b> – Does not indicate the dying gasp to the peer OAM entity.</li> </ul>

### 4.5.4 Loopback Settings

This screen allows the user to configure the loopback state of the local link. Loopback is used to place the remote OAM entity in a state where every received frame (except OAMPDUs) is echoed back over the same interface on which the frames are received. The normal traffic is disabled at the remote entity and only the loopback frames are transmitted on the interface.

Select	Port	Remote LB enable/disable
<input type="radio"/>	Gi0/1	No Loopback <input type="button" value="v"/>
<input checked="" type="radio"/>	Gi0/2	No Loopback <input type="button" value="v"/>

Label	Description
<b>Select</b>	Click to select the port for which the configuration needs to be done.
<b>Port</b>	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).
<b>Remote LB</b>	Select the loopback status for the OAM entity. This status is

<p><b>enable/disable</b></p>	<p>determined by a combination of the local parser and multiplexer states, the remote parser and multiplexer states and by the actions of the local OAM client. The list contains:</p> <ul style="list-style-type: none"> <li>- No Loopback – Local OAM client operates in normal mode with no loopback in progress.</li> <li>- Initiating – OAM client is waiting for a response for the loopback OAMPDU sent after initiating a loopback. The local OAM entity has not yet received any acknowledgment from the remote OAM entity regarding the reception of loopback command request.</li> <li>- Remote - LB – Local OAM client knows that the remote OAM entity is in loopback mode.</li> <li>- Terminating - LB – Local OAM client is in the process of terminating the remote loopback.</li> <li>- Local - LB – Remote OAM client has put the local OAM entity in loopback mode.</li> <li>- Unknown – The OAM loopback is in a transition state.</li> </ul>
------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 4.6 RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

### 4.6.1 Basic Settings

The screen allows the user to configure the RMON status. Once the status is enabled RMON starts monitoring the remote networks and collects data for storage in the table.



Label	Description
<b>RMON Status</b>	<p>Select the status of RMON on the switch. The default option is <b>Disabled</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Enabled - Enables RMON in the switch. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis.</li> <li>– Disabled - Disables RMON in the switch. On disabling, the RMON's network monitoring is called off.</li> </ul>

## 4.6.2 Alarms

This screen allows the user to configure RMON alarm settings. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. This is done to raise an alarm when the specified alarm condition occurs.

Label	Description
<b>Index</b>	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 from 1 to 65535.
<b>Interval</b>	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 from 1 to 65535.
<b>Variable</b>	Enter the MIB object variable on which the alarm is set. For successful configuration the Variable has to be a valid Object

	ID.
<b>Sample type</b>	<p>Select the sample type to be compared against the thresholds. The default option is <b>Absolute value</b>. The list contains:</p> <ul style="list-style-type: none"> <li>– Absolute value - Compares the value of the selected variable directly with the thresholds at the end of the sampling interval.</li> <li>– Delta value - Subtracts the value of the selected variable at the last sample from the current value, and compares the difference with the thresholds at the end of the sampling interval.</li> </ul>
<b>Rising Threshold</b>	Enter the Rising Threshold value. This value ranges from 0 to 2147483647.
<b>Falling Threshold</b>	Enter the Falling Threshold value. This value ranges from 0 to 2147483647.
<b>Rising Event Index</b>	Enter the index of the event to be raised when the Rising threshold is reached. This value ranges from 1 to 65535.
<b>Falling Event Index</b>	Enter the index of the event to be raised when the Falling threshold is reached. This value ranges from 1 to 65535.
<b>Owner</b>	Enter the entity details that configured this entry and is using the resources assigned to it.
<b>Select</b>	Select the index to modify the attributes of the selected entry.
<b>Alarm Value</b>	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 absolute Value, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds.
<b>Startup Alarm</b>	<p>Displays the alarm that is sent when the entry is set as valid for the first time. The list contains:</p> <ul style="list-style-type: none"> <li>– RisingAlarm – Denotes that the first sample after the entry becoming valid is greater than or equal to the rising threshold.</li> </ul>

	<ul style="list-style-type: none"> <li>- FallingAlarm – Denotes that the first sample after the entry becoming valid is less than or equal to the falling threshold.</li> <li>- RisingOrFallingAlarm – Denotes that either Rising or Falling Alarm is sent based on the sample in comparison with the rising and falling threshold.</li> </ul>
<b>Status</b>	<p>Select the required status of alarm. The list contains:</p> <ul style="list-style-type: none"> <li>- Valid – Sets the status as <b>Valid</b> if the entry is completely created.</li> <li>- Under Creation – Sets the status as Under Creation if the entry is created and not completely configured</li> <li>- Entries in this state are not fully active. Entries exists in the Under Creation state until the management station has finished configuring the entry and sets this object to valid or invalid state. Invalid – Sets this status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry.</li> </ul>

### 4.6.3 Ethernet Statistics

This screen contains statistics measured by the probe for each monitored interface on the device. The statistics in this group reflect all packets on the local network segment attached to the identified interface.

Index  \*

Data Source  \*

Owner

Select	Index	Data Source	Drop Events	Octets	Packets	Broadcast Packets	Multiast Packets	Owner	Status
<input type="button" value="Apply"/>									

Label	Description
<b>Index</b>	Enter the Ethernet Statistics index that uniquely identifies an entry in the Ethernet Statistics table. This value ranges from 1 to 65535.

<b>Data Source</b>	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
<b>Owner</b>	Enter the details of the entity that configured this entry and is using the resources assigned to it
<b>Select</b>	Select the index to modify the attributes of the selected entry.
<b>Drop Events</b>	Displays the number of events in which the packets were dropped by the probe due to lack of resources. This number does not specify the number of packets dropped but the number of times the packets were dropped.
<b>Octets</b>	Displays the total number of octets of data received from the network (excluding the framing bits but including FCS octets). This can be used as a reasonable estimate of 10-Megabit Ethernet utilization.
<b>Packets</b>	Displays the total number of packets received from the network. This includes bad packets, broadcast packets and multicast packets received.
<b>Broadcast Packets</b>	Displays the total number of good packets received that were directed to the broadcast address.
<b>Multiast Packets</b>	Displays the total number of good packets received that were directed to the multicast address.
<b>Status</b>	Select the required status of event. The list contains: <ul style="list-style-type: none"> <li>– Valid – Sets the status as <b>Valid</b> if the entry is completely created.</li> <li>– Under Creation – Sets the status as Under Creation if the entry is created and not completely configured</li> </ul>

#### 4.6.4 Events

This screen allows the user to configure RMON event settings. 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.



Event Index	<input type="text"/>
Description	<input type="text"/>
Type	None <input type="button" value="v"/>
Community	<input type="text"/>
Owner	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Select	Event Index	Description	Type	Community	Owner	Last Time Sent	Status
<input type="radio"/>	34	event1	None <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	0	Valid <input type="button" value="v"/>
<input type="radio"/>	48	event2	None <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	0	Valid <input type="button" value="v"/>
<input checked="" type="radio"/>	65535	event3	None <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	0	Valid <input type="button" value="v"/>
<input type="button" value="Apply"/>							

Label	Description
<b>Event Index</b>	Enters a number that uniquely identifies an entry in the Events table. Each such entry defines one event that is to be generated when appropriate conditions occur. This values ranges from 1 to 65535.
<b>Description</b>	Enter a brief description of the event. This value is a string of maximum size 127.
<b>Type</b>	Select the type of event to be configured. This is the type of notification that the probe makes about this event. The list contains: <ul style="list-style-type: none"> <li>- Log - Creates an entry in the log table for each event.</li> <li>- SNMP Trap - Sends an SNMP trap to one or more management stations</li> <li>- Log and Trap – Creates an entry in the log table and sends an SNMP trap.</li> <li>- None – Sets the event type as <b>None</b> which implies that no notifications are sent.</li> </ul>
<b>Community</b>	Enter the SNMP community string to which the SNMP trap is to be sent.
<b>Owner</b>	Enter the entity that configured this entry and is using the resources assigned to it.
<b>Select</b>	Select the index to modify the attributes of the selected entry.
<b>Last Time Sent</b>	Displays the time this event entry last generated an event. If this entry has not generated any events, the value will be zero.
<b>Status</b>	Select the required status of event. The list contains:

	<ul style="list-style-type: none"> <li>- Valid – Sets the status as Valid if the entry is completely created.</li> <li>- Under Creation – Sets the status as Under Creation if the entry is created and not completely configured</li> </ul>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.6.5 History

This screen allows the user to configure RMON history settings. The History module controls the periodic statistical sampling of the data collected by statistics module from various types of networks. This module stores the sample collected from the etherstat table to the etherHistory table

Index  \*

Data Source  \*

Buckets Requested

Interval

Owner

Select	Index	Data Source	Buckets Requested	Buckets Granted	Interval	Owner	Status
<input type="button" value="Apply"/>							

Label	Description
<b>Index</b>	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. This value ranges from 1 to 65535.
<b>Data Source</b>	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.
<b>Buckets Requested</b>	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 from 1 to 65535. The default value is <b>50</b> .
<b>Interval</b>	Enter the time interval (in seconds) over which the data is sampled for each bucket to collect the statistics. This value ranges from 1 to 3600 seconds. The default value is <b>1800</b> seconds.
<b>Owner</b>	Enter the details of the entity that configured this entry and is using the resources assigned to it.
<b>Select</b>	Select the index to modify the attributes of the selected entry.
<b>Buckets Granted</b>	Displays the number of buckets granted for collecting the RMON statistics. This is the number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this History Control Entry. This value ranges from 1 to 65535. This is a read-only field.
<b>Status</b>	Select the required status of event. The list contains: <ul style="list-style-type: none"> <li>– Valid – Sets the status as <b>Valid</b> if the entry is completely created.</li> <li>– Under Creation – Sets the status as Under Creation if the entry is created and not completely configured</li> <li>– Invalid – Sets this status as Invalid if the entry is removed. It also effectively disassociates the mapping identified with the entry</li> </ul>

## 4.7 Statistics

The Statistics link allows the user to view the various displays screens for the configurations applied to the system.

### 4.7.1 Interface

The Interface link allows the user to view the interface related statistics screens through the following tabs.

#### 4.7.1.1 Interface Clear

This screen allows the user to clear the details in the interface counter for a particular interface or for all the interfaces.

Clear Interface Counters  All  
 Interface

Interface  ▼

Label	Description
<b>Clear Interface Counters</b>	Choose to clear all counters or only interface counters.
<b>Interface</b>	Select an interface from the drop-down list.

### 4.7.1.2 Interface

This screen displays the management information applicable to all the interfaces available in the switch.

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	Transmitted Nunicast Packets	Transmitted Discards	Transmitted Errors
Gi0/1	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/2	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/3	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/4	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/5	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/6	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0
Gi0/7	1500	10000000000	0	0	0	0	0	0	0	0	0	0	0

### 4.7.1.3 Ethernet

This screen displays the statistics for a collection of Ethernet-like interfaces attached to the RGS-PR9000-A.

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	Frame Too Long	Received Internal MAC Errors	Ether ChipSet	Symbol Errors	Duplex Status
Gi0/1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/5	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼
Gi0/7	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex ▼

## 4.7.2 MSTP

The MSTP link allows the user to view the MSTP statistics screens through the following tabs.

### 4.7.2.1 Information

This screen displays the information corresponding to the Multiple Spanning Tree protocol.



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	Protocol Migration Count	Effective Port State	EdgePort Oper Status	Link Type	PseudoRootId
------	--------------------	------------------------------	--------------	-----------------------	---------------------------------	-----------------	----------------------------	--------------------------------------	----------------------------	--------------------------	----------------------	----------------------	-----------	--------------

## 4.7.4 LA

The LA link allows the user to view the LA statistics screens through the following tabs.

### 4.7.4.1 PortLACP Stats

This screen displays the Link Aggregation Protocol statistics for each port on the device.

Port	Received PDUs	Received Marker PDUs	Received Marker Response	Received Unknown PDUs	Received Illegal PDUs	Transmitted PDUs	Transmitted Marker PDUs	Transmitted Marker Response
Gi0/1	0	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0	0

### 4.7.4.2 Neighbour Stats

This screen displays the Neighbor statistics for each port on the device.

Port	Partner SystemID	Oper Key	Partner Port Priority
Gi0/1	00:00:00:00:00:00	0	0
Gi0/2	00:00:00:00:00:00	0	0
Gi0/3	00:00:00:00:00:00	0	0
Gi0/4	00:00:00:00:00:00	0	0
Gi0/5	00:00:00:00:00:00	0	0
Gi0/6	00:00:00:00:00:00	0	0
Gi0/7	00:00:00:00:00:00	0	0

## 4.7.5 LLDP

The LLDP link allows the user to view the LLDP statistics screens through the following tabs.

### 4.7.5.1 Traffic

This screen allows the user to view or clear the LLDP counters on specified interface.

Interface	Frames out	Entries Aged	Frames In	Frames Rx in Error	Frames Discarded	Unrecognized TLVs	Total TLVs Discarded	PDU length error Drops
Gi0/1	461	9	387	0	0	0	0	0
Gi0/2	461	9	387	0	0	0	0	0
Gi0/3	461	9	387	0	0	0	0	0
Gi0/4	461	9	387	0	0	0	0	0
Gi0/5	461	9	387	0	0	0	0	0
Gi0/6	461	9	387	0	0	0	0	0
Gi0/7	461	9	387	0	0	0	0	0

### 4.7.5.2 Statistics

This screen displays the LLDP remote table statistics information.

Remote Table Last Change Time	<input type="text" value="1201000"/>
Remote Table Inserts	<input type="text" value="11"/>
Remote Table Deletes	<input type="text" value="10"/>
Remote Table Drops	<input type="text" value="0"/>
Remote Table Ageouts	<input type="text" value="9"/>
Remote Table Updates	<input type="text" value="0"/>

### 4.7.5.3 Errors

This screen displays the details of LLDP error information such as total memory allocation failures and count of total input queue overflows.

Total Memory Allocation Failures	<input type="text" value="0"/>
Total Input Queue Overflows	<input type="text" value="0"/>
Total Table Overflows	<input type="text" value="0"/>

## 4.7.6 802.1x

The 802.1x link allows the user to view the 802.1x statistics screens through the following tabs.

### 4.7.6.1 Session Stats

This screen displays the session statistics for an authenticator PAE (Port Access Entity). It

shows the current values collected for each session that is still in progress or the final values for the last valid session on each port where there is no current active session.

Port	Session ID	Received Frames	Transmitted Frames	Session Time (secs)	Session Terminate Cause	User Name
------	------------	-----------------	--------------------	---------------------	-------------------------	-----------

### 4.7.6.2 Supp-Session Stats

This screen displays the Supplicant Session statistics.

Port	Eapol FrRx	Eapol FrTx	Eapol Start FrTx	Eapol Logoff FrTx	Eapol Respld FrTx	Eapol Resp FrTx	Eapol Reqld FrRx	Eapol Req FrRx	Invalid Eapol FrRx	Eap LenErr FrRx	Last Eapol FrVersion	Last Eapol FrSource
------	------------	------------	------------------	-------------------	-------------------	-----------------	------------------	----------------	--------------------	-----------------	----------------------	---------------------

### 4.7.6.3 Mac-Session Stats

This screen displays the MAC Session statistics.

Select	Supplicant MacAddr	Frames Rx	Frames Tx	Session ID	Session Terminate Cause	User Name
--------	--------------------	-----------	-----------	------------	-------------------------	-----------

## 4.7.7 RADIUS

This screen displays the 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
-------	-----------------------	-----------------	-----------------	-----------------------	-----------------------------	-----------------------------	-----------------------------	--------------------------------	----------------------------------	--------------------------	------------------------	-----------------	---------------------

## 4.7.8 IGMP Snooping

The IGMP Snooping link allows the user to view the IGMP Snooping related statistics screens through the following tabs.

### 4.7.8.1 IGS Clear Statistics

This screen displays the IGMP snooping clear statistics.

Clear Vlan Counters  All  Vlan ID

Vlan ID

### 4.7.8.2 IGS Statistics

This screen displays the IGMP snooping statistics pertaining to IGMP snooping v1 and v2.

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 Transmitted
---------	--------------------------	------------------------	-----------------------------------	-----------------------	----------------------	----------------------	-----------------------------	---------------------------	--------------------------	-------------------------



### 4.7.8.3 IGS V3 Statistics

This screen displays the IGMP snooping statistics pertaining to IGMP snooping v3.

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
---------	---------------------	---------------------------	---------------------------	---------------------------	---------------------------	-------------------------	-------------------------	-----------------

## 4.7.9 MLD Snooping

The MLD Snooping link allows the user to view the IGMP Snooping related statistics screens through the following tabs.

### 4.7.9.1 MLDS Statistics

This screen displays the MLD snooping statistics pertaining to MLDv1.

VLAN ID	General Queries Received	Group Queries Received	Group and Source Queries Received	MLD Reports Received	MLD Dones Received	MLD Packets Dropped	General Queries Transmitted	Group Queries Transmitted	MLD Reports Transmitted	MLD Dones Transmitted
---------	--------------------------	------------------------	-----------------------------------	----------------------	--------------------	---------------------	-----------------------------	---------------------------	-------------------------	-----------------------

### 4.7.9.2 MLDS V2 Statistics

This screen displays the MLD snooping statistics pertaining to MLDv2.

VLAN ID	V2 Reports Received	IS_INCL Messages Received	IS_EXCL Messages Received	TO_INCL Messages Received	TO_EXCL Messages Received	ALLOW Messages Received	BLOCK Messages Received	V2 Reports Sent
---------	---------------------	---------------------------	---------------------------	---------------------------	---------------------------	-------------------------	-------------------------	-----------------

## 4.7.10 IP

The IP link allows the user to view the IPv4 related statistics screens through the following tabs.

### 4.7.10.1 ARP Cache

This screen displays the ARP cache related statistics information such as MAC address, for all interfaces of the switch.

Interface	MAC Address	IP Address	Media Type
vlan1	00:1d:aa:82:94:e0	192.168.2.1	Dynamic
vlan1	90:2b:34:83:e6:35	192.168.2.25	Dynamic
vlan1	74:d4:35:ca:c9:03	192.168.2.131	Dynamic
vlan1	ac:22:0b:7e:8f:33	192.168.2.233	Dynamic

### 4.7.10.2 ICMP Statistics

This screen displays the ICMP transmission and reception related statistics information such as Received Redirect, Transmitted Error and so on.

Received Message	2415
Received Error	0
Receive Destination Unreachable	0
Received Redirect	0
Received Echo Requests	2415
Received Echo Replies	0
Receive Source Quenches	0
Transmitted Message	4510
Transmitted Error	3
Transmitted Destination Unreachable	2095
Transmitted Redirect	0
Transmitted Echo Requests	0
Transmitted Echo Replies	2415
Transmitted Source Quenches	0

### 4.7.10.3 IPV4 IfSp Stats

This screen displays the IPv4 specific statistics information such as HCInOct, for all interfaces available in the switch.

VersionType	Iface	HCRcvd	HCInOct	Hdr Errs	InNoRoutes	Adr Errs	UnknownProtos	Truncd Pkts	HCForwardDatagrams	Reasm Reqds	Reasm OKs	Reasm Fails	Discdrs	HCInDelivers		
IPV4	37	81603	8908573	0	1	0	0	0	1	0	0	0	0	66584		
HCOut Rqst	HCOut FwdDgms	Out Discards	Out FragRqds	Out FragOk	Out FragFails	Frag Creates	HcOut Transmits	HCOutOct	HCRcvd Mcast Pkts	HCRcvd Mcast Octs	HCSend Mcast Pkts	HCSend Mcast Octs	HCRcvd Bcast Pkts	HCSend Bcast Pkts	DisConty time	Refresh Rate
22065	0	0	0	0	0	0	22065	6309993	0	0	0	0	45762	3	0	1000

### 4.7.10.4 IPV4 SysSp Stats

This screen displays the IPv4 specific global statistics information such as HCRcvd, for the switch.

VersionType	HCRcvd	HCInOct	HdrErrs	InNoRoutes	AdrErrs	UknownProtos	Trunctd Pkts	HCForwardDatagrams	ReasmReqds	ReasmOKs	ReasmFails	Discdrs	HCInDelivers	HCOutRqst	
IPv4	83528	9134494	0	1	0	0	0	1	0	0	0	0	67417	22637	
HCOutFwdDgms	OutDiscards	OutFragRqds	OutFragOKs	OutFragFails	FragCreates	HcOutTransmits	HCOutOct	HCRcvdMcastPkts	HCRcvdMcastOcts	HCSendMcastPkts	HCSendMcastOcts	HCRcvdBcastPkts	HCSendBcastPkts	DisContytime	RefreshRate
0	0	0	0	0	0	22636	6529931	0	0	0	0	46100	3	0	1000

### 4.7.11 RIP

Context Id	IP Address	Received Bad Packets	Received Bad Routes	Triggered Updates	Periodic Updates
------------	------------	----------------------	---------------------	-------------------	------------------

This screen displays the Routing Information Protocol statistics for each of the interface in the device.

### 4.7.12 OSPF

The OSPF link allows the user to view the OSPF statistics screens through the following tabs.

#### 4.7.12.1 Route Information

This screen displays the information regarding the OSPF routes. It includes the IP Address, Mask, Type Of Service, Next Hop, Interface index, Route type, Cost, Area ID, and Type 2 Cost.

Context Name	IP Address	Subnet Mask	TOS	Gateway	Type	Area ID	Cost	Type 2 Cost	Interface
--------------	------------	-------------	-----	---------	------	---------	------	-------------	-----------

#### 4.7.12.2 Link State Database

This screen displays the information on a single Link State Advertisement. It includes the link state ID, type, area ID, router ID, age, sequence and checksum.

Context Id	Area ID	Type	Link State ID	Router ID	Sequence	Checksum	Age
------------	---------	------	---------------	-----------	----------	----------	-----

#### 4.7.12.3 Redundancy Information

This screen displays the OSPF redundancy information such as HotStandby Admin State, HotStandby State, HotStandby Bulk Update Status, No Of Hellos Synced and No Of LSAs Synced available in the switch.

HotStandby Admin State	<input type="text" value="Disabled"/>
HotStandby State	<input type="text" value="Active StandbyDown"/>
HotStandby Bulk Update Status	<input type="text" value="Not Started"/>
No Of Hellos Synced	<input type="text" value="0"/>
No Of LSAs Synced	<input type="text" value="0"/>

### 4.7.13 VRRP

This screen displays the VRRP Global Statistics and per VRID Statistics.

#### Global Statistics

Checksum Errors	Version Errors	Virtual Router ID Errors
0	0	0

#### Per VRID

Virtual Router ID	Interface Address	Address Type	Transitions to Master	New Master Reason	Advertisement Received	V3 Advertisement Transmitted	V2 Advertisement Transmitted	V2 Advertisement ignored	Skew Time (in msec)	Master Down Interval (in msec)	Received Master Advt Interval (in msec)	Advertisement Interval Error
-------------------	-------------------	--------------	-----------------------	-------------------	------------------------	------------------------------	------------------------------	--------------------------	---------------------	--------------------------------	-----------------------------------------	------------------------------

Auth Fail	IP TTL Errors	Priority Zero Packet Received	Priority Zero Packet Transmitted	Invalid Packet Type Received	Address List Errors	Invalid Authentication Type	Authentication Type Mismatch	Packet Length Errors	Proto Error Reason
-----------	---------------	-------------------------------	----------------------------------	------------------------------	---------------------	-----------------------------	------------------------------	----------------------	--------------------

### 4.7.14 IGMP

This screen displays various IGMP statistics including IGMP Queries received and transmitted, IGMP reports (v1/v2/v3) received, and IGMP leaves received.

Interface	General queries received	Group queries received	Group and source queries received	V1/V2 reports received	V3 reports received	General queries transmitted	Group queries transmitted	Group and source queries transmitted
-----------	--------------------------	------------------------	-----------------------------------	------------------------	---------------------	-----------------------------	---------------------------	--------------------------------------

### 4.7.15 MLD

This screen displays the MLD Statistics Information.

Interface	General queries received	Group queries received	Group and source queries received	V1 reports received	V2 reports received	General queries transmitted	Group queries transmitted	Group and source queries transmitted
-----------	--------------------------	------------------------	-----------------------------------	---------------------	---------------------	-----------------------------	---------------------------	--------------------------------------

### 4.7.16 IGMP Proxy

This screen displays the IGMP Proxy related statistics information such as the V1/V2 and V3 reports transmitted and leaves received.

Interface	V1/V2 reports transmitted	V3 reports transmitted	V2 Leaves transmitted
-----------	---------------------------	------------------------	-----------------------

### 4.7.17 RMON

This screen displays the collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.

Index	Data Source	Drop Events	Packets	Octets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packets
etherStatsIndex_KEY	etherStatsDataSource_KEY	etherStatsDropEvents_KEY	etherStatsPkts_KEY	etherStatsOctets_KEY	etherStatsBroadcastPkts_KEY	etherStatsMulticastPkts_KEY	etherStatsCRCAlignErrors_KEY	etherStatsUndersizePkts_KEY	etherStatsOversizePkts_KEY
Fragments	Jabbers	Collisions	Out FCS Errors	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets		
etherStatsFragments_KEY	etherStatsJabbers_KEY	etherStatsCollisions_KEY	rmonStatsOutFCSErrors_KEY	etherStatsPkts64Octets_KEY	etherStatsPkts65to127Octets_KEY	etherStatsPkts128to255Octets_KEY	etherStatsPkts256to511Octets_KEY		
512-1023 Octets	1024-1518 Octets	Overflow Packets	Overflow Octets	Overflow 64 Octets	Overflow 65-127 Octets				
etherStatsPkts512to1023Octets_KEY	etherStatsPkts1024to1518Octets_KEY	etherStatsHighCapacityOverflowPkts_KEY	etherStatsHighCapacityOverflowOctets_KEY	etherStatsHighCapacityOverflowPkts64Octets_KEY	etherStatsHighCapacityOverflowPkts65to127Octets_KEY				
Overflow 128-255 Octets	Overflow 256-511 Octets	Overflow 512-1023 Octets	Overflow 1024-1518 Octets						
etherStatsHighCapacityOverflowPkts128to255Octets_KEY	etherStatsHighCapacityOverflowPkts256to511Octets_KEY	etherStatsHighCapacityOverflowPkts512to1023Octets_KEY	etherStatsHighCapacityOverflowPkts1024to1518Octets_KEY						

# Command Line Interface Management

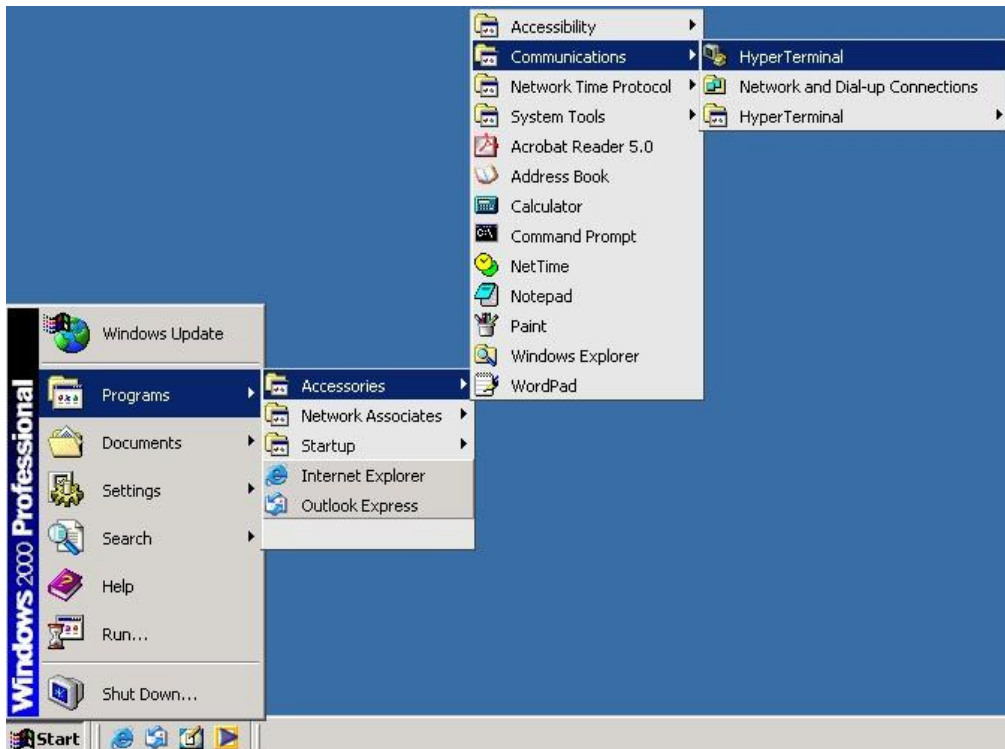
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

## **CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)**

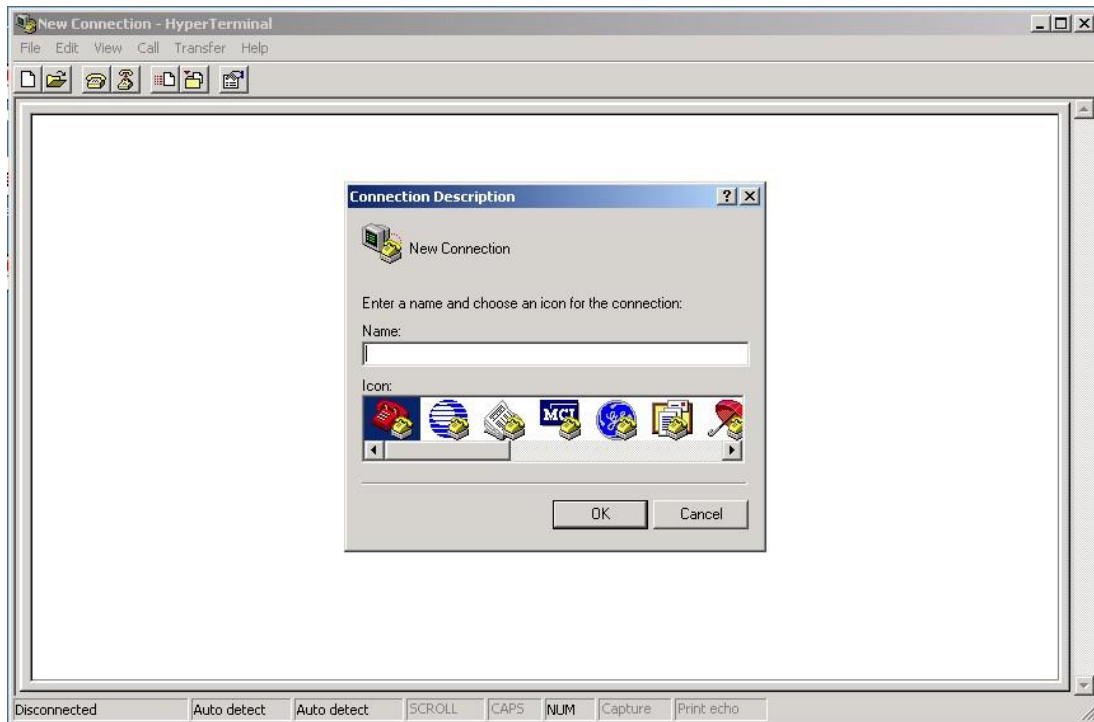
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

Follow the steps below to access the console via RS-232 serial cable.

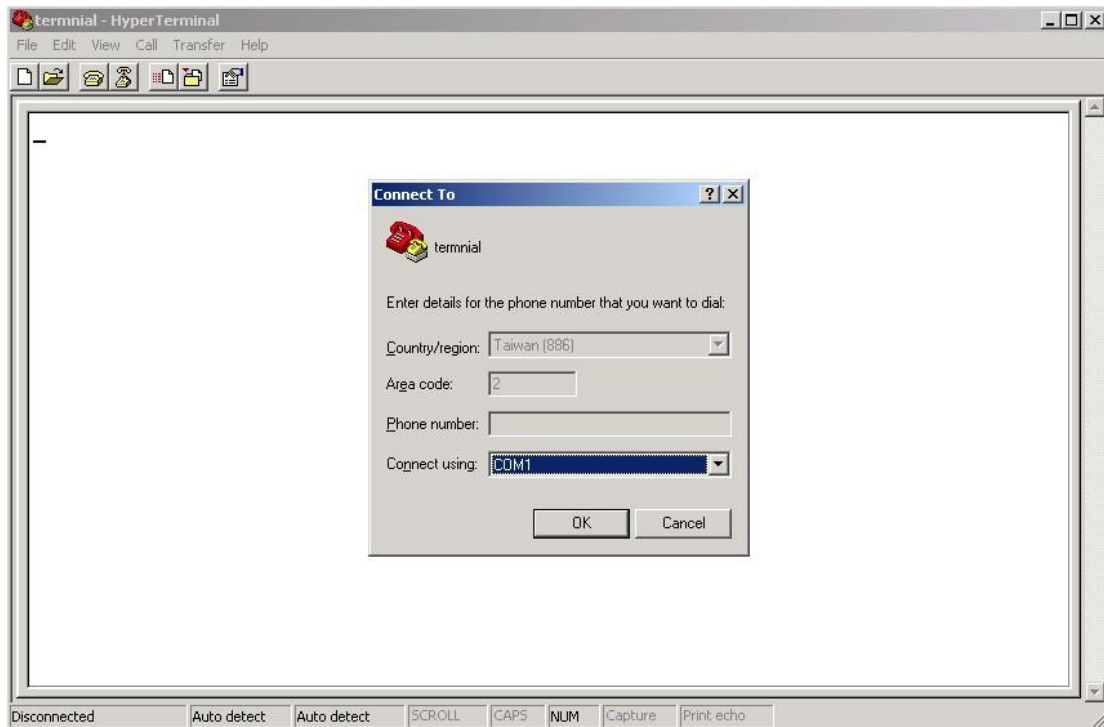
Step 1: On Windows desktop, click on **Start -> Programs -> Accessories -> Communications -> Hyper Terminal**



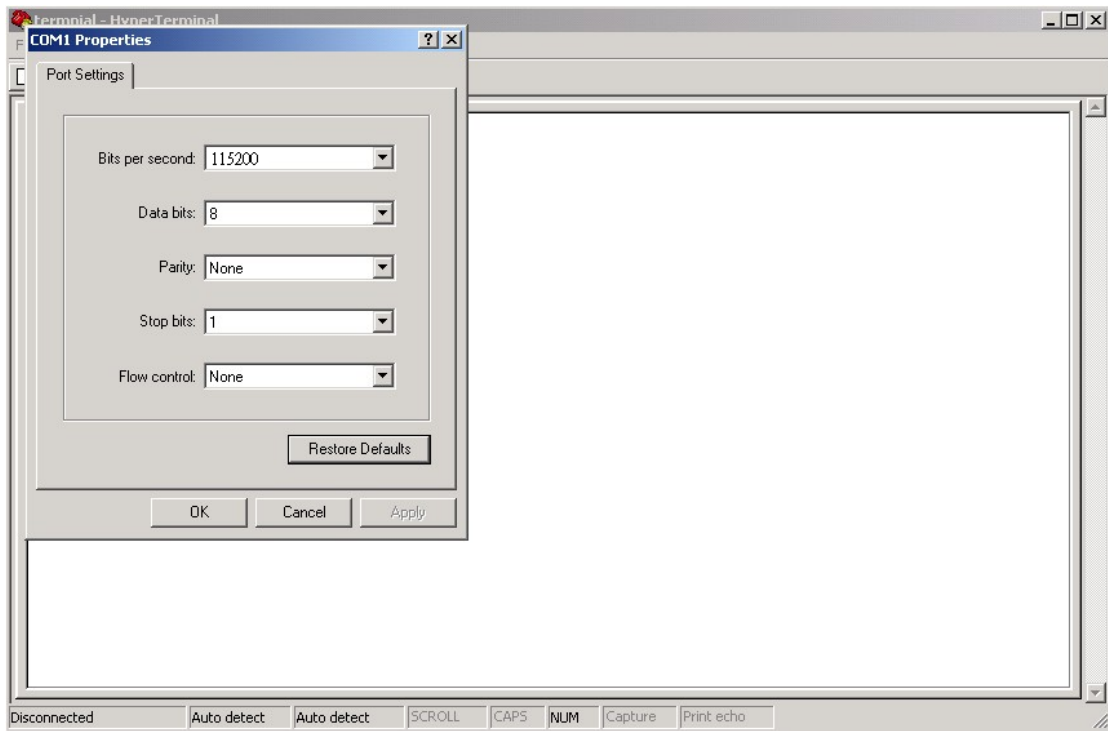
Step 2: Input a name for the new connection.



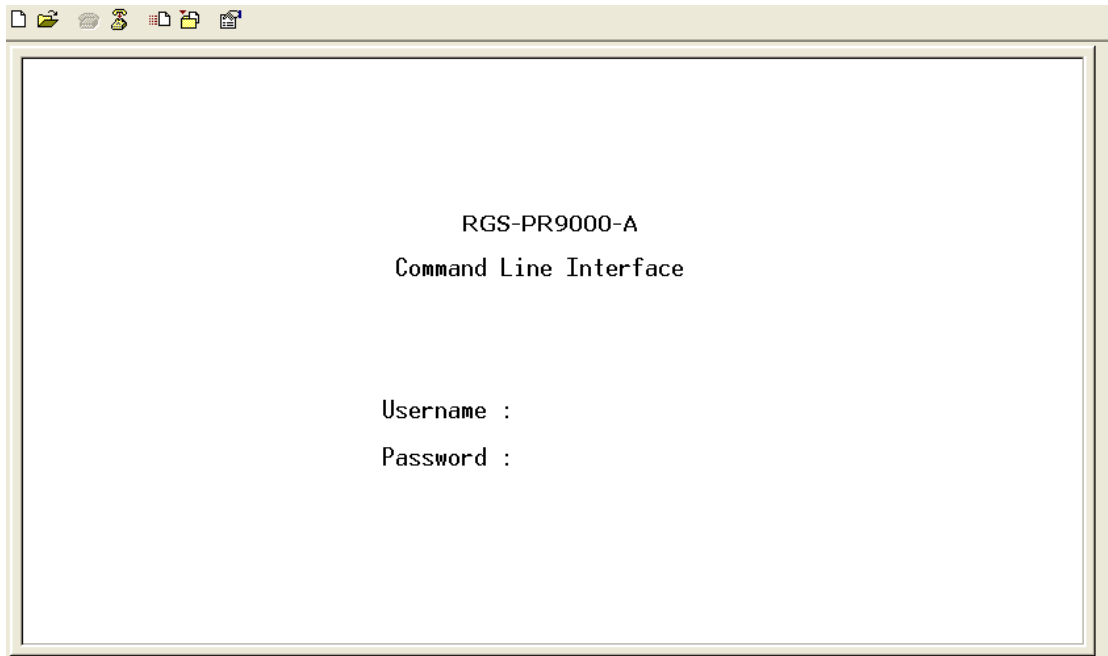
Step 3: Select a COM port in the drop-down list.



Step 4: A pop-up window that indicates COM port properties appears, including bits per second, data bits, parity, stop bits, and flow control.



Step 5: The console login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browsers), then press **Enter**.



**CLI Management by Telnet**

You can use **TELNET** to configure the switch. The default values are:

IP Address: **192.168.10.1**



Subnet Mask: **255.255.255.0**

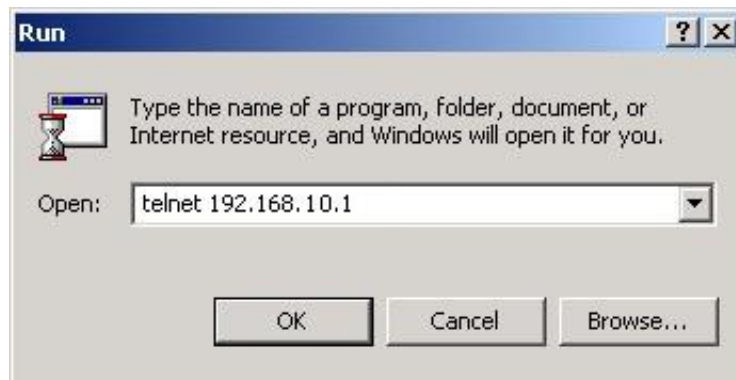
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access console via Telnet.

Step 1: Telnet to the IP address of the switch from the **Run** window by inputting commands (or from the MS-DOS prompt) as below.



Step 2: The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter**.

**Commander Groups**

```

Command Groups:
-----
System      : System settings and reset options
IP          : IP configuration and Ping
Port       : Port management
MAC        : MAC address table
ULAN       : Virtual LAN
PULAN      : Private ULAN
Security    : Security management
STP        : Spanning Tree Protocol
Aggr       : Link Aggregation
LACP       : Link Aggregation Control Protocol
LLDP       : Link Layer Discovery Protocol
PoE        : Power Over Ethernet
QoS        : Quality of Service
Mirror     : Port mirroring
Config     : Load/Save of configuration via TFTP
Firmware   : Download of firmware via TFTP
PTP        : IEEE1588 Precision Time Protocol
Loop Protect : Loop Protection
IPMC       : MLD/IGMP Snooping
Fault      : Fault Alarm Configuration
Event      : Event Selection
DHCP Server : DHCP Server Configuration
Ring       : Ring Configuration
Chain      : Chain Configuration
RCS        : Remote Control Security
Fastrecovery : Fast-Recovery Configuration
SFP        : SFP Monitor Configuration
DeviceBinding : Device Binding Configuration
MRP        : MRP Configuration
Modbus     : Modbus TCP Configuration
    
```

**System**

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
Log [<log_id>] [all info warning error] [clear]	

**IP**

IP>	Configuration
	DHCP [enable disable]

	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]
	SNTP [<ip_addr_string>]

### Port

port>	Configuration [<port_list>] [up down]
	Mode [<port_list>] [auto 10hdx 10fdx 100hdx 100fdx 1000fdx sfp_auto_ams]
	Flow Control [<port_list>] [enable disable]
	State [<port_list>] [enable disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable disable actiphy dynamic]
	Excessive [<port_list>] [discard restart]
	Statistics [<port_list>] [<command>] [up down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

### MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto disable secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

### VLAN

VLAN>	Configuration [<port_list>]
	PVID [<port_list>] [<vid> none]
	FrameType [<port_list>] [all tagged untagged]
	IngressFilter [<port_list>] [enable disable]
	tx_tag [<port_list>] [untag_pvid untag_all tag_all]
	PortType [<port_list>] [unaware c-port s-port s-custom-port]

	EtypeCustomSport [<etype>]
	Add <vid> <name> [<ports_list>]
	Forbidden Add <vid> <name> [<port_list>]
	Delete <vid> <name>
	Forbidden Delete <vid> <name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)]
	[combined static nas all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
	Status [<port_list>]
[combined static nas mstp all conflicts]	

**Private VLAN**

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable disable]

**Security**

Security >	Switch <b>Switch security setting</b>
	Network <b>Network security setting</b>
	AAA <b>Authentication, Authorization and Accounting setting</b>

**Security Switch**

Security/switch>	Password <password>
	Auth <b>Authentication</b>
	SSH <b>Secure Shell</b>
	HTTPS <b>Hypertext Transfer Protocol over Secure Socket Layer</b>
	RMON <b>Remote Network Monitoring</b>

**Security Switch Authentication**

Security/switch/auth>	Configuration
	Method [console telnet ssh web] [none local radius] [enable disable]

### Security Switch SSH

Security/switch/ssh>	Configuration
	Mode [enable disable]

### Security Switch HTTPS

Security/switch/ssh>	Configuration
	Mode [enable disable]

### Security Switch RMON

Security/switch/rmon>	Statistics Add <stats_id> <data_source>
	Statistics Delete <stats_id>
	Statistics Lookup [<stats_id>]
	History Add <history_id> <data_source> [<interval>] [<buckets>]
	History Delete <history_id>
	History Lookup [<history_id>]
	Alarm Add <alarm_id> <interval> <alarm_variable> [absolute delta]<rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising falling both]
	Alarm Delete <alarm_id>
	Alarm Lookup [<alarm_id>]

### Security Network

Security/Network>	Psec	<b>Port Security Status</b>
	NAS	<b>Network Access Server (IEEE 802.1X)</b>
	ACL	<b>Access Control List</b>
	DHCP	<b>Dynamic Host Configuration Protocol</b>

### Security Network Psec

Security/Network/Psec>	Switch [<port_list>]
	Port [<port_list>]

### Security Network NAS

Security/Network/NAS>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [auto authorized unauthorized macbased]
	Reauthentication [enable disable]
	ReauthPeriod [<reauth_period>]
	EapolTimeout [<eapol_timeout>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]
	Authenticate [<port_list>] [now]
	Statistics [<port_list>] [clear eapol radius]

### Security Network ACL

Security/Network/ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
	Add [<ace_id>] [<ace_id_next>][<(port <port_list>)>] [<(policy <policy> <policy_bitmask>)>][<tagged>] [<vid>] [<tag_prio>] [<dmac_type>][<(etype <etype>)>] [<smac>] [<dmac>])   (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>])   (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>])   icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>])   (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>])   (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>]) [permit deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]

	Clear
	Status
	[combined static loop_protect dhcp ptp ipmc conflicts]
	Port State [<port_list>] [enable disable]

**Security Network DHCP**

Security/Network/DHCP>	Configuration
	Mode [enable disable]
	Server [<ip_addr>]
	Information Mode [enable disable]
	Information Policy [replace keep drop]
	Statistics [clear]

**Security Network AAA**

Security/Network/AAA>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Statistics [<server_index>]

**STP**

STP>	Configuration
	Version [<stp_version>]
	Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable disable]
	bpduGuard [enable disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]

	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Edge [<port_list>] [enable disable]
	Port AutoEdge [<port_list>] [enable disable]
	Port P2P [<port_list>] [enable disable auto]
	Port RestrictedRole [<port_list>] [enable disable]
	Port RestrictedTcn [<port_list>] [enable disable]
	Port bpduGuard [<port_list>] [enable disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

**Aggr**

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac dmac ip port] [enable disable]

**LACP**

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Key [<port_list>] [<key>]
	Role [<port_list>] [active passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]

**LLDP**

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Statistics [<port_list>] [clear]



	Info [<port_list>]
--	--------------------

**QoS**

QoS>	DSCP Map [<dscp_list>] [<class>] [<dpl>]
	DSCP Translation [<dscp_list>] [<trans_dscp>]
	DSCP Trust [<dscp_list>] [enable disable]
	DSCP Classification Mode [<dscp_list>] [enable disable]
	DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
	Storm Unicast [enable disable] [<packet_rate>]
	Storm Multicast [enable disable] [<packet_rate>]
	Storm Broadcast [enable disable] [<packet_rate>]
	QCL Add [<qce_id>] [<qce_id_next>] [<port_list> [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type> [(etype [<etype>])   (LLC [<DSAP>] [<SSAP>] [<control>])   (SNAP [<PID>])   (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment> [<sport>] [<dport>])   (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport> [<dport>])] [<class>] [<dp>] [<classified_dscp>]
	QCL Delete <qce_id>
	QCL Lookup [<qce_id>]
	QCL Status [combined static conflicts]
	QCL Refresh

**Mirror**

Mirror>	Configuration [<port_list>]
---------	-----------------------------

	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

**Dot1x**

Dot1x>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [macbased auto authorized unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear eapol radius]
	Clients [<port_list>] [all <client_cnt>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]

**IGMP**

IGMP>	Configuration [<port_list>]
	Mode [enable disable]
	State [<vid>] [enable disable]
	Querier [<vid>] [enable disable]
	Fastleave [<port_list>] [enable disable]
	Router [<port_list>] [enable disable]
	Flooding [enable disable]
	Groups [<vid>]
	Status [<vid>]

**ACL**

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]

	Add [<ace_id>] [<ace_id_next>] [switch   (port <port>)   (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>])   (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>])   (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>])   (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>])   (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>])   (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>]) [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear

**Mirror**

Mirror>	Configuration [<port_list>]
	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

**Config**

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

**Firmware**

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

**SNMP**

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable disable]
	Trap Security Engine ID [<engineid>]

	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr> [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5 SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]
	Access Delete <index>
Access Lookup [<index>]	

### Firmware

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

### PTP

PTP>	Configuration [<clockinst>]
	PortState <clockinst> [<port_list> [enable disable internal]
	ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>]

	[<vid>] [<prio>]
	ClockDelete <clockinst> [<devtype>]
	DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
	CurrentDS <clockinst>
	ParentDS <clockinst>
	Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
	PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>]
	LocalClock <clockinst> [update show ratio] [<clockratio>]
	Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
	Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
	SlaveTableUnicast <clockinst>
	UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
	ForeignMasters <clockinst> [<port_list>]
	EgressLatency [show clear]
	MasterTableUnicast <clockinst>
	ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>] [<vcxo_enable>]
	OnePpsAction [<one_pps_clear>]
	DebugMode <clockinst> [<debug_mode>]
	Wireless mode <clockinst> [<port_list>] [enable disable]
	Wireless pre notification <clockinst> <port_list>
	Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

**Loop Protect**

Loop Protect>	Configuration
---------------	---------------

	Mode [enable disable]
	Transmit [<transmit-time>]
	Shutdown [<shutdown-time>]
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Action [<port_list>] [shutdown shut_log log]
	Port Transmit [<port_list>] [enable disable]
	Status [<port_list>]

### IPMC

IPMC>	Configuration [igmp]
	Mode [igmp] [enable disable]
	Flooding [igmp] [enable disable]
	VLAN Add [igmp] <vid>
	VLAN Delete [igmp] <vid>
	State [igmp] [<vid>] [enable disable]
	Querier [igmp] [<vid>] [enable disable]
	Fastleave [igmp] [<port_list>] [enable disable]
	Router [igmp] [<port_list>] [enable disable]
	Status [igmp] [<vid>]
	Groups [igmp] [<vid>]
	Version [igmp] [<vid>]

### Fault

Fault>	Alarm PortLinkDown [<port_list>] [enable disable]
	Alarm PowerFailure [pwr1 pwr2 pwr3] [enable disable]

### Event

Event>	Configuration
	Syslog SystemStart [enable disable]
	Syslog PowerStatus [enable disable]
	Syslog SnmpAuthenticationFailure [enable disable]
	Syslog RingTopologyChange [enable disable]
	Syslog Port [<port_list>] [disable linkup linkdown both]

	SMTP SystemStart [enable disable]
	SMTP PowerStatus [enable disable]
	SMTP SnmpAuthenticationFailure [enable disable]
	SMTP RingTopologyChange [enable disable]
	SMTP Port [<port_list>] [disable linkup linkdown both]

### DHCP Server

DHCP Server>	Mode [enable disable]
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

### Ring

Ring>	Mode [enable disable]
	Master [enable disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable disable]
	Couple Port [<port>]
	Dualhoming Mode [enable disable]
	Dualhoming Port [<port>]

### Chain

Chain>	Configuration
	Mode [enable disable]
	1stUplinkPort [<port>]
	2ndUplinkPort [<port>]
	EdgePort [1st 2nd none]

### RCS

RCS>	Mode [enable disable]
	Add [<ip_addr>] [<port_list>] [web_on web_off] [telnet_on telnet_off] [snmp_on snmp_off]
	Del <index>
	Configuration

### FastRecovery

FastRecovery>	Mode [enable disable]
	Port [<port_list>] [<fr_priority>]

### SFP

SFP>	syslog [enable disable]
	temp [<temperature>]
	Info

### DeviceBinding

Devicebinding>	Mode [enable disable]
	Port Mode [<port_list>] [disable scan binding shutdown]
	Port DDOS Mode [<port_list>] [enable disable]
	Port DDOS Sensibility [<port_list>] [low normal medium high]
	Port DDOS Packet [<port_list>] [rx_total rx_unicast rx_multicast rx_broadcast tcp udp]
	Port DDOS Low [<port_list>] [<socket_number>]
	Port DDOS High [<port_list>] [<socket_number>]
	Port DDOS Filter [<port_list>] [source destination]
	Port DDOS Action [<port_list>] [do_nothing block_1_min block_10_mins block shutdown only_log reboot_device]
	Port DDOS Status [<port_list>]
	Port Alive Mode [<port_list>] [enable disable]
	Port Alive Action [<port_list>] [do_nothing link_change shutdown only_log reboot_device]
	Port Alive Status [<port_list>]
	Port Stream Mode [<port_list>] [enable disable]
	Port Stream Action [<port_list>] [do_nothing only_log]
	Port Stream Status [<port_list>]
	Port Addr [<port_list>] [<ip_addr>] [<mac_addr>]



	Port Alias [<port_list>] [<ip_addr>]
	Port DeviceType [<port_list>] [unknown ip_cam ip_phone ap pc plc nvr]
	Port Location [<port_list>] [<device_location>]
	Port Description [<port_list>] [<device_description>]

**MRP**

MRP>	Configuration
	Mode [enable disable]
	Manager [enable disable]
	React [enable disable]
	1stRingPort [<mrp_port>]
	2ndRingPort [<mrp_port>]
	Parameter MRP_TOPchgT [<value>]
	Parameter MRP_TOPNRmax [<value>]
	Parameter MRP_TSTshortT [<value>]
	Parameter MRP_TSTdefaultT [<value>]
	Parameter MRP_TSTNRmax [<value>]
	Parameter MRP_LNKdownT [<value>]
	Parameter MRP_LNKupT [<value>]
Parameter MRP_LNKNRmax [<value>]	

**Modbus**

Modbus>	Status
	Mode [enable disable]

# Technical Specifications

ORing Switch Model	RGS-PR9000-A-LV	RGS-PR9000-A-HV
<b>Physical Ports</b>		
Slot Number	<b>3</b>	
10G Base-X with SFP+ port	<b>4(optional)</b>	
<b>Technology</b>		
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.z for 1000Base-X IEEE 802.3ae for 10Gigabit Ethernet IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol ) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)	
CPU	Core clock 800MHz	
SDRAM Size	DDR2 256MBytes	
Flash ROM Size	128MBytes NAND Flash	
MAC Table	16k	
Priority Queues	8	
Processing	Store-and-Forward	
Switch Properties	Switching latency: 7 us Switching bandwidth: 128Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define	
Jumbo frame	Up to 10K Bytes	
Security Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) Single 802.1x and Multiple 802.1x MAC-based authentication QoS assignment MAC address limit TACACS+ VLAN (802.1Q ) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH / SSL enhance network security Web and CLI authentication and authorization IP source guard	
Software Features	IPv4 routing protocols – RIP v1/v2, OSPF v2 IPv6 routing protocols – RIP v6, OSPF v3 VRRP for router redundancy IEEE 802.1D Bridge, auto MAC address learning/aging and MAC address (static) MMRP and MVRP MSTP/RSTP/STP Ethernet redundancy Redundant Ring (O-Ring) with recovery time less than 30ms over 250 units TCP/IP stack for IPv4 and IPv6 (including ARP, ICMP, ND, UDP) GARP, GMRP and GVRP TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic Private VLANs PVRST+ (Per VLAN Rapid Spanning Tree Protocol - enhanced) Q-in-Q VLAN tunneling and provider bridging	

	IGMP snooping/filtering/Proxy RADIUS client for IPv4 and IPv6 SNMP v1/v2c/v3 agent and MIB support IGMP v2/v3 Snooping IP-based bandwidth management Application-based QoS management Port configuration, status, statistics, monitoring, security DHCP Server/Client/Relay for IPv4 Modbus TCP SMTP Client NTP Server TFTP	
Network Redundancy	O-Ring O-Chain MSTP/RSTP/STP	
RS-232 Serial Console Port	RS-232 in RJ-45 connector with console cable. 115200bps, 8, N, 1, and support backup unit	
<b>LED Indicators</b>		
System Ready Indicator (PWR)	Green: Indicates that the system ready. The LED is blinking when the system is upgrading firmware	
Power Indicator (PWR1 / PWR2)	Green: Power LED x 2	
Ring Master Indicator (R.M.)	Green: Indicates that the system is operating in O-Ring Master mode	
O-Ring Indicator (Ring)	Green : Indicates that the system operating in O-Ring mode Green Blinking: Indicates that the Ring is broken.	
Fault Indicator (Fault)	Amber: Indicate unexpected event occurred	
Reset To Default Running Indicator (DEF)	Green: System resets to default configuration	
Supervisor Login Indicator (RMT)	Green: System is accessed remotely	
Smart LED Display system	Link (LINK) / Speed (SPD) / Duplex (FDX) / Remote (RMT) green LED indicator x 4 Mode select Button (MODE) : Link (LINK) / Speed (SPD) / Duplex (FDX) / Remote (RMT) mode select button Port 1 ~ 28 Link LED show : Green x 28	
<b>Fault Contact</b>		
Relay	Relay output to carry capacity of 1A at 24VDC	
<b>Power</b>		
Redundant power input modular	Dual 48VDC (36~72VDC) power inputs at terminal block	Dual 100~240VAC / 100~370VDC power inputs at terminal block
Power consumption (Typ.)	46watts	43.5watts
Overload current protection	Present	
<b>Physical Characteristic</b>		
Enclosure	19 inches rack mountable	
Weight (g) without modules	5,250g	5,400g
Dimension (W x D x H)	440(W) x 325(D) x 44(H) mm (17.32x12.8x1.73 inches)	
<b>MTBF(mean time between failures)</b>		
Time	130,66hrs	
<b>Environmental</b>		
Storage Temperature	-40 to 85°C	
Operating Temperature	-20 to 60°C (with 10G) -40 to 75 °C (without 10G)	
Operating Humidity	5% to 95% Non-condensing	
<b>Regulatory Approvals</b>		
Power Automation	IEC 61850-3, IEEE 1613 (pending)	
EMI	FCC Part 15, CISPR (EN55022) class A	
Railway	EN50121-4(EN50121-1)	
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11	
Shock	IEC60068-2-27	

Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
<b>Warranty</b>	5 years