

Interface Masters

◀ TECHNOLOGIES ▶

Innovative Network Solutions

Niagara 2932-4XL

Web User Manual

INTERFACE MASTERS: ISSWebum_Base/20090930

Revision Number: 27.0

Interface Masters

◀ TECHNOLOGIES ▶
Innovative Network Solutions

Copyright © 2010 Interface Masters Inc. All Rights Reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of Interface Masters.

Printed in _____

TRADEMARKS INTERFACE MASTERS and THE INTERFACE MASTERS LOGO are trademarks of Interface Masters Inc. in the U.S. and other countries. The use of any of these trademarks without Interface Masters prior written consent is strictly prohibited. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Interface Masters Inc. disclaims any proprietary interest in the trademarks and trade names other than its own.

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Interface Masters. Information in this document is subject to change without notice.

REQUESTS For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Interface Masters on www.InterfaceMasters.com

DOCUMENT No.: INTERFACE MASTERS: ISSWebum_Base/20090930

Contents

CHAPTER 1:	INTRODUCTION	13
	1.1 PURPOSE	13
	1.2 SCOPE	13
	1.3 DEFINITIONS AND ACRONYMS	13
	1.4 WEB INTERFACE CONVENTIONS	15
CHAPTER 2:	WEB INTERFACE OVERVIEW	16
	2.1 LOGIN PAGE	17
	2.2 HOME PAGE	17
	2.2.1 System Acknowledgement	18
CHAPTER 3:	SYSTEM	21
	3.1 SYSTEM INFORMATION	22
	3.2 SYSTEM RESOURCES	23
	3.3 NVRAM SETTINGS	25
	3.4 IP AUTHORIZED MANAGER	27
	3.5 SAVE AND RESTORE	29
	3.5.1 Save	29
	3.5.2 Restore	31
	3.5.3 Erase	32
	3.5.4 Remote Restore	33
	3.6 LOG TRANSFER	33
	3.7 IMAGE DOWNLOAD	35
	3.8 FILE TRANSFER	36
	3.8.1 File Upload	36
	3.8.2 File Download	37
	3.9 TACACS	38
	3.9.1 Tacacs Settings	38
	3.9.2 Tacacs AS	40
	3.10 ENTITY MIB	41
	3.10.1 Physical Entity Details	41
	3.10.2 Logical Entity Details	44
	3.10.3 LP Mapping Details	46
	3.10.4 Alias Mapping Details	47
	3.10.5 Contains Mapping Details	48
	3.11 SNMP	49
	3.11.1 SNMP Scalars	49
	3.11.2 SNMP Unicast	51
	3.11.3 SNMP Broadcast	53
	3.11.4 SNMP Multicast	54
	3.12 SNMP	55
	3.12.1 AGENT	56
	3.12.1.1 Community	56
	3.12.1.2 Group	57
	3.12.1.3 Group Access	58
	3.12.1.4 View	60
	3.12.1.5 Target Address	61
	3.12.1.6 TargetParameter	62
	3.12.1.7 User	64
	3.12.1.8 Trap Manager	65
	3.12.2 AGENTX	66
	3.13 SYSLOG	67

3.13.1	BSD Syslog.....	68
3.13.1.1	SYSLOG ScalarsConf-----	68
3.13.1.2	SYSLOG FileTable-----	70
3.13.1.3	SYSLOG MailTable-----	71
3.13.1.4	SYSLOG FwdTable-----	72
CHAPTER 4:	LAYER2 MANAGEMENT _____	73
4.1	PORT MANAGER.....	74
4.1.1	Basic Settings.....	74
4.1.2	Port Monitoring.....	76
4.1.3	Traffic Class.....	77
4.1.4	Port Control.....	78
4.1.5	Rate Limiting.....	79
4.2	VLAN.....	80
4.2.1	Basic Settings.....	81
4.2.2	Port Settings.....	82
4.2.3	StaticVLANs.....	84
4.2.4	ProtocolGroup.....	85
4.2.5	PortProtocol.....	86
4.2.6	PortMacMAP.....	87
4.2.7	UnicastMac.....	88
4.2.8	Wildcard.....	89
4.2.9	Switchportfiltering.....	90
4.3	VLAN SUBNET.....	91
4.4	DYNAMIC VLAN.....	92
4.4.1	DynamicVlan.....	92
4.4.2	Port Settings.....	93
4.4.3	GarpTimers.....	95
4.5	MSTP.....	96
4.5.1	Basic Settings.....	97
4.5.2	Timers.....	98
4.5.3	Port Configuration.....	99
4.5.4	VLAN Mapping.....	101
4.5.5	Port Settings.....	102
4.5.6	CIST Port Status.....	103
4.6	RSTP.....	105
4.6.1	Global Settings.....	105
4.6.2	Basic Settings.....	106
4.6.3	Port Settings.....	107
4.6.4	Port Status.....	109
4.7	LA.....	110
4.7.1	Basic Settings.....	111
4.7.2	Interface Settings.....	111
4.7.3	PortChannelSettings.....	112
4.7.4	Port Settings.....	114
4.7.5	Port StateInfo.....	116
4.7.6	Load Balancing.....	117
4.8	802.1X.....	118
4.8.1	Basic Settings.....	118
4.8.2	Port Settings.....	119
4.8.3	Timers.....	121
4.8.4	Local AS.....	123
4.8.5	Radius Settings.....	124
4.8.6	MacSession Info.....	125
4.9	FILTERS.....	126
4.9.1	Unicast Filters.....	126

	4.9.2 Multicast Filters	127
	4.9.3 Multicast Forwarding.....	128
CHAPTER 5:	LAYER-3 MANAGEMENT	131
	5.1 IP	132
	5.1.1 Vlan Interface.....	132
	5.1.2 IPv4 AddrConf	133
	5.1.3 IP route	134
	5.1.4 LoopBack Settings.....	135
	5.2 DHCP SERVER	136
	5.2.1 Basic Settings	136
	5.2.2 Pool Settings.....	137
	5.3 DHCP RELAY.....	139
	5.3.1 Basic Settings	139
	5.3.2 Interface Conf	140
CHAPTER 6:	MULTICAST	143
	6.1 IGMP SNOOPING	144
	6.1.1 Basic Settings	144
	6.1.2 Timer.....	146
	6.1.3 VlanConfiguration	148
	6.1.4 InterfaceConfiguration	149
	6.1.5 RouterPortConf.....	151
	6.1.6 RouterPorts.....	152
	6.1.7 FwdInformation	153
	6.1.8 McastReceiverInfo	153
	6.2 DYNAMIC MULTICAST.....	154
	6.2.1 DynamicMulticast.....	155
	6.2.2 Port Settings	155
	6.3 TAC	157
	6.3.1 Profile.....	157
	6.3.2 Profile filters	158
CHAPTER 7:	ETHERNET OAM	161
	7.1 BASIC SETTINGS.....	161
	7.2 PORT SETTINGS	162
	7.3 LINKEVENT SETTINGS.....	165
	7.4 LOOPBACK SETTINGS	167
CHAPTER 8:	RMON	171
	8.1 BASIC SETTINGS.....	171
	8.2 ALARMS	172
	8.3 ETHERNET STATISTICS	174
	8.4 EVENTS.....	175
	8.5 HISTORY	176
CHAPTER 9:	RMONV2	179
CHAPTER 10:	DSMON	181
CHAPTER 11:	STATISTICS	183

Figures

Figure 2-1: Login Page	17
Figure 2-2: Home Page	18
Figure 2-3: System Acknowledgement Page	19
Figure 3-1: System Information Page - System Group	22
Figure 3-2: System Resources Page – System Group	24
Figure 3-3: Factory Default Settings - System Group	26
Figure 3-4: IP Authorized Manager - System Group	28
Figure 3-5: Save configuration - System Group	30
Figure 3-6: Restore Configuration - System Group	31
Figure 3-7: Erase Configuration - System Group	32
Figure 3-8: Remote Restore - System Group	33
Figure 3-9: Log Transfer Settings – System Group	34
Figure 3-10: Software Upgrade – System Group	35
Figure 3-11: File Upload – System Group	36
Figure 3-12: File Download – System Group	38
Figure 3-13: TACACS Server Configuration - System Group	39
Figure 3-14: TACACS Active Server Configuration - System Group	40
Figure 3-15: Physical Table Entries - System Group	42
Figure 3-16: Logical Table Entries - System Group	45
Figure 3-17: LP Mapping Table Entries - System Group	47
Figure 3-18: Alias Mapping Table Entries - System Group	48
Figure 3-19: Physical Contains Table - System Group	49
Figure 3-20: SNMP Scalars Configuration - System Group	50
Figure 3-21: SNMP Unicast Table - System Group	52
Figure 3-22: SNMP Broadcast Configuration - System Group	53
Figure 3-23: SNMP Multicast Configuration - System Group	54
Figure 3-24: SNMP Agent Control Settings – System Group	55
Figure 3-25: SNMP Community Settings - System Group	57
Figure 3-26: SNMP GROUP Settings - System Group	58
Figure 3-27: SNMP Group Access Settings - System Group	59
Figure 3-28: SNMP View Tree Settings - System Group	60
Figure 3-29: SNMP Target Address Settings - System Group	61
Figure 3-30: SNMP Target Param Settings - System Group	63
Figure 3-31: SNMP Security Settings - System Group	64
Figure 3-32: SNMP Trap Settings - System Group	66
Figure 3-33: SNMP Agentx Subagent Settings – System Group	67
Figure 3-34: SYSLOG Settings – System Group	68
Figure 3-35: BSD Syslog Settings – System Group	69
Figure 3-36: BSD Syslog File Table – System Group	70
Figure 3-37: BSD Syslog MailTable – System Group	71
Figure 3-38: Syslog FwdTable – System Group	72
Figure 4-1: Layer2 Management Page	74
Figure 4-2: Port Basic Settings - Layer 2 Group	75
Figure 4-3: Port Monitoring - Layer 2 Group	76
Figure 4-4: VLAN Traffic Class Mapping - Layer 2 Group	77
Figure 4-5: Port Control - Layer 2 Group	78
Figure 4-6: Rate Limiting –Layer 2 Group	80
Figure 4-7: VLAN Basic Settings - Layer 2 Group	81
Figure 4-8: VLAN Port Settings - Layer 2 Group	83
Figure 4-9: Static VLAN Configuration - Layer 2 Group	84
Figure 4-10: VLAN Protocol Group Settings - Layer 2 Group	85

Figure 4-11: Port VLAN Protocol Settings - Layer 2 Group.....	86
Figure 4-12: VLAN Port MAC Map – Layer 2 Group	87
Figure 4-13: VLAN Unicast MAC Settings – Layer 2 Group.....	88
Figure 4-14: Wildcard Settings – Layer 2 Group	90
Figure 4-15: SwitchPort VLAN Filtering – Layer 2 Group.....	91
Figure 4-16: VLAN Subnet Port-Map – Layer 2 Group	92
Figure 4-17: Dynamic VLAN Global Configuration – Layer 2 Group.....	93
Figure 4-18: Dynamic VLAN Port Configuration – Layer 2 Group	94
Figure 4-19: Garp Timers Configuration– Layer 2 Group.....	96
Figure 4-20: MSTP Basic Settings – Layer 2 Group	97
Figure 4-21: MSTP Timers Configuration – Layer 2 Group.....	99
Figure 4-22: CIST Settings - Layer 2 Group.....	100
Figure 4-23: VLAN Mapping - Layer 2 Group.....	102
Figure 4-24: Port Settings - Layer 2 Group	103
Figure 4-25: MSTP CIST Port Status - Layer 2 Group-2.....	104
Figure 4-26: RSTP Basic Settings – Layer 2 Group.....	105
Figure 4-27: RSTP Configuration – Layer 2 Group	106
Figure 4-28: RSTP Port Status Configuration - Layer 2 Group.....	108
Figure 4-29: RSTP Port Status – Layer 2 Group.....	110
Figure 4-30: LA Basic Settings – Layer 2 Group.....	111
Figure 4-31: LA Port Channel Interface Basic Settings – Layer 2 Group.....	112
Figure 4-32: LA Port Channel Settings – Layer 2 Group.....	113
Figure 4-33: LA Port Settings – Layer 2 Group	115
Figure 4-34: LA Port StateMachine Information – Layer 2 Group.....	116
Figure 4-35: LA Load Balancing Policy - Layer 2 Group	117
Figure 4-36: 802.1x Basic Settings - Layer 2 Group	118
Figure 4-37: 802.1x Port Settings - Layer 2 Group	119
Figure 4-38: 802.1x Timer Configuration - Layer 2 Group	122
Figure 4-39: Local Authentication Server Configuration - Layer 2 Group	123
Figure 4-40: Radius Server Configuration - Layer 2 Group	124
Figure 4-41: Mac Session Info - Layer 2 Group	125
Figure 4-42: L2 Unicast Filter Configuration - Layer 2 Group	126
Figure 4-43: L2 Multicast Filter Configuration - Layer 2 Group.....	127
Figure 4-44: Forward Ports Configuration - Layer 2 Group.....	128
Figure 5-1: Layer 3 Management Page.....	131
Figure 5-2: VLAN Interface Basic Settings - - Layer 3 Group	132
Figure 5-3: IPv4 Interface Settings- Layer 3 Group.....	133
Figure 5-4: IP Route Configuration - Layer 3 Group	134
Figure 5-5: LoopBack Basic Settings - Layer 3 Group	135
Figure 5-6: DHCP Basic Settings - Layer 3 Group	137
Figure 5-7: DHCP Pool Settings - Layer 3 Group	138
Figure 5-8: DHCP Relay Configuration - Layer 3 Group.....	139
Figure 5-9: DHCP Relay Interface Configuration - Layer 3 Group.....	140
Figure 6-1: Multicast Management - Layer 3 Group.....	143
Figure 6-2: IGMP Snooping Configuration - Multicast Group.....	144
Figure 6-3: IGS Timer Settings - Multicast Group	147
Figure 6-4: IGS Snooping Vlan Configuration - Multicast Group	148
Figure 6-5: IGS Snooping Interface Configuration - Multicast Group.....	150
Figure 6-6: IGS Vlan Router Port Configuration - Multicast Group	151
Figure 6-7: IGMP Snooping VLAN Router Ports - Multicast Group	152
Figure 6-8: MAC Based Multicast Forwarding Table - Multicast Group.....	153
Figure 6-9: Multicast Receiver Table - Multicast Group	154
Figure 6-10: Dynamic Multicast Global Configuration	155
Figure 6-11: Dynamic Multicast Port Configuration.....	156
Figure 6-12: TAC Profile Configuration – Multicast Group.....	157
Figure 6-13: TAC Profile Filter Configuration – Multicast Group.....	158

Figure 7-1: Ethernet OAM Basic Settings – EOAM Group.....	162
Figure 7-2: Ethernet OAM Port Settings – EOAM Group.....	163
Figure 7-3: Ethernet OAM Link Event Settings – EOAM Group.....	165
Figure 7-4: Ethernet OAM Loopback Settings – EOAM Group.....	168
Figure 8-1: RMON Basic Settings - RMON Group	172
Figure 8-2: RMON Alarm Configuration - RMON Group.....	173
Figure 8-3: Ethernet Statistics Configuration - RMON Group	174
Figure 8-4: Event Configuration - RMON Group	175
Figure 8-5: History Control Configuration - RMON Group.....	177
Figure 9-1: RMONv2 Basic Settings – RMONv2 Group.....	179
Figure 10-1: DSMON Basic Settings – DSMON Group	181
Figure 11-1: Statistics - Statistics Group	183
Figure 11-2: Interface Statistics - Statistics Group	186
Figure 11-3: TCP Statistics - Statistics Group.....	187
Figure 11-4: UDP Current Connection – Statistics Group.....	187
Figure 11-5: UDP Statistics - Statistics Group	188
Figure 11-6: IGMP Snooping Clear Statistics – Statistics Group	188

Tables

Table 1-1: Acronyms Used in this Document	13
Table 3-1: System Information	22
Table 3-2: System Resources	24
Table 3-3: Factory Default Settings	26
Table 3-4: IP Authorized Manager	28
Table 3-5: Save configuration	30
Table 3-6: Restore Configuration	31
Table 3-7: Erase Configuration	32
Table 3-8: Log Transfer Settings	34
Table 3-9: Software Upgrade	35
Table 3-10: File Upload	36
Table 3-11: File Download	38
Table 3-12: Configuring TACACS Server	39
Table 3-13: Configuring TACACS Active Server	40
Table 3-14: Configuring Physical Table	42
Table 3-15: Configuring Logical Table	45
Table 3-16: SNMP Scalars Configuration	50
Table 3-17: SNMP Unicast Table	52
Table 3-18: SNMP Broadcast Configuration	53
Table 3-19: SNMP Multicast Configuration	54
Table 3-20: Community Settings	57
Table 3-21: Group Settings	58
Table 3-22: SNMP Group Access Settings	59
Table 3-23: SNMP View Tree Settings	60
Table 3-24: SNMP Target Address Settings	62
Table 3-25: SNMP Target Param Settings	63
Table 3-26: SNMP Security Settings	64
Table 3-27: SNMP Trap Settings	66
Table 3-28: SNMP Agentx Subagent Settings	67
Table 3-29: BSD Syslog Settings	69
Table 3-30: BSD Syslog File Table	70
Table 3-31: BSD Syslog MailTable	71
Table 3-32: Syslog FwdTable	72
Table 4-1: Port Basic Settings	75
Table 4-2: Port Monitoring	76
Table 4-3: VLAN Traffic Class Mapping	78
Table 4-4: Port Control	78
Table 4-5: Rate Limiting	80
Table 4-6: VLAN Basic Settings	81
Table 4-7: VLAN Port Settings	83
Table 4-8: Static VLAN Configuration	84
Table 4-9: VLAN Protocol Group Settings	85
Table 4-10: Port VLAN Protocol Settings	87
Table 4-11: VLAN Port MAC Map	88
Table 4-12: VLAN Unicast MAC Settings	88
Table 4-13: Wildcard Settings	90
Table 4-14: SwitchPort VLAN Filtering	91
Table 4-15: VLAN Subnet Port-Map	92
Table 4-16: Dynamic VLAN Global Configuration	93
Table 4-17: Dynamic VLAN Port Configuration	94
Table 4-18: Garp Timers Configuration	96

Table 4-19: MSTP Basic Settings.....	97
Table 4-20: MSTP Timers Configuration	99
Table 4-21: CIST Settings	100
Table 4-22: VLAN Mapping	102
Table 4-23: Port Settings.....	103
Table 4-24: Port Settings.....	104
Table 4-25: RSTP Basic Settings	106
Table 4-26: RSTP Configuration	107
Table 4-27: RSTP Port Status Configuration	108
Table 4-28: RSTP Port Status	110
Table 4-29: LA Basic Settings	111
Table 4-30: LA Port Channel Interface Basic Settings	112
Table 4-31: LA Port Channel Settings	113
Table 4-32: LA Port Settings	115
Table 4-33: LA Port StateMachine Information	116
Table 4-34: 802.1x Basic Settings.....	118
Table 4-35: 802.1x Port Settings	120
Table 4-36: 802.1x Timer Configuration	122
Table 4-37: Local Authentication Server Configuration.....	123
Table 4-38: Radius Server Configuration	124
Table 4-39: Mac Session Info.....	126
Table 4-40: L2 Unicast Filter Configuration	127
Table 4-41: L2 Multicast Filter Configuration.....	128
Table 4-42: Forward Ports Configuration	129
Table 5-1: VLAN Interface Basic Settings	132
Table 5-2: IPv4 Interface Settings	134
Table 5-3: IP Route Configuration	135
Table 5-4: LoopBack Basic Settings.....	136
Table 5-5: DHCP Basic Settings	137
Table 5-6: DHCP Pool Settings	138
Table 5-7: DHCP Relay Configuration.....	139
Table 5-8: DHCP Relay Interface Configuration	140
Table 6-1: Enabling IGS	145
Table 6-2: IGS Basic Settings	145
Table 6-3: IGS Timer Settings	147
Table 6-4: IGMP Snooping Vlan Configuration	148
Table 6-5: IGMP Snooping Interface Configuration	150
Table 6-6: IGMP Snooping Vlan Router Port Configuration.....	151
Table 6-7: IGMP Snooping Router Ports.....	152
Table 6-8: Displaying Group Information – MAC Based Multicast Forwarding Table	153
Table 6-9: IGMP Snooping Multicast Receiver Table	154
Table 6-10: Configuring Dynamic Multicast Global	155
Table 6-11: Configuring Dynamic Multicast Port	156
Table 6-12: Configuring TAC Profile.....	157
Table 6-13: TAC Profile Filters	158
Table 7-1: Ethernet OAM Basic Settings.....	162
Table 7-2: Ethernet OAM Port Settings.....	163
Table 7-3: Ethernet OAM Link Event Settings.....	165
Table 7-4: Ethernet OAM Loopback Settings.....	168
Table 8-1: RMON Basic Settings.....	172
Table 8-2: RMON Alarm Configuration.....	173
Table 8-3: RMON Ethernet Statistics	174
Table 8-4: RMON Event Configuration.....	175
Table 8-5: RMON History Control Configuration	177
Table 9-1: RMONv2 Basic Settings.....	179
Table 10-1: DSMON Basic Settings	181

Chapter 1

Introduction

This chapter states the purpose and scope of this document. It also details on the acronyms used in this document, the Web conventions followed for Web pages and the available packages.

1.1 Purpose

This document is designed to provide **ISS** (Intelligent Switch Solution) enterprise users with the information required to configure the switch through the Web. The Web pages have been presented as screenshots in this document to make the information more accessible.

1.2 Scope

This document explains in detail all Web pages and fields of the enterprise package. It does not include the details of the HTTP (Hyper Text Transfer Protocol) server architecture, backend processing of Web pages or the protocol details.

1.3 Definitions and Acronyms

Table 1-1: Acronyms Used in this Document

Acronym	Explanation
ACL	Access Control List
AS	Autonomous System
BPDU	Bridge Protocol Data Unit

Acronym	Explanation
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DLF	Destination Lookup Failure
DSCP	Differentiated Services Code Point
DSMON	Differentiated Services Monitoring
DST	Daylight Saving Time
FDB	Forwarding Database
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HOL	Head Of Line
HTTP	Hyper Text Transfer Protocol
ID	Identifier
IGMP	Internet Group Management Protocol
IGS	IGMP Snooping
IP	Internet Protocol
ISS	Intelligent Switch Solution
L2-VPN	Layer 2 Virtual Private Network
LA	Link Aggregation
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LDP	Label Distribution Protocol
MAC	Media Access Control
MIB	Management Information Base
MLDS	Multicast Listener Discovery Snooping
MP	Message Processing
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management System
NVRAM	Non Volatile Random Access Memory
PB	Provider Bridge
PIM	Protocol Independent Multicasting
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RARP	Reverse Address Resolution Protocol
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	SSH File Transfer Protocol

Acronym	Explanation
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
VLAN	Virtual LAN

1.4 Web Interface Conventions

- In Web pages involving tables, the values to be configured are represented as blank cells or with a drop-down menu to select the required value.
- A field entry with a * symbol displayed in a Web page, denotes that it is a mandatory field.
- For the read/write values in the table, there is provision to select a particular entry and modify the same.
- The LEDs displayed on the top of the pages denote the ports. A green light indicates that the port is up and a red light indicates that the port is down.
- In few pages,  indicates output areas specific to the configuration.

Chapter

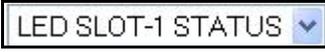
2

Web Interface Overview

The web interface can be configured through Web browsers such as the Internet Explorer or Netscape Navigator¹. The web interface starts with a default IP address, which is also the management IP address. This IP address is essentially provided for remote management of the switch. For managing the switch through Web browsers, enter the default IP address to start accessing the switch. For example, if the management IP address of the switch is 192.168.1.1, the switch can be accessed through the Web browser by entering **http://192.168.1.1** in the address space of the Web browser.



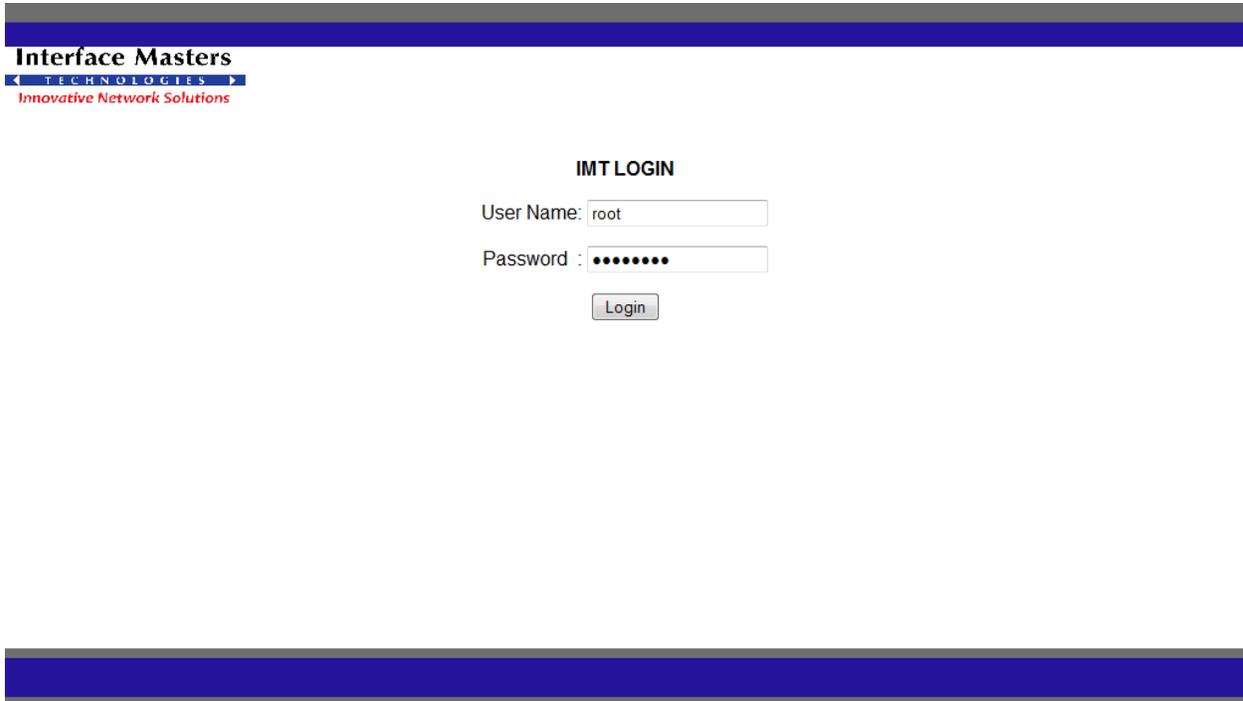
Notes

- Web User Interface facilitates new and inexperienced users to create the basic routing and security functions, quickly and effectively. Advanced configuration options can be set only through the CLI.
- The drop down list  specifying the selected LED slot is displayed in all the Web pages, when stacking is enabled (that is, RMGR is set as YES). The stacking feature is applicable only for the Enterprise package executed in BCM. The screenshots in this document are not updated for this change.
- The screenshots in this document have been updated only for the newly added and the updated Web pages. Hence, the existing screens will not match the left pane view of the User interface.

¹ The settings for the screenshots depicted in the document are configured using Internet Explorer. These screenshots are taken in Windows.

2.1 Login Page

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



The screenshot shows the login page for Interface Masters. At the top left, there is a logo for Interface Masters Technologies with the tagline 'Innovative Network Solutions'. The main heading is 'IMT LOGIN'. Below this, there are two input fields: 'User Name:' with the text 'root' entered, and 'Password:' with a masked password represented by seven dots. A 'Login' button is positioned below the password field.

Figure 2-1: Login Page

Enter the **User Name** and **Password** and click **Login**.

This **User Name** and **Password** are used for accessing the Switch through the Web for switch configuration. The user name and password entered are validated at the switch end.

2.2 Home Page

Successful validation of the user name and password displays the Home page. This page presents a brief overview of the solution.

The **Home** page also includes the following links to Management pages, which have been categorized based on the protocol feature and functionality:

- System
- Layer2 Management
- Layer-3 Management
- Multicast
- Ethernet OAM
- RMON

- RMONv2
- DSMON
- Statistics

You can click the following links that are displayed in top of the Web pages:

- **Support:** To get high-quality and responsive technical support.
- **Help:** To open the help page.
- **About:** To get additional information about Web management.
- **Log Out:** To Log out the Web session through which the user is connected.

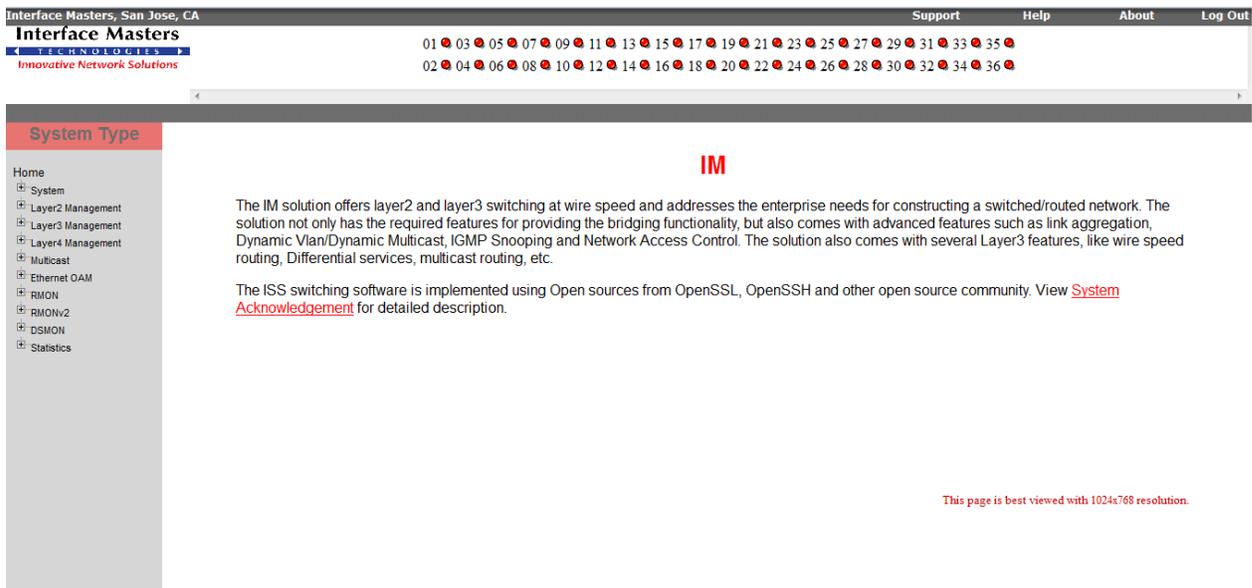


Figure 2-2: Home Page

2.2.1 System Acknowledgement

The **System Acknowledgement** link in the home page displays the acknowledgement information for the various software used in the solution.

Click **System Acknowledgement** link to open the acknowledgement page.

Interface Masters, San Jose, CA

Support Help About Log Out

Interface Masters
TECHNOLOGIES
Innovative Network Solutions

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

System Type

ISS

The SSH functionality in this switch is implemented using the open source software from <http://www.openssh.org> developed by Theo de Raadt, Niels Provos, Markus Friedl, Bob Beck, Aaron Campbell and Dug Song. All copyrights listed at <http://www.openssh.org> apply.

The SSL functionality in this switch is implemented using the open source software from <http://www.openssl.org> which include software written by Er.c A. Young and Tim J. Hudson. All copyrights listed at <http://www.openssl.org> apply.

This switch includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim J. Hudson (tjh@cryptsoft.com). PLEASE REMEMBER THAT EXPORT/IMPORT AND/OR USE OF STRONG CRYPTOGRAPHY SOFTWARE, PROVIDING CRYPTOGRAPHY HOOKS OR EVEN JUST COMMUNICATING TECHNICAL DETAILS ABOUT CRYPTOGRAPHY SOFTWARE IS ILLEGAL IN SOME PARTS OF THE WORLD. SO, WHEN YOU IMPORT THIS PACKAGE TO YOUR COUNTRY, RE-DISTRIBUTE IT FROM THERE OR EVEN JUST EMAIL TECHNICAL SUGGESTIONS OR EVEN SOURCE PATCHES TO THE AUTHOR OR OTHER PEOPLE YOU ARE STRONGLY ADVISED TO PAY CLOSE ATTENTION TO ANY EXPORT/IMPORT AND/OR USE LAWS WHICH APPLY TO YOU. THE AUTHORS OF OPENSSL ARE NOT LIABLE FOR ANY VIOLATIONS YOU MAKE HERE. SO BE CAREFUL, IT IS YOUR RESPONSIBILITY

[Back to Home page.](#)

This page is best viewed with 1024x768 resolution.

http://192.168.1.227/iss/system_acknowledqe.html?Gambit=cdkdcdddtdkdkchppqgqehkdbqeqnjqogbdctddd

Figure 2-3: System Acknowledgement Page

Chapter

3

System

This chapter describes the configuration of the various system related features.

The **System** link on the left pane provides access to the following links:

- System Information
- System Resources
- ACL²
- QoSIngress²
- QoSEgress²
- IP Authorized Manager
- Save and Restore
- Log Transfer
- Image Download
- File Transfer
- TACACS
- Entity MIB
- SNMP
- SNMP
- SYSLOG

By default, the **System Information** page is loaded.

²The configuration parameters provided in the link are described in ISSBCMWebum document.

3.1 System Information

The **System Information** page allows you to configure the system information.

To configure system information

1. Select **System > System Information** to open **System Information** page.

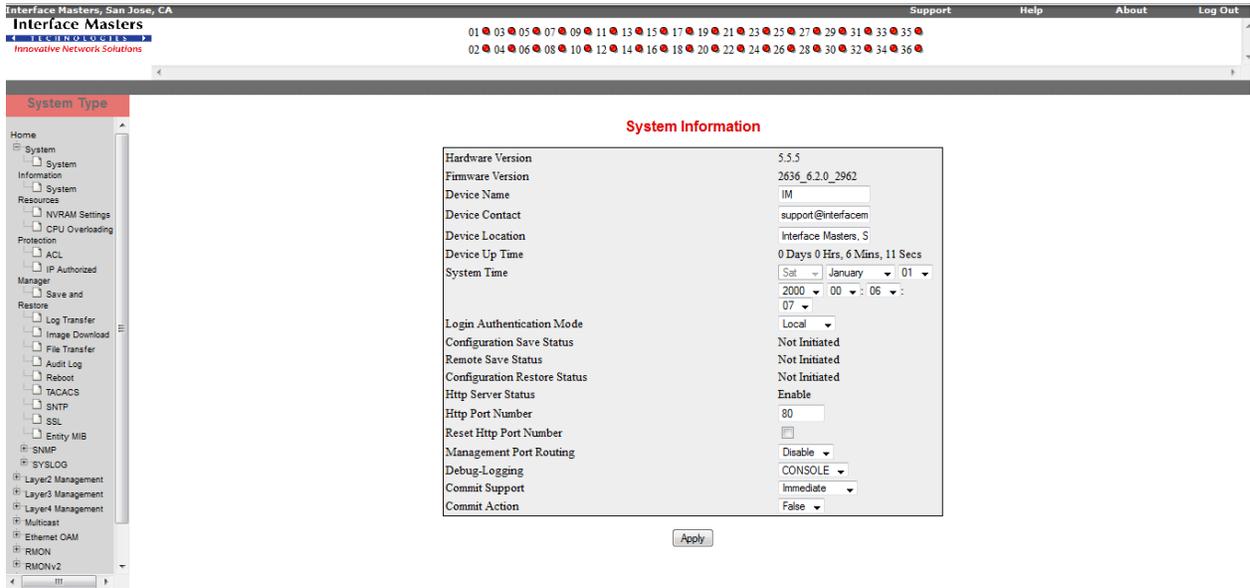


Figure 3-1: System Information Page - System Group

2. Configure the parameters described in Table 3-1.

Table 3-1: System Information

Field Name	Description
Hardware Version	Specifies the hardware version number.
Firmware Version	Specifies the firmware version number.
Software Version	Specifies the version of the software as mentioned in the cswcfg.txt file.
Device Name	Specifies the name of the device. Default device name is IM.
Device Contact	Specifies the textual identification of the contact person for this managed node, along with the information on how to contact the person. If the contact information is not available, this value takes a zero-length string.
Device Location	Specifies the physical location of this node. If the location is unknown, this value takes a zero-length string.
Device Up Time	Displays the time from which device is up.
Login Authentication Mode	Specifies the login authentication mode. Options are: <ul style="list-style-type: none"> • Local – Authentication is done locally. • Remote – Authentication is done in the remote side through a RADIUS Server.

Field Name	Description
	<ul style="list-style-type: none"> Tacacs - Authentication is done through a TACACS+ server.
Configuration Save Status	Specifies the configuration save status.
Remote Save Status	Specifies the remote save status.
Configuration Restore Status	Specifies the configuration restoration status.
Http Server Status	Specifies the HTTP server status in the system. Options are: <ul style="list-style-type: none"> Enable Disable
Http Port Number	<p>Specifies the port to be used by the host to configure the router using the Web interface.</p> <p>This value ranges between 0 and 65535. Default value is 80.</p> <p><input type="checkbox"/> The HTTP server must be disabled, before configuring the port number.</p>

- Click **Apply** for the configuration to take effect.

3.2 System Resources

The System Resources link contains the following pages

System Resources

Fan Details

By default, the **System Resources** page is loaded

The **System Resources** page allows you to periodically diagnose the following:

- RAM usage
- CPU usage
- Flash usage
- Temperature threshold and
- Power Supply threshold

The corresponding NPAPIs or System calls are used to configure the System diagnostics that determine the current state of the system resources. These NPAPIs are ported for a specific target platform/system. Diagnostics are repeated every 10 seconds. This time can be increased or decreased based on the requirement.

To configure System Resources

- Select **System > System Resources** to open **System Resources** page.

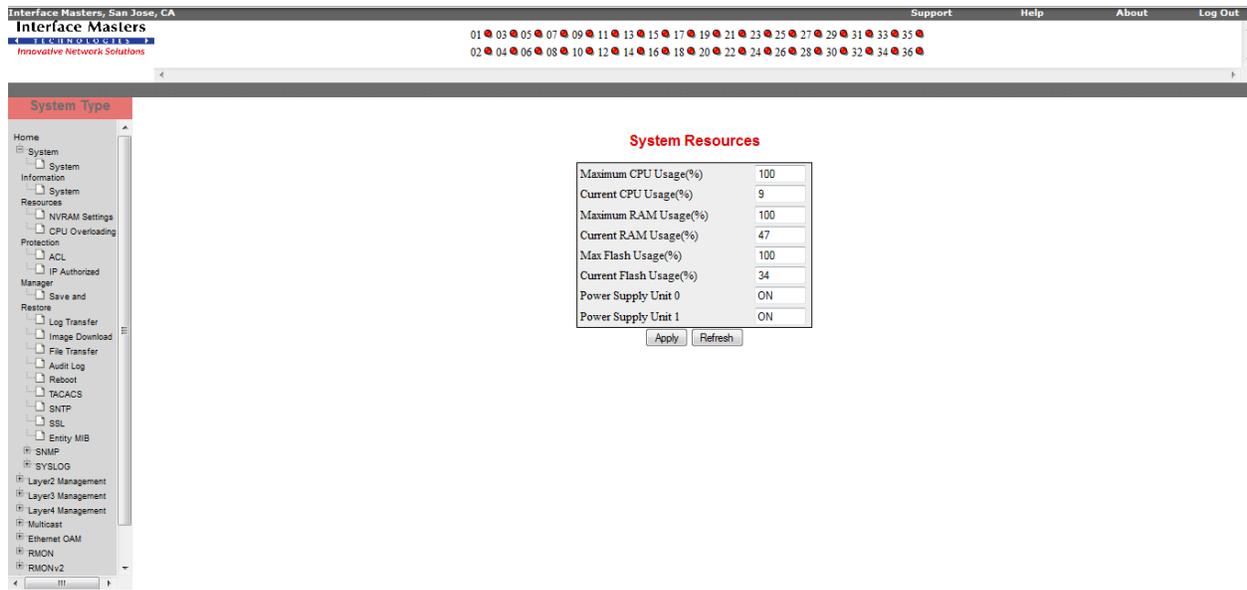


Figure 3-2: System Resources Page – System Group

2. Configure the parameters described in Table 3-2.

Table 3-2: System Resources

Field Name	Description
Minimum Temperature (celsius)	Indicates the minimum threshold temperature of the Switch in celsius. The configurable minimum range of threshold temperature is from -14 to 30 degree celsius. The default minimum threshold temperature is -14 degree celsius. When the current temperature drops below the threshold, an SNMP trap with maximum severity is sent to the SNMP Manager.
Maximum Temperature (celsius)	Indicates the maximum threshold temperature of the Switch in celsius. The configurable maximum threshold temperature is 35 to 40 degree celsius. The default maximum threshold temperature is 40 degree celsius. When the current temperature rises above the threshold, an SNMP trap with maximum severity is sent to the SNMP Manager.
Current Temperature (celsius)	Indicates the current temperature of the Switch in celsius. An SNMP trap with maximum severity is sent to the SNMP Manager, if there is any rise or drop in the temperature of the Switch.
Maximum CPU Usage (%)	Indicates the maximum CPU usage of the Switch in percentage. The configurable value ranges from 1 to 100 percentages. The default maximum CPU usage is 100%. When the CPU load exceeds the threshold value, an SNMP trap with maximum severity is sent to the SNMP Manager.
Current CPU Usage (%)	Indicates the current CPU threshold of the Switch in percentage. The default CPU Usage is 0%.
Maximum Power Supply (volts)	Indicates the maximum power supply of the Switch in volts. The configurable maximum power supply is 1 to 255 volts. The default value is 230 volts.

Field Name	Description
	When the current voltage exceeds the threshold value, an SNMP trap with maximum severity is sent to the SNMP Manager.
Minimum Power Supply (volts)	<p>Indicates the minimum power supply of the Switch in volts.</p> <p>The configurable minimum power supply is 1 to 255 volts. The default value is 100 volts.</p> <p>When the current voltage drops from the threshold value, an SNMP trap with maximum severity is sent to the SNMP Manager.</p>
Current Power Supply (volts)	Indicates the current power supply in volts. The default Power Supply is 230 volts.
Maximum RAM Usage (%)	<p>Indicates the maximum RAM usage of the Switch in percentage.</p> <p>The configurable value ranges from 1 to 100 percentage. The default value is 100%.</p> <p>When the RAM usage crosses the threshold percentage an SNMP trap with maximum severity is sent to the SNMP Manager.</p>
Current RAM Usage (%)	Indicates the current RAM usage of the switch in percentage.
Max Flash Usage (%)	<p>Indicates the maximum Flash usage of the Switch in percentage.</p> <p>The configurable value ranges from 1 to 100 percentage.</p> <p>The default value is 95%.</p> <p>When the Flash usage crosses the threshold percentage, an SNMP trap with maximum severity is sent to the SNMP Manager.</p>
Current Flash Usage (%)	Indicates the current Flash usage of Switch in percentage.

3. Click **Apply** for the configuration to take effect.
4. Click **Refresh** to display the Current temperature, CPU Usage, Power Supply, RAM usage and Flash usage.

3.3 NVRAM Settings

The **Factory Default Settings** page allows you to configure the NVRAM (Non Volatile Random Access Memory).

To configure NVRAM

1. Select **System > NVRAM Settings** to open **Factory Default Settings** page.

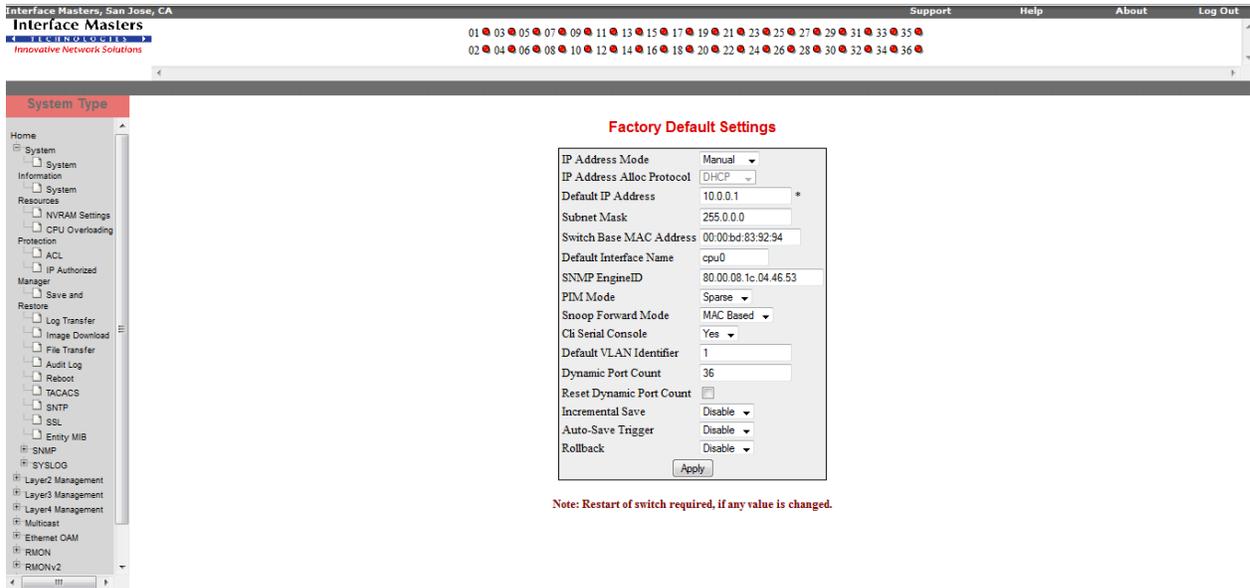


Figure 3-3: Factory Default Settings - System Group

2. Configure the parameters described in Table 3-3.

Table 3-3: Factory Default Settings

Field Name	Description
IP Address Mode	<p>Specifies the means by which the default interface in the device gets the IP address. Options are:</p> <ul style="list-style-type: none"> • Manual – The default interface takes the issDefaultIpAddr configured in the system. • Dynamic – The default interface gets the IP address through dynamic IP address configuration protocols such as RARP (Reverse Address Resolution Protocol) client, BootP client and DHCP Client. <p>By default, Manual mode is selected.</p> <p><input type="checkbox"/> If the system fails to get the IP address dynamically through all the above protocols, the default interface uses the issDefaultIpAddr configured in the system.</p>
IP Address Alloc Protocol ³	<p>Specifies the protocol to be used to obtain IP address for this interface. This is valid only when IP Address Mode is set to Dynamic. Options are:</p> <ul style="list-style-type: none"> • RARP – Reverse Address Resolution Protocol • DHCP – Dynamic Host Configuration Protocol • BOOTP Boot Protocol. <p>By default, DHCP option is selected.</p>
Default IP Address	Specifies the default IP address of the system.
Subnet Mask	Specifies the IP subnet mask for the default IP address.

³ Currently, the RARP option is not supported.

Field Name	Description
Switch Base MAC Address	Specifies the Ethernet address (base address) of the switch.
Default Interface Name	Specifies the name of the default interface that can be used for communicating with the system for configuration through SNMP or Web interface. By default, eth0 is selected.
SNMP EngineID	Specifies the SNMP Engine ID (Identifier).
PIM Mode	Specifies the PIM mode of the system. Options are: <ul style="list-style-type: none"> Dense Sparse By default, Sparse is selected.
Snoop Forward Mode	Specifies the IGMP (Internet Group Management Protocol) snooping mode. Options are: <ul style="list-style-type: none"> IP based - The hardware supports programming of S, G and *, G entries. MAC based - The hardware supports only MAC based multicast tables.
CLI Serial Console	Indicates whether the CLI console prompt will be made available to the user for the session through serial console. Options are: <ul style="list-style-type: none"> Yes - CLI prompt will be available in serial console. No - CLI prompt will not be available in serial console session. This does not affect the availability of CLI prompt in sessions established through Telnet.
Default VLAN Identifier	Specifies the default VLAN Identifier to be used at system startup. The VLAN Module creates this VLAN as the default VLAN. This value ranges between 1 and 4094. Default value is 1.

3. Click **Apply** for the configuration to take effect.



Restart the switch for the configuration to take effect.

3.4 IP Authorized Manager

The **IP Authorized Manager** page allows you to configure the IP authorized manager.

To configure IP authorized manager

1. Select **System > IP Authorized Manager** to open **IP Authorized Manager** page.

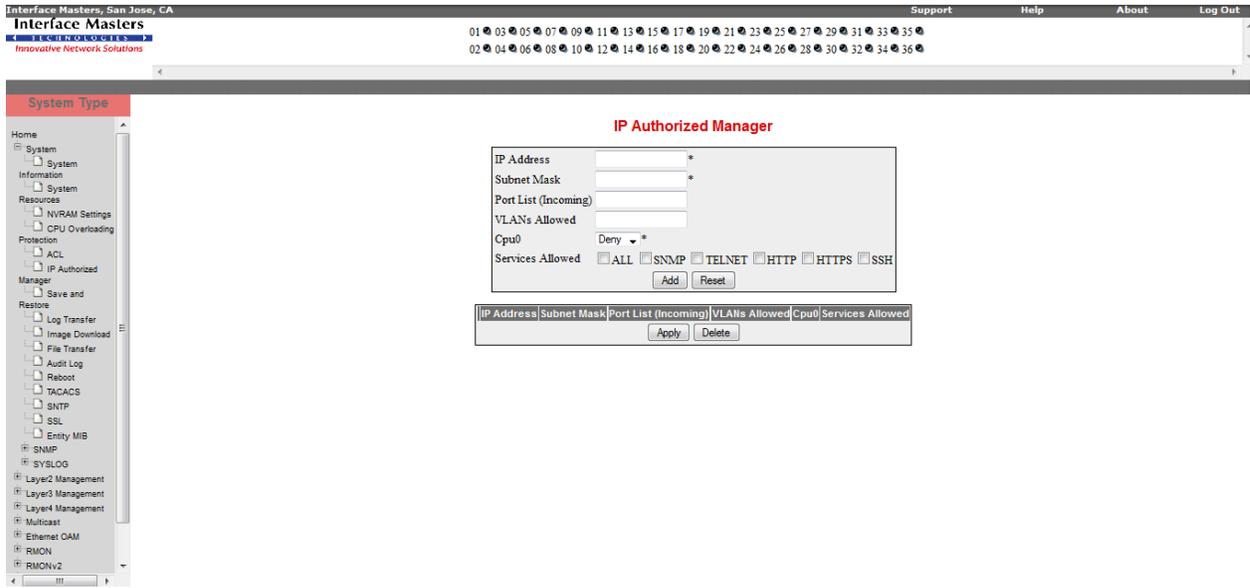


Figure 3-4: IP Authorized Manager - System Group

2. Configure the parameters described in Table 3-4.

Table 3-4: IP Authorized Manager

Field Name	Description
IP Address	Specifies the Network or Host address from which the switch can be managed. An address 0.0.0.0 indicates Any Manager .
Subnet Mask	Specifies the Mask for specified IP Address. Value 0.0.0.0 indicates mask for Any Manager .
Port List (Incoming)	Specifies the port numbers through which the manager can access the switch. <input type="checkbox"/> By default, the authorized manager is allowed to access the switch through all the ports. If a set of ports are configured in the Port List, the manager can access the switch only through the configured ports.
VLANs Allowed	Specifies the VLANs in which the IP authorized manager can reside. <input type="checkbox"/> By default, the manager is allowed to reside in any VLAN. If a set of VLANs are configured in the VLANs Allowed list, the manager can reside only in the configured VLAN set. Access to the switch will be denied from any other VLAN.
Cpu0	Specifies whether the manager can access the switch through OOB Port. Options are: <ul style="list-style-type: none"> Deny - Denies the OOB Interface access to the switch through the manager. Allow - Allows the OOB Interface access to the switch through the manager. By default, Deny is selected.
Services Allowed	Specifies the allowed services through which the manager can access the switch. Options are: <ul style="list-style-type: none"> ALL SNMP

Field Name	Description
	<ul style="list-style-type: none">• TELNET• HTTP• HTTPS• SSH
	By default, ALL is selected.

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.5 Save and Restore

The **Save and Restore** link allows you to configure Save and Restore options through the following links:

- Save
- Restore
- Erase
- Remote Restore

By default, the **Save Configuration** page is loaded.

3.5.1 Save

The **Save configuration** page allows you to save the essential configuration in the Flash.

To Save Configuration in the Flash

1. Select **System > Save and Restore** to open **Save configuration** page.

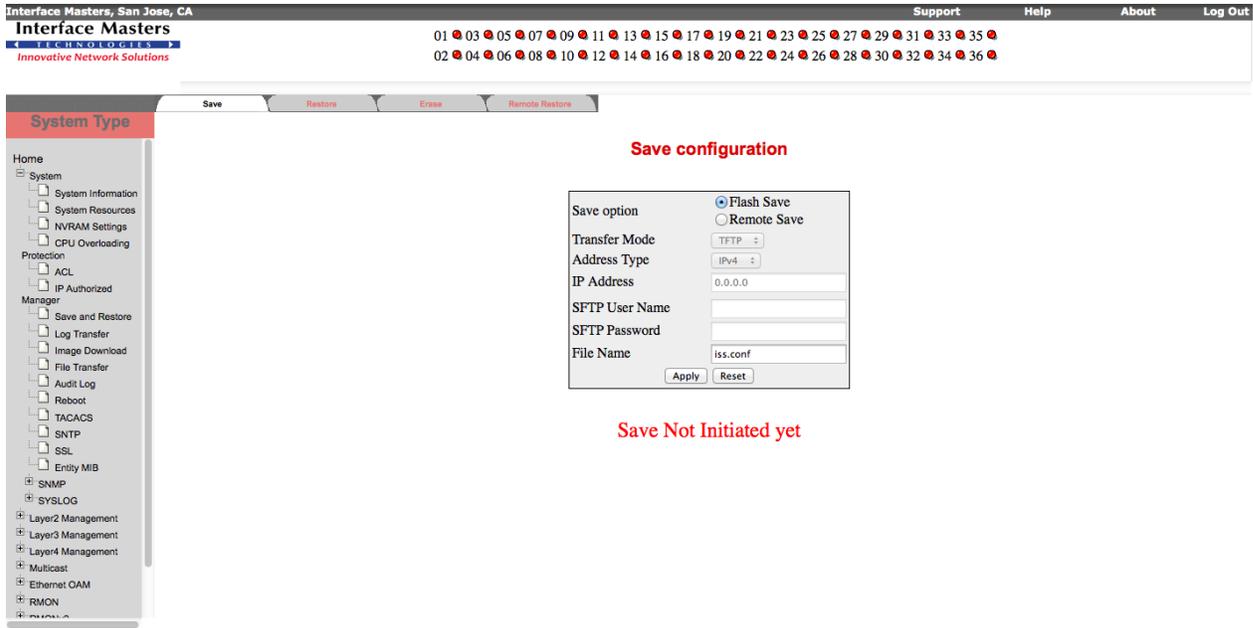


Figure 3-5: Save configuration - System Group

2. Configure the parameters described in Table 3-5.

Table 3-5: Save configuration

Field Name	Description
Save option	Specifies the save option for the configurations of the switch. Options are: <ul style="list-style-type: none"> Flash Save - The configurations will be saved in flash in the specified file name. Remote Save - The configurations will be saved in specified remote system.
Transfer Mode	Specifies the transfer mode for saving the switch configurations on to the remote system. The options are: <ul style="list-style-type: none"> TFTP – Saves the switch configurations on to the remote system in TFTP (Trivial File Transfer Protocol) mode. SFTP – Saves the switch configurations on to the remote system in SFTP (SSH File Transfer Protocol) mode. The default value is TFTP . <input type="checkbox"/> This field is applicable only for the Remote Save option.
IP Address	Specifies the IP Address of the remote system in which the switch configurations are to be saved. This is valid only if Save Option is chosen as Remote Save .
SFTP User Name	Specifies the user name required for saving the switch configurations on to the remote system in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is TFTP. This field is applicable only for the Remote Save option.
SFTP Password	Specifies the password required for saving the switch configurations on to the remote system in SFTP mode. This field is a string with size varying between 1 and

Field Name	Description
	20.
	<input type="checkbox"/> This field is disabled if the transfer mode is TFTP. This field is applicable only for the Remote Save option.
File Name	Specifies the name of the file in which the switch configurations are to be saved. Default file name is iss.conf.
	<ol style="list-style-type: none"> Click Apply for the configuration to take effect. Click Reset to clear the configured values.

3.5.2 Restore

The **Restore configuration** page allows you to restore the configuration from the Flash.

To Restore configuration

- Select **System > Save and Restore > Restore** to open **Restore configuration** page.

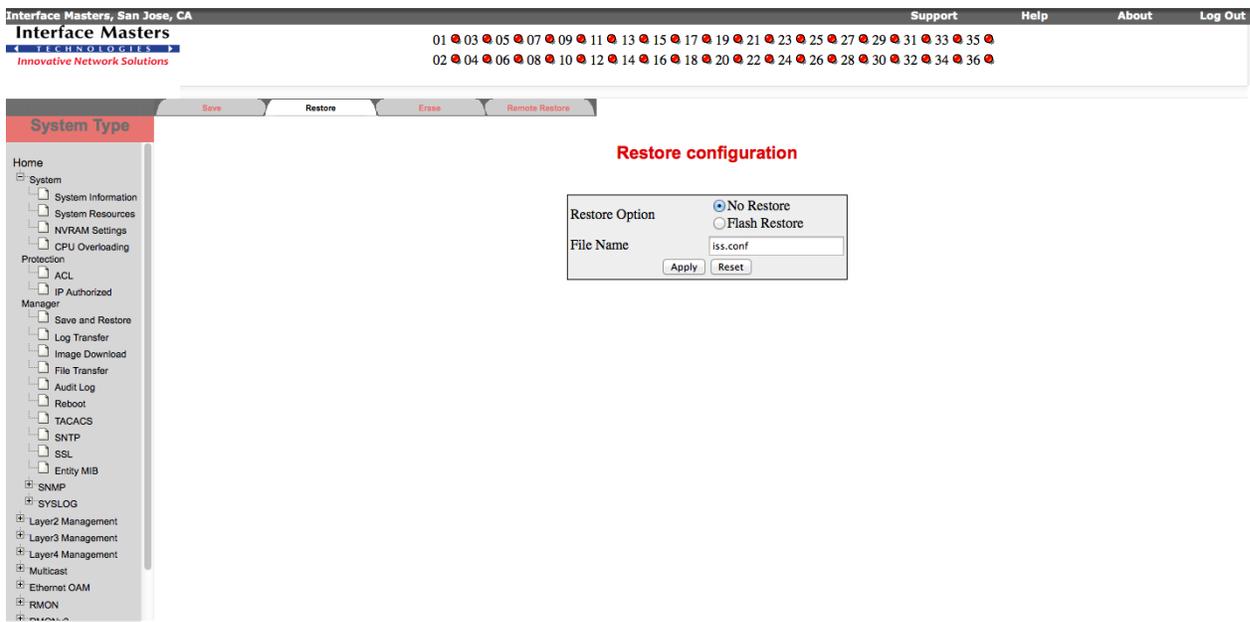


Figure 3-6: Restore Configuration - System Group

- Configure the parameters described in Table 3-6.

Table 3-6: Restore Configuration

Field Name	Description
Restore option	Specifies whether the switch configurations have to be restored or not. Options are: <ul style="list-style-type: none"> No Restore - The switch configurations will not be restored when the system is restarted. Flash Restore - The configurations will be restored from the Startup Configuration File in the flash when the system is restarted.

Field Name	Description
File Name	Specifies the configuration file name in the remote system, which has to be downloaded to the Startup Configuration File in the flash. Default file name is iss.conf.

- Click **Apply** for the configuration to take effect.
- Click **Reset** to clear the configured values.

3.5.3 Erase

The **Erase configuration** page allows you to erase saved configuration from NVRAM, Flash or specified saved file.

To Erase Configuration

- Select **System** > **Save and Restore** > **Erase** to open **Erase configuration** page.

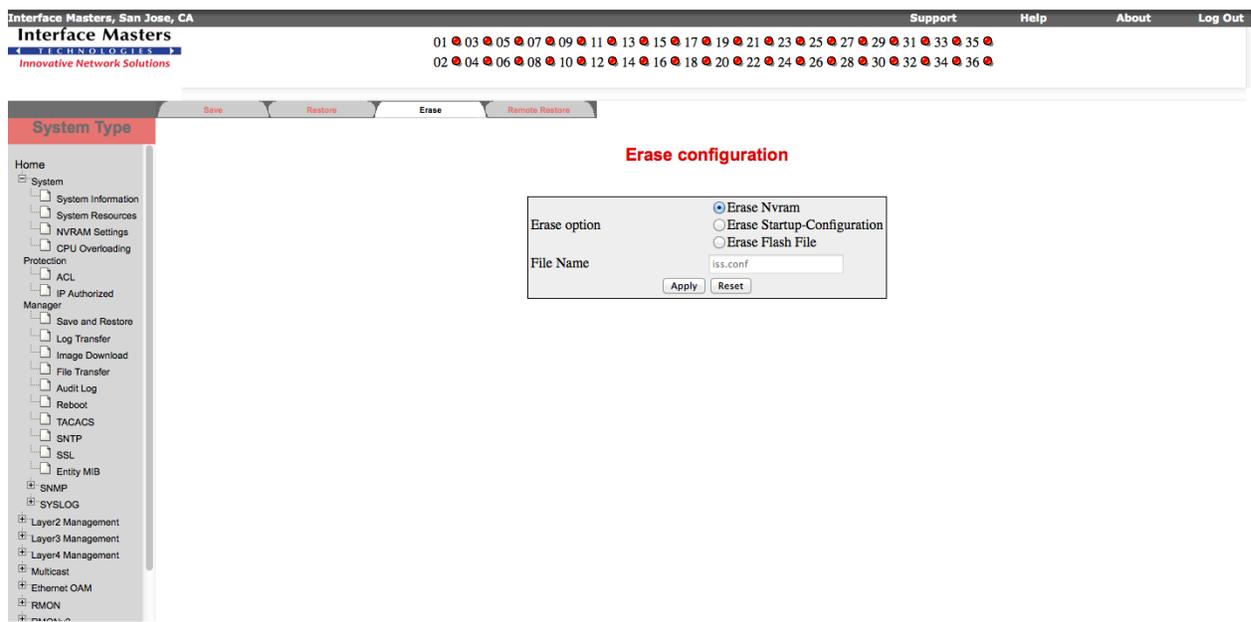


Figure 3-7: Erase Configuration - System Group

- Configure the parameters described in Table 3-7.

Table 3-7: Erase Configuration

Field Name	Description
Erase option	Specifies whether the switch configurations have to be erased or not. Options are: <ul style="list-style-type: none"> Erase Nvram - The switch configurations in NVRAM will be erased. Erase Startup-Configuration - The switch configurations provided in the Startup Configuration File of the flash will be erased. Erase Flash File - The switch configurations in the specified file will be erased.
File Name	Specifies the configuration file name in the remote system that has to be erased.

Field Name	Description
	This is valid only if Erase Flash File is selected.
	Default file name is iss.conf.

- Click **Apply** for the configuration to take effect.
- Click **Reset** to clear the configured values.

3.5.4 Remote Restore

The **Load File** page allows you to browse a file from a specific location.

To Load File

- Select **System > Save and Restore > Remote Restore** to open **Load File** page.

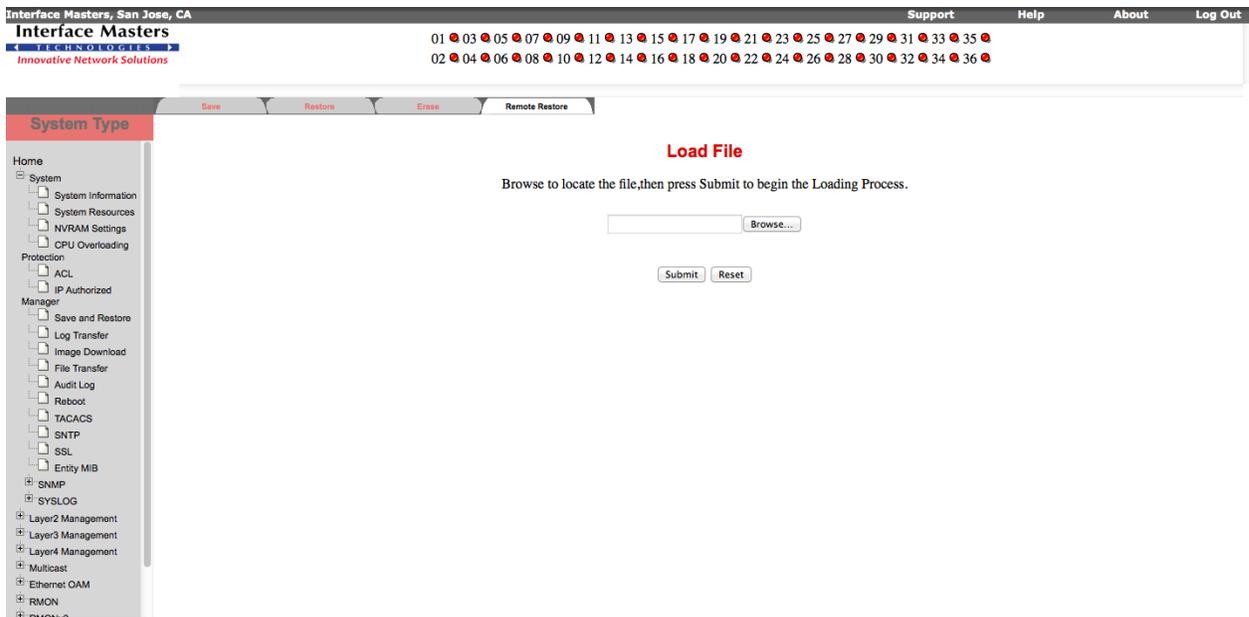


Figure 3-8: Remote Restore - System Group

- Click **Browse** to locate and select the file.
- Click **Submit** to begin the Loading Process.
- Click **Cancel** to abort the process.

3.6 Log Transfer

The **Log Transfer Settings** page allows you to configure log transfer parameters.

To configure log transfer parameters:

- Select **System > Log Transfer** to open **Log Transfer Settings** page.

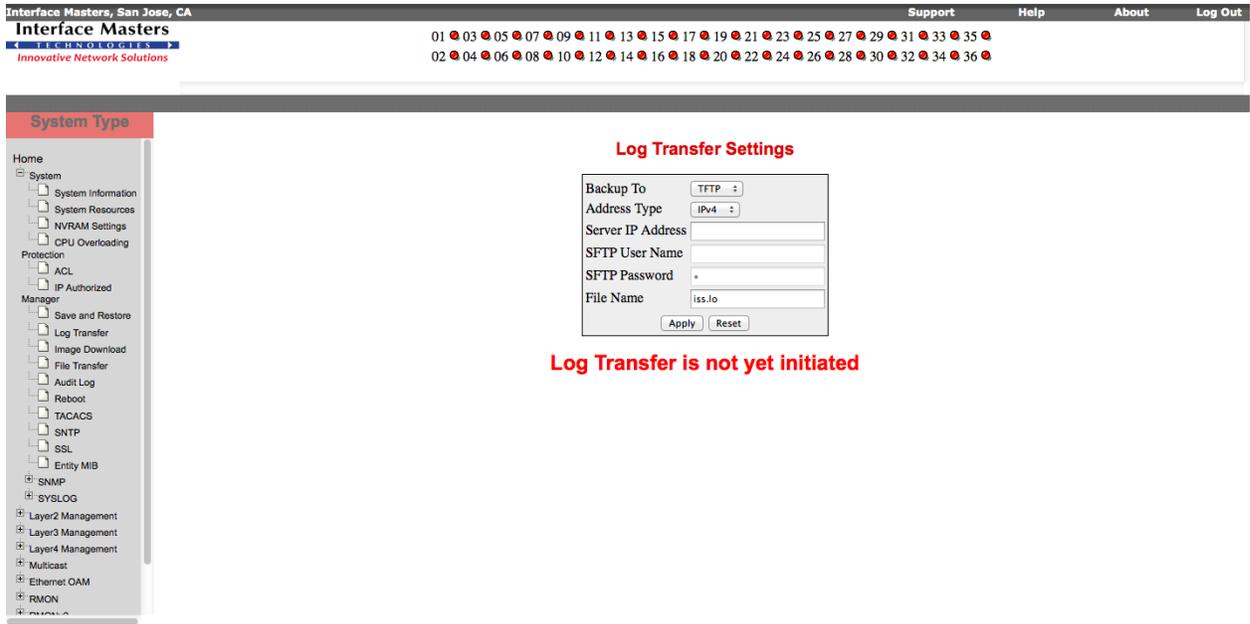


Figure 3-9: Log Transfer Settings – System Group

2. Configure the parameters described in the Table 3-8.

Table 3-8: Log Transfer Settings

Field Name	Description
Backup To	Specifies the transfer mode for uploading log file to the remote system. The options are: <ul style="list-style-type: none"> • TFTP – Uploads the log file in TFTP (Trivial File Transfer Protocol) mode. • SFTP – Uploads the log file in SFTP (SSH File Transfer Protocol) mode. The default value is TFTP .
Server IP Address	Specifies the IP address of the machine to which the log file is to be uploaded.
SFTP User Name	Specifies the user name required for uploading log file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
SFTP Password	Specifies the password required for uploading log file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
File Name	Specifies the file name in which the logs are saved in the remote system.

3. Click **Apply** for the configuration to take effect.
4. Click **Reset** to discard the entered information.

3.7 Image Download

The **Software Upgrade** page allows you to configure parameters related to downloading of image from remote server.

To configure parameters related image download

1. Select **System > Image Download** to open **Software Upgrade** page.

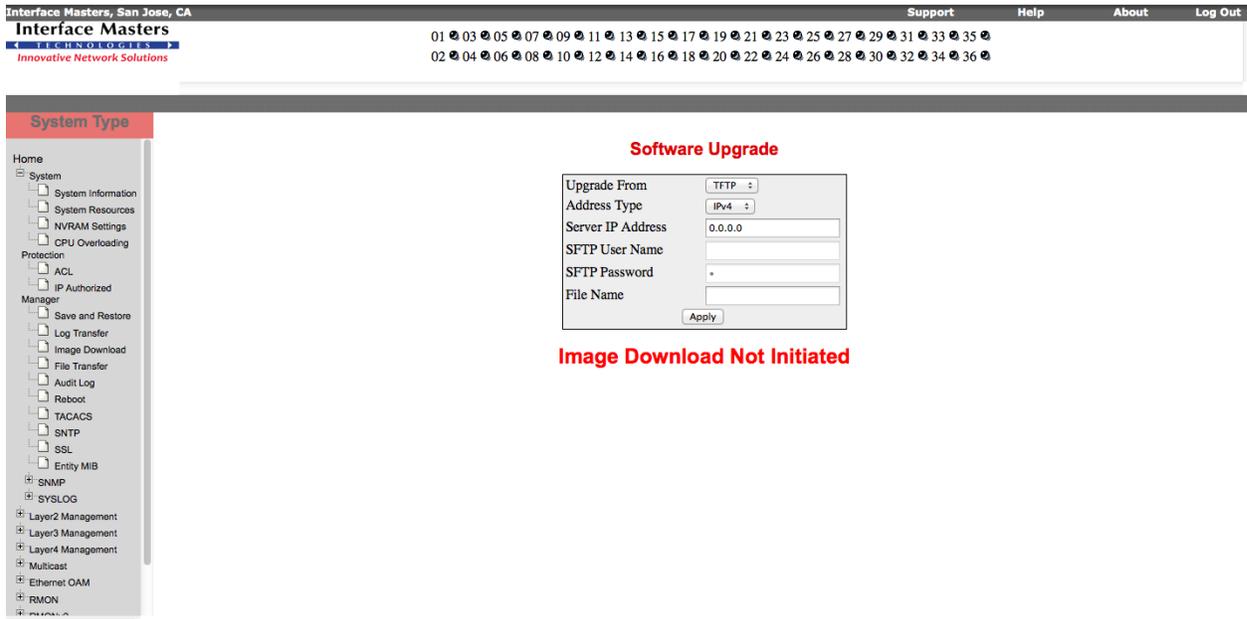


Figure 3-10: Software Upgrade – System Group

2. Configure the parameters described in the Table 3-9.

Table 3-9: Software Upgrade

Field Name	Description
Upgrade From	<p>Specifies the type of server from which image should be downloaded. The options are:</p> <ul style="list-style-type: none"> • TFTP – Sets the server type as TFTP (Trivial File Transfer Protocol) mode. • SFTP – Sets the server type as SFTP (SSH File Transfer Protocol) mode. <p>The default value is TFTP.</p>
Server IP Address	<p>Specifies the IP address of the machine from which the image is to be downloaded.</p>
SFTP User Name	<p>Specifies the user name required for downloading image from SFTP server. This field is a string with size varying between 1 and 20.</p> <p><input type="checkbox"/> This field is disabled if the server is TFTP server.</p>

Field Name	Description
SFTP Password	Specifies the password required for downloading image from SFTP server. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the server is TFTP server.
File Name	Specifies the name of the image to be downloaded from the remote system.

3. Click **Apply** for the configuration to take effect.

3.8 File Transfer

The file transfer link allows you to upload file to remote server or download file from remote server through the following links

- File Upload
- File Download

By default, the **File Upload** page is loaded.

3.8.1 File Upload

The **File Upload** page allows you to upload file to remote server.

To configure file upload parameters

1. Select **System > File Transfer** to open **File Upload** page.

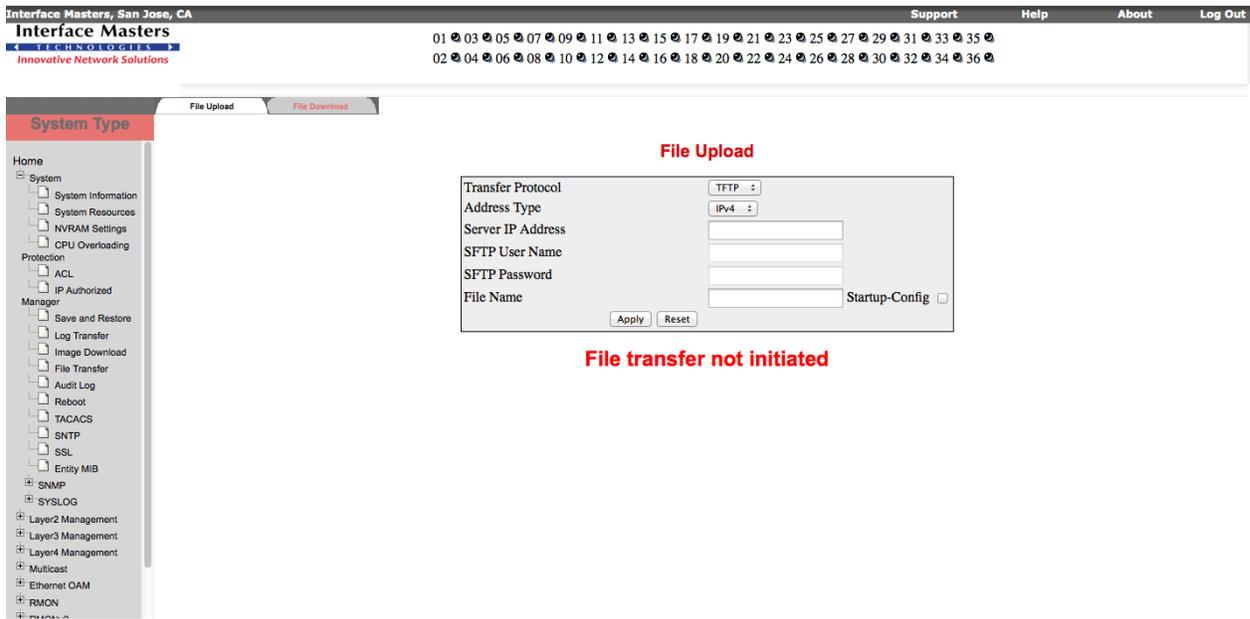


Figure 3-11: File Upload – System Group

2. Configure the parameters described in the Table 3-10.

Table 3-10: File Upload

Field Name	Description
Transfer Protocol	Specifies the transfer mode for uploading file to the remote system. The options are: <ul style="list-style-type: none"> TFTP – Uploads the file in TFTP (Trivial File Transfer Protocol) mode. SFTP – Uploads the file in SFTP (SSH File Transfer Protocol) mode. The default value is TFTP .
Server IP Address	Specifies the IP address of the machine to which the file is to be uploaded.
SFTP User Name	Specifies the user name required for uploading file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
SFTP Password	Specifies the password required for uploading file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
File Name	Specifies the name of the file to be uploaded to the remote system.

3. Click **Apply** for the configuration to take effect.
4. Click **Reset** to discard the entered information.

3.8.2 File Download

The **File Download** page allows you to download file from remote server.

To configure file download parameters

1. Select **System > File Transfer > File Download** to open **File Download** page.

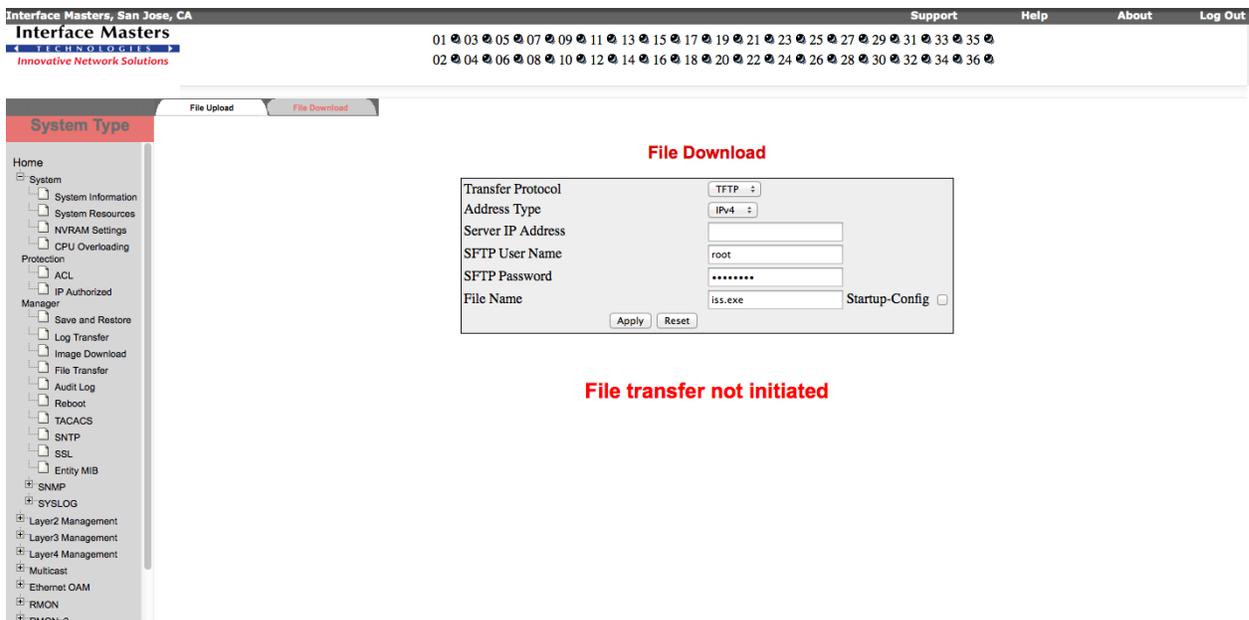


Figure 3-12: File Download – System Group

2. Configure the parameters described in the Table 3-11.

Table 3-11: File Download

Field Name	Description
Transfer Protocol	Specifies the transfer mode for downloading file from the remote system. The options are: <ul style="list-style-type: none"> • TFTP – Downloads the file in TFTP (Trivial File Transfer Protocol) mode. • SFTP – Downloads the file in SFTP (SSH File Transfer Protocol) mode. The default value is TFTP .
Server IP Address	Specifies the IP address of the machine from which the file is to be downloaded.
SFTP User Name	Specifies the user name required for downloading file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
SFTP Password	Specifies the password required for downloading file in SFTP mode. This field is a string with size varying between 1 and 20. <input type="checkbox"/> This field is disabled if the transfer mode is selected as TFTP.
File Name	Specifies the name of the file to be downloaded from the remote system.

3. Click **Apply** for the configuration to take effect.
4. Click **Reset** to discard the entered information.

3.9 TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server 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.

The **TACACS** link allows you to configure TACACS through the following links:

- Tacacs Settings
- Tacacs AS

By default, the **TACACS Server Configuration** page is loaded.

3.9.1 Tacacs Settings

The **TACACS Server Configuration** page allows you to configure the details of TACACS server.

To configure TACACS Server

1. Select **System > TACACS** to open the **TACACS Server Configuration** page.

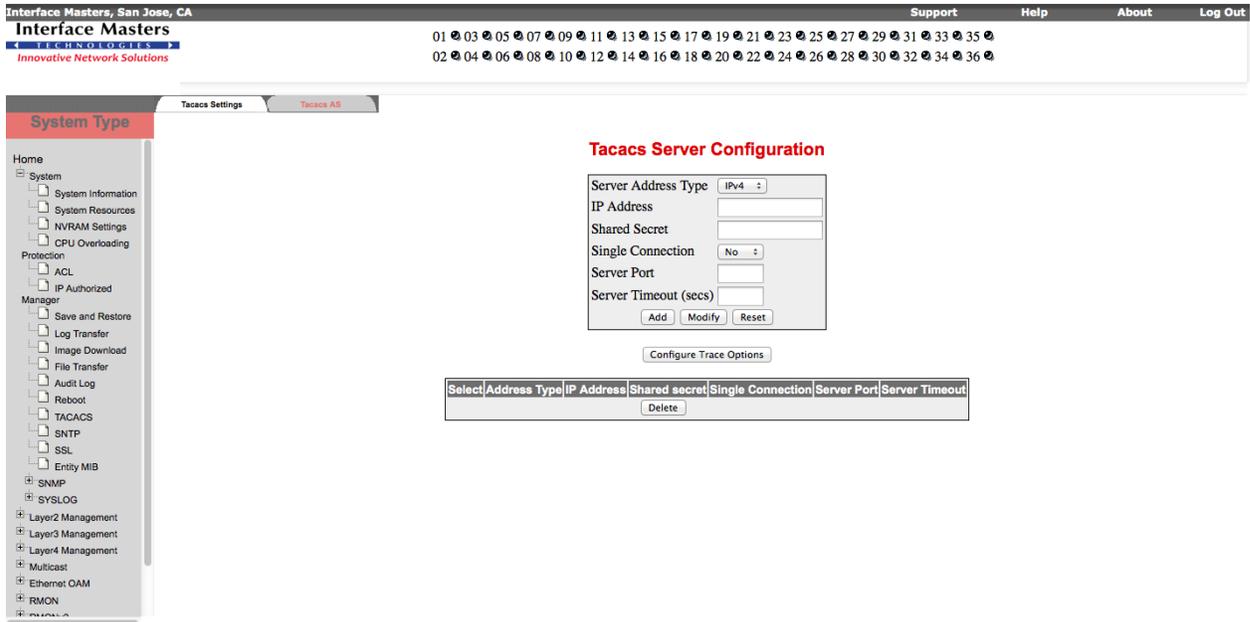


Figure 3-13: TACACS Server Configuration - System Group

- Configure the parameters described in Table 3-12.

Table 3-12: Configuring TACACS Server

Field	Description
Server Address Type	Specifies the server address type. Options are: <ul style="list-style-type: none"> IPV4 - Internet Protocol Version 4 IPV6 - Internet Protocol Version 6
IP Address	Specifies the server IP address. <input type="checkbox"/> ISS TACACS allows maximum of 5 server information to be configured.
Shared Secret	Specifies the secret key shared between the client and server for encryption and decryption.
Single Connection	Informs whether single connect support is enabled/ disabled for the server. Options are: <ul style="list-style-type: none"> Yes – Multiple sessions are handled over a single TCP connection. No – Multiple sessions are not allowed to handle over a single TCP connection. By default, Single Connection is set to No.
Server Port	Specifies the server port number for TACACS protocol. The default values are 49 for IPv4 and 4949 for IPv6.
Server Timeout (secs)	Specifies the timeout value within which a response is expected from server. The default value for Server Time out is 5 seconds.

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

3.9.2 Tacacs AS

The **TACACS Active Server Configuration** page allows you to configure the details of TACACS active server.

To configure TACACS Active Server

1. Select **System > TACACS > TACACS AS** to open the **TACACS Active Server Configuration** page.

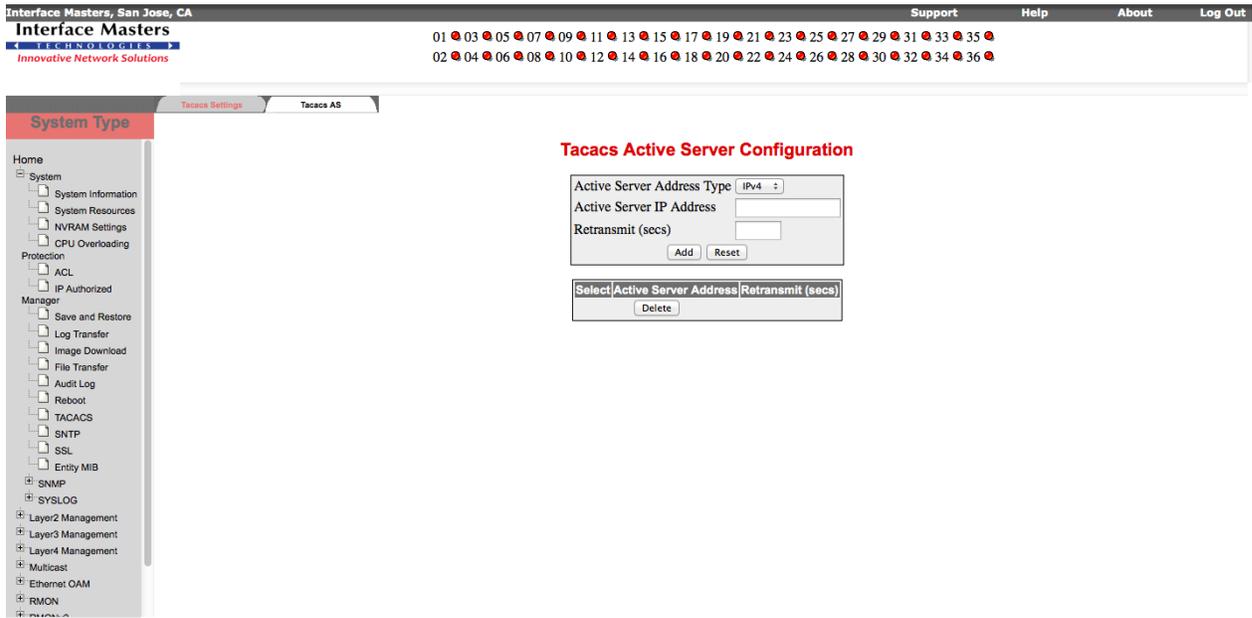


Figure 3-14: TACACS Active Server Configuration - System Group

2. Configure the parameters described in Table 3-13.

Table 3-13: Configuring TACACS Active Server

Field	Description
Active Server Address Type	Specifies the address type of the active server. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
Active Server IP Address	Specifies the active server IP address. If Active Server IP address is set to zero, then the active server concept is disabled.
Retransmit (secs)	Specifies the number of times the TACACS client server searches the list of TACACS servers. This value ranges between 1 and 100 seconds. The default value of Retransmit is 2 seconds.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Click **Delete** for the entry to be deleted.

3.10 Entity MIB

Entity MIB is a standardized way of representing a single agent which supports multiple instances of one MIB and is specified by RFC4133.

The **Entity MIB** link allows you to configure Entity MIB through the following links:

- Physical Entity Details
- Logical Entity Details
- LP Mapping Details
- Alias Mapping Details
- Contains Mapping Details

By default, the **Physical Table Entries** page is loaded.

3.10.1 Physical Entity Details

The **Physical Table Entries** page allows you to configure the physical table entries. The physical table contains one row per physical entity and provides information such as Physical Description, Physical VendorType, Physical Class and Physical ContainedIn. These information help an NMS (Network Management System) to identify, characterize and relate a particular entry to other entries in the Physical table.

To configure Physical table

1. Select **System > Entity MIB** to open the **Physical Table Entries** page.

The screenshot shows the web interface for Interface Masters. At the top, there is a navigation bar with 'Interface Masters, San Jose, CA' on the left and 'Support', 'Help', 'About', and 'Log Out' on the right. Below this is a breadcrumb trail: 'System > Entity MIB > Physical Table Entries'. The main content area is titled 'Physical Table Entries' and contains a table with the following fields:

Physical Index :	1
Physical Description :	Network Element
Physical VendorType :	IMT
Physical ContainedIn :	0
Physical Class :	Chassis
Physical ParentRelPos :	0
Physical Name :	IM
Physical HardwareRev :	5.5.5
Physical FirmwareRev :	2636_6.2.0_2962
Physical SoftwareRev :	6.2.0
Physical Serial Num :	not available
Physical MfgName :	IMT
Physical ModelName :	not available
Physical Alias :	DummyName
Physical AssetID :	DummyId
Physical FRU Status :	True
Physical MfgDate :	00/00/00
Physical Uris :	not available

On the left side of the interface, there is a navigation tree under 'System Type' with the following items: Home, System (expanded), System Information, System Resources, NVRAM Settings, CPU Overloading, Protection (expanded), ACL, IP Authorized, Manager (expanded), Save and Restore, Log Transfer, Image Download, File Transfer, Audit Log, Reboot, TACACS, SNMP, SSL, Entity MIB (expanded), SNMP, SYSLOG, Layer2 Management, Layer3 Management, Layer4 Management, and Multicast.

Interface Masters, San Jose, CA Support Help About Log Out

Interface Masters
TECHNOLOGIES
Innovative Network Solutions

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

Physical Entity Details Logical Entity Details LP Mapping Details Alias Mapping Details Contains Mapping Details

System Type

Home
System
System Information
System Resources
NVRAM Settings
CPU Overloading
Protection
ACL
IP Authorized
Manager
Save and Restore
Log Transfer
Image Download
File Transfer
Audit Log
Reboot
TACACS
SNTP
SSL
Entity MIB
SNMP
SYSLOG
Layer2 Management
Layer3 Management
Layer4 Management
Multicast
Ethernet OAM
RMON

Physical Index : 2
Physical Description : not available
Physical VendorType : not available
Physical ContainedIn : 1
Physical Class : Cpu
Physical ParentRelPos : 1
Physical Name : not available
Physical HardwareRev : not available
Physical FirmwareRev : not available
Physical SoftwareRev : not available
Physical Serial Num : not available
Physical MfgName : not available
Physical ModelName : not available
Physical Alias : not available
Physical AssetID : not available
Physical FRU Status : True
Physical MfgDate : not available
Physical Uri : not available

Physical Index : 3
Physical Description : not available
Physical VendorType : not available
Physical ContainedIn : 1
Physical Class : Power Supply

Interface Masters, San Jose, CA Support Help About Log Out

Interface Masters
TECHNOLOGIES
Innovative Network Solutions

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

Physical Entity Details Logical Entity Details LP Mapping Details Alias Mapping Details Contains Mapping Details

System Type

Home
System
System Information
System Resources
NVRAM Settings
CPU Overloading
Protection
ACL
IP Authorized
Manager
Save and Restore
Log Transfer
Image Download
File Transfer
Audit Log
Reboot
TACACS
SNTP
SSL
Entity MIB
SNMP
SYSLOG
Layer2 Management
Layer3 Management
Layer4 Management
Multicast
Ethernet OAM
RMON

Physical AssetID : not available
Physical FRU Status : False
Physical MfgDate :
Physical Uri : not available

Physical Index : 44
Physical Description : Ethernet Interface
Physical VendorType : not available
Physical ContainedIn : 8
Physical Class : Port
Physical ParentRelPos : 36
Physical Name : extreme-ethernet 0/36
Physical HardwareRev : not available
Physical FirmwareRev : not available
Physical SoftwareRev : not available
Physical Serial Num : not available
Physical MfgName : not available
Physical ModelName : not available
Physical Alias : Ex0/36
Physical AssetID : not available
Physical FRU Status : False
Physical MfgDate :
Physical Uri : not available

Apply

Figure 3-15: Physical Table Entries - System Group

2. Configure the parameters described in Table 3-14.

Table 3-14: Configuring Physical Table

Field	Description
Physical Index	Specifies the index for the physical entity.
Physical Description	Specifies a textual description of the physical entity. This field contains a string that identifies the manufacturer's name for the physical entity,

Field	Description
	and is set to a distinct value for each version or model of the physical entity.
Physical VendorType	Indicates the vendor-specific hardware type of the physical entity. If no vendor-specific registration identifier exists for the physical entity, or the value is unknown by the agent, then the value { 0 0 } is set.
Physical ContainedIn	Specifies the value of physical index for the physical entity which contains this physical entity. A value of zero indicates that this physical entity is not contained in any other physical entity.
Physical Class	Indicates of the general hardware type of the physical entity.
Physical HardwareRev	Specifies the vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier actually printed on the component itself (if present). If the revision information is stored internally in a non-printable (for example, binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific hardware revision string is associated with the physical component, or if the information is unknown to the agent, then this object contains a zero-length string.
Physical FirmwareRev	Specifies the vendor-specific firmware revision string for the physical entity. If the revision information is stored internally in a non-printable (for example, binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific firmware revision string is associated with the physical component, or if the information is unknown to the agent, then this object contains a zero-length string.
Physical SoftwareRev	Specifies the vendor-specific software revision string for the physical entity. If the revision information is stored internally in a non-printable (for example, binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software revision string is associated with the physical component, or if the information is unknown to the agent, then this object contains a zero-length string.
Physical Serial Num	Specifies the vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present).
Physical MfgName	Specifies the name of the manufacturer of the physical component. The preferred value is the manufacturer name string actually printed on the component itself (if present). If the manufacturer name string associated with the physical component is unknown to the agent, then this object contains a zero-length string.
Physical ModelName	Specifies the vendor-specific model name identifier string associated with the physical component. The preferred value is the customer-visible part number, which may be printed on the component itself. If the model name string associated with the physical component is unknown to the agent, then this object contains a zero-length string.

Field	Description
Physical Alias	Specifies the alias name for the physical entity, as specified by a network manager, and provides a non-volatile handle for the physical entity.
Physical AssetID	Specifies a user-assigned asset tracking identifier (as specified by a network manager) for the physical entity, and provides non-volatile storage of this information.
Physical FRU Status	Indicates whether the physical entity is considered as a FRU (Field Replaceable Unit) by the vendor. If this object contains the value 1, then the physical entry identifies a FRU. For all physical entries that represent components permanently contained within a FRU, the value 2 is returned.
Physical MfgDate	Specifies the date of manufacturing of the managed entity. If the manufacturing date is unknown or not supported, this field is not instantiated. In this case, the special value '0000000000000000'H may also be returned.
Physical Uris	Specifies additional identification information about the physical entity. The object contains URIs and, therefore the syntax of this object must conform to RFC 3986.

3. Click **Apply** for the configuration to take effect.

3.10.2 Logical Entity Details

The **Logical Table Entries** page allows you to configure the logical table entries.

To configure Logical table

1. Select **System > Entity MIB > Logical Entity Details** to open the **Logical Table Entries** page.

Interface Masters, San Jose, CA

Support Help About Log Out

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

Physical Entity Details Logical Entity Details LP Mapping Details Alias Mapping Details Contains Mapping Details

System Type

Home

- System
 - System Information
 - System Resources
 - NVRAM Settings
 - CPU Overloading
- Protection
 - ACL
 - IP Authorized Manager
 - Save and Restore
 - Log Transfer
 - Image Download
 - File Transfer
 - Audit Log
 - Reboot
 - TACACS
 - SNTP
 - SSL
 - Entity MIB
- SNMP
- SYSLLOG
- Layer2 Management
- Layer3 Management
- Layer4 Management
- Multicast
- Ethernet OAM
- RMON

Logical Table Entries

Logical Index	Logical Description	Logical Type	Logical Community	Logical Address	Logical TDomain	Logical ContextEngineId	Logical ContextName
1	Interface Masters Technology	1937007728.1851876096.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
2	Interface Masters Technology	1937007724.1818521600.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
3	Interface Masters Technology	1937007727.1949527148.1685061632.0.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
4	Interface Masters Technology	1937007727.1949396076.1685061632.0.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
5	Interface Masters Technology	1937007724.1630628972.1685061632.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
6	Interface Masters Technology	1936616816.1296646764.1685061632.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
7	Interface Masters Technology	1768312137.1112097388.1685061632.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
8	Interface Masters Technology	1937007732.1668311408.1987575808.0.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
9	Interface Masters Technology	1937007733.1685088624.1987575808.0.0.0.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
10	Interface Masters Technology	1937007717.1952999792.1987575808.0.0.0	64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default
11	Interface Masters Technology		64:65:66:61:75:6c:74			80:00:08:1c:04:46:53	default

Interface Masters, San Jose, CA		Support	Help	About	Log Out	
Interface Masters <small>Innovative Network Solutions</small>		01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35				
		02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36				
System Type						
<small>Physical Entity Details</small> <small>Logical Entity Details</small> <small>LP Mapping Details</small> <small>Alias Mapping Details</small> <small>Contains Mapping Details</small>						
System Type Home System System Information System Resources NVRAM Settings CPU Overloading Protection ACL IP Authorized Manager Save and Restore Log Transfer Image Download File Transfer Audit Log Reboot TACACS SNTP SSL Entity MIB SNMP SYSLOG Layer2 Management Layer3 Management Layer4 Management Multicast Ethernet OAM RMON	12	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	13	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	14	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	15	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	16	Interface Masters Technology	1937007714.1735406704.1987575808.0.0.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	17	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	18	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	19	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	20	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	21	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	22	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	23	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	24	Interface Masters Technology	1919774574.1735406704.1987575808.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default

Interface Masters, San Jose, CA		Support	Help	About	Log Out	
Interface Masters <small>Innovative Network Solutions</small>		01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35				
		02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36				
System Type						
<small>Physical Entity Details</small> <small>Logical Entity Details</small> <small>LP Mapping Details</small> <small>Alias Mapping Details</small> <small>Contains Mapping Details</small>						
System Type Home System System Information System Resources NVRAM Settings CPU Overloading Protection ACL IP Authorized Manager Save and Restore Log Transfer Image Download File Transfer Audit Log Reboot TACACS SNTP SSL Entity MIB SNMP SYSLOG Layer2 Management Layer3 Management Layer4 Management Multicast Ethernet OAM RMON	145	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	146	Interface Masters Technology	1937007721.1886812272.2021226610.1984776514.0.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	147	Interface Masters Technology	64:65:66:61:75:6c:74		80:00:08:1c:04:46:53	default
	148	Interface Masters Technology	1937007727.1936746096.2021226610.1984776514.0.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	149	Interface Masters Technology	1937007727.1937011312.2021226610.1984776514.0.0.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	150	Interface Masters Technology	1937007730.1768977008.2021226610.1984776514.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	151	Interface Masters Technology	1718841203.1885762160.2021226610.1984776514.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	152	Interface Masters Technology	1718973519.1936746068.1702065223.1919907184.0.0.0.0.0.0.0.0.0.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	153	Interface Masters Technology	1718841961.1886414420.1702065223.1919907184.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	154	Interface Masters Technology	1718842485.1852597844.1702065223.1919907184.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	155	Interface Masters Technology	1718841972.1835820628.1702065223.1919907184.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	156	Interface Masters Technology	1718837618.1886152276.1702065223.1919907184.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default
	157	Interface Masters Technology	1718839664.1987602004.1702065223.1919907184.0.0	64:65:66:61:75:6c:74	80:00:08:1c:04:46:53	default

Figure 3-16: Logical Table Entries - System Group

2. Configure the parameters described in Table 3-15.

Table 3-15: Configuring Logical Table

Field	Description
Logical Index	Specifies the index for the logical entity. Thi value is a positive integer and ranges between 1 and 2147483647.

Field	Description
Logical Description	Specifies the textual description of the logical entity. This field contains a string that identifies the manufacturer's name for the logical entity, and should be set to a distinct value for each version of the logical entity.
Logical Type	Specifies the type of logical entity. This typically is the Object identifier name of the node in the SMI (Structure of Management Information) naming hierarchy which represents the major MIB module, or the majority of the MIB modules, supported by the logical entity. If an appropriate node in the SMI's naming hierarchy cannot be identified, the value mib-2 is used.
Logical Community	Specifies an SNMPv1 or SNMPv2C community-string, which can be used to access detailed management information for the logical entity.
Logical TAddress	Specifies the transport service address by which the logical entity receives network management traffic, formatted according to the corresponding value of Logical TDomain.
Logical TDomain	Indicates the kind of transport service by which the logical entity receives network management traffic. Possible values are presently found in the Transport Mappings for Simple Network Management Protocol.
Logical ContextEngineID	Specifies the authoritative context Engine ID that is used to send an SNMP message related information held by the logical entity, to the address specified by the associated Logical TAddress/Logical TDomain pair.
Logical ContextName	Specifies the context name that is used to send an SNMP message related information held by the logical entity, to the address specified by the associated Logical TAddress/Logical TDomain pair.

3.10.3 LP Mapping Details

The **LP Mapping Table Entries** page allows you to view the logical entity to physical entity associations. For each logical entity, there are zero or more mappings to the physical resources, which are used to realize that logical entity.

To view Logical to Physical mapping

1. Select **System > Entity MIB > LP Mapping Details** to open the **LP Mapping Table Entries** page.

The screenshot displays the 'LP Mapping Table Entries' page in the Interface Masters application. The page title is 'LP Mapping Table Entries' and it features a 'Logical Index' section. The main content area contains a grid of mapping entries, each consisting of a logical index number followed by the text 'Logical Index - 1 is mapped to Physical Index - [number]'. The logical index numbers range from 1 to 120, with some numbers (1, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120) highlighted in red. The page also includes a navigation menu on the left and a breadcrumb trail at the top.

Figure 3-17: LP Mapping Table Entries - System Group

3.10.4 Alias Mapping Details

The **Alias Mapping Table Entries** page allows you to view the mappings of physical equipment and logical entity to external MIB identifiers.

To view Alias mapping

1. Select **System > Entity MIB > Alias Mapping Details** to open the **Alias Mapping Table Entries** page.

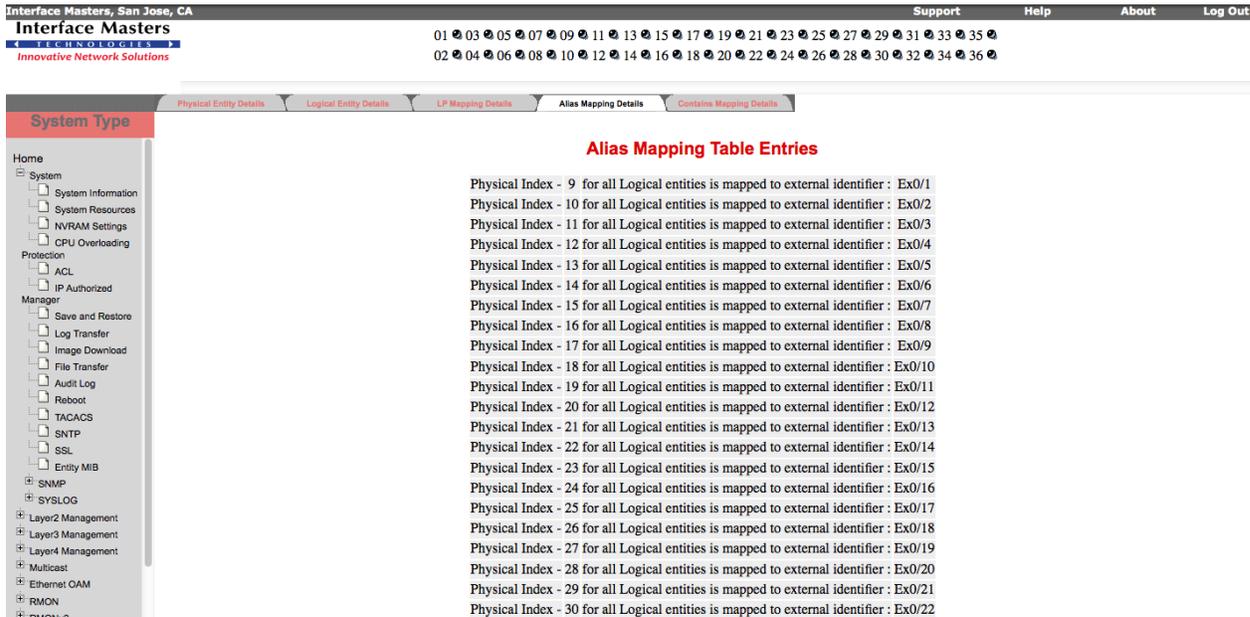


Figure 3-18: Alias Mapping Table Entries - System Group

3.10.5 Contains Mapping Details

The **Physical Contains Table** page allows you to view the container/containee relationships between the physical entities.

To view Physical entities relationship

1. Select **System > Entity MIB > Contains Mapping Details** to open the **Physical Contains Table** page.

The screenshot shows the 'Physical Contains Table' for a System Group. The table lists 23 physical components and their containment relationships with Physical Index - 1 and Physical Index - 8.

Physical Component	Contained In
Physical component with Index - 2	Physical Index - 1
Physical component with Index - 3	Physical Index - 1
Physical component with Index - 4	Physical Index - 1
Physical component with Index - 5	Physical Index - 1
Physical component with Index - 6	Physical Index - 1
Physical component with Index - 7	Physical Index - 1
Physical component with Index - 8	Physical Index - 1
Physical component with Index - 9	Physical Index - 8
Physical component with Index - 10	Physical Index - 8
Physical component with Index - 11	Physical Index - 8
Physical component with Index - 12	Physical Index - 8
Physical component with Index - 13	Physical Index - 8
Physical component with Index - 14	Physical Index - 8
Physical component with Index - 15	Physical Index - 8
Physical component with Index - 16	Physical Index - 8
Physical component with Index - 17	Physical Index - 8
Physical component with Index - 18	Physical Index - 8
Physical component with Index - 19	Physical Index - 8
Physical component with Index - 20	Physical Index - 8
Physical component with Index - 21	Physical Index - 8
Physical component with Index - 22	Physical Index - 8
Physical component with Index - 23	Physical Index - 8

Figure 3-19: Physical Contains Table - System Group

3.11 SNTP

The 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.

The **SNTP** link allows you to configure SNTP through the following links:

- SNTP Scalars
- SNTP Unicast
- SNTP Broadcast
- SNTP Multicast
- SNTP Anycast⁴

By default, the **SNTP Scalars Configuration** page is loaded.

3.11.1 SNTP Scalars

The **SNTP Scalars Configuration** page allows you to configure the SNTP scalars.

To configure SNTP Scalars

1. Select **System > SNTP** to open the **SNTP Scalars Configuration** page.

⁴ This functionality is not supported in this release.

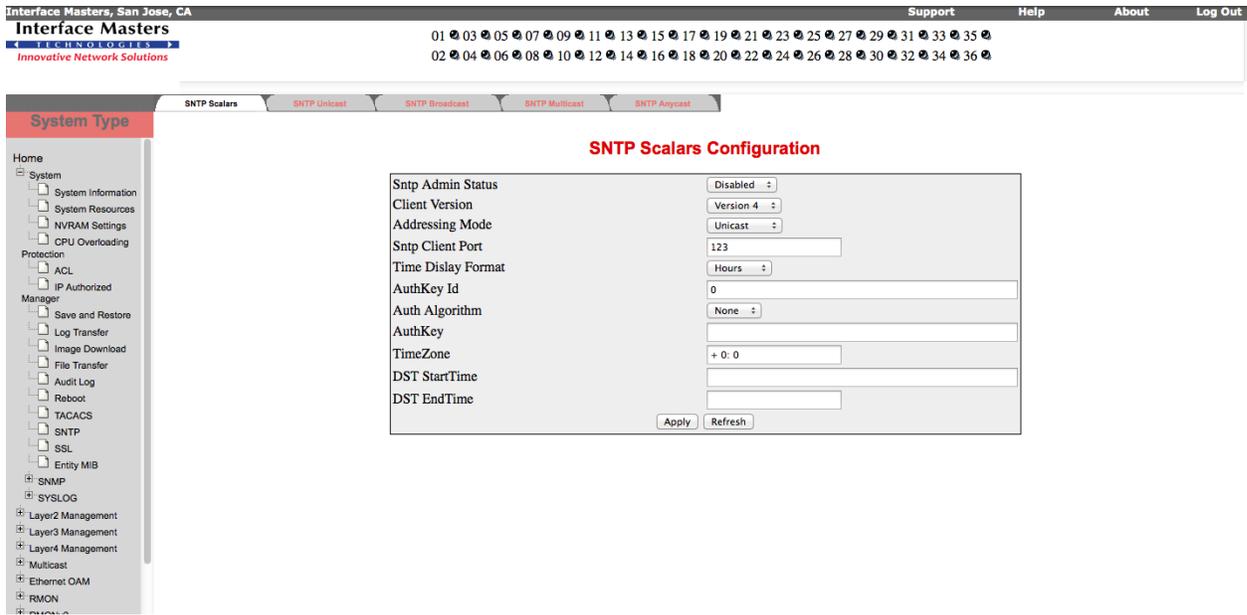


Figure 3-20: SNTP Scalars Configuration - System Group

2. Configure the parameters described in Table 3-16.

Table 3-16: SNTP Scalars Configuration

Field	Description
Sntp Admin Status	<p>Specifies the SNTP client module status. Options are:</p> <ul style="list-style-type: none"> Enabled – Enables the SNTP client module. Disabled – Disables the SNTP client module. <p>By default, this is Disabled.</p> <p><input type="checkbox"/> All the configurations are active only when the SNTP module is enabled.</p>
Client Version	<p>Specifies the SNTP client module version. Options are:</p> <ul style="list-style-type: none"> Version 1 Version 2 Version 3 Version 4 <p>The default version is Version 4.</p> <p><input type="checkbox"/> All the SNTP requests are sent out with the current configured version number. When required, the administrator can change the current version number.</p>
Addressing Mode	<p>Specifies the SNTP client addressing mode. Options are:</p> <ul style="list-style-type: none"> Unicast - SNTP client operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server. Broadcast - SNTP client operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.

Field	Description
	<ul style="list-style-type: none"> • Multicast - SNTP client operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates. • Anycast - SNTP client operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses. <p>The default addressing mode is Unicast.</p>
Sntp Client Port	Specifies the SNTP client port number. This value can be 123 or ranges between 1025 and 65535. The default value is 123.
Time Display Format	Specifies the time display format. Options are: <ul style="list-style-type: none"> • Hours – 24 hours format. • Am/Pm – 12 hours AM/PM format. <p>The default format is Hours.</p>
AuthKey Id	Specifies the key identifier identifying the cryptographic key used to generate the message-authentication code.
Auth Algorithm	Specifies the SNTP authentication algorithm. Options are: <ul style="list-style-type: none"> • None • md5 - Message Digest-5 • des - Data Encryption Standard <p>The default authentication algorithm is None.</p>
AuthKey	Specifies the authentication key that is used to implement NTP authentication.
TimeZone	Specifies the system time zone with respect to UTC. That is, plus indicates forward time zone and minus indicates backward time zone. The valid format is (+/-)HH:MM.
DST StartTime	Specifies the DST (Daylight Saving Time) start time. The valid format is [weekofmonth-weekofday-month, HH:MM]. <ul style="list-style-type: none"> <input type="checkbox"/> DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year.
DST EndTime	Specifies the DST end time. The valid format is [weekofmonth-weekofday-month, HH:MM].

3. Click **Apply** for the configuration to take effect.

3.11.2 SNTP Unicast

The **SNTP Unicast Table** page allows you to configure the SNTP unicast parameters.

To configure SNTP Unicast Table

1. Select **System > SNTP > SNTP Unicast** to open the **SNTP Unicast Table** page.

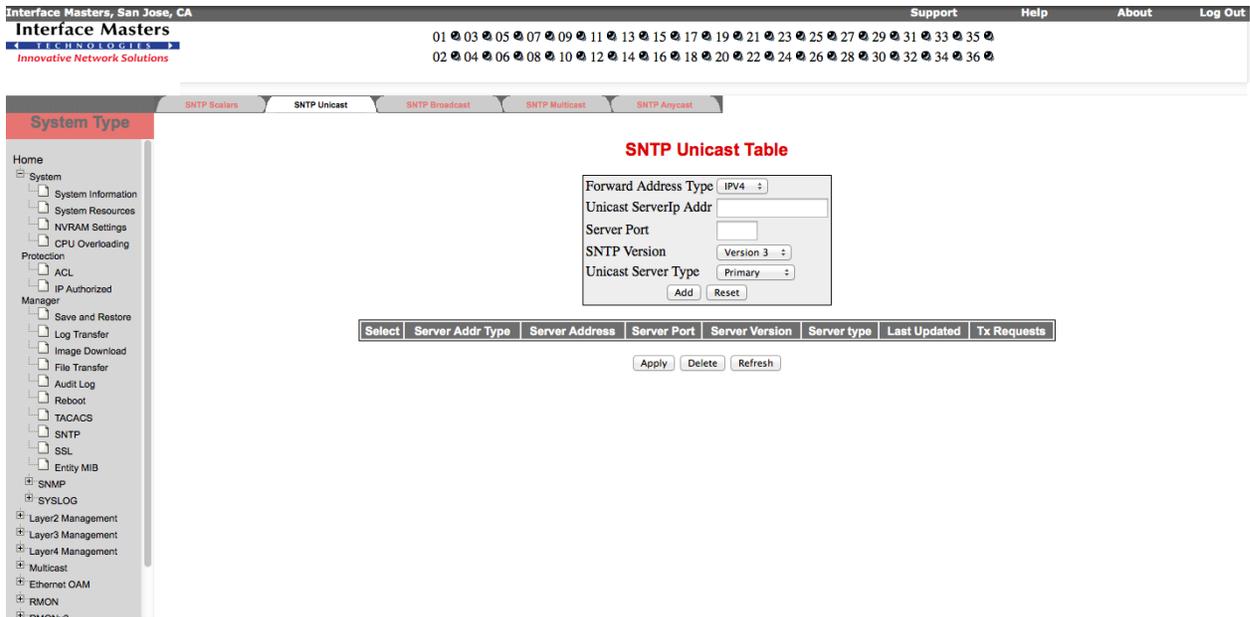


Figure 3-21: SNTP Unicast Table - System Group

2. Configure the parameters described in Table 3-17.

Table 3-17: SNTP Unicast Table

Field	Description
Forward Address Type	Specifies the address type of the unicast server in the Unicast addressing mode. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
Unicast ServerIp Addr	Specifies the unicast IPv4/IPv6 server address in the Unicast addressing mode.
Server Port	Specifies the SNTP port on which the server is UP. This value can be 123 or any value which ranges between 1025 and 65535.
SNTP Version	Specifies the SNTP version supported by the server. Options are: <ul style="list-style-type: none"> • Version 3 • Version 4
Unicast Server Type	Specifies the Unicast server type. Options are: <ul style="list-style-type: none"> • Primary - Primary server • Secondary - Secondary server
Last Updated	Specifies the local time when the system time was successful.
Tx Requests	Specifies the number of SNTP requests sent in the Unicast addressing mode.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.11.3 SNMP Broadcast

The **SNTP Broadcast Configuration** page allows you to configure the SNMP broadcast parameters.

To configure SNMP Broadcast Configuration

1. Select **System > SNMP > SNMP Broadcast** to open the **SNTP Broadcast Configuration** page.

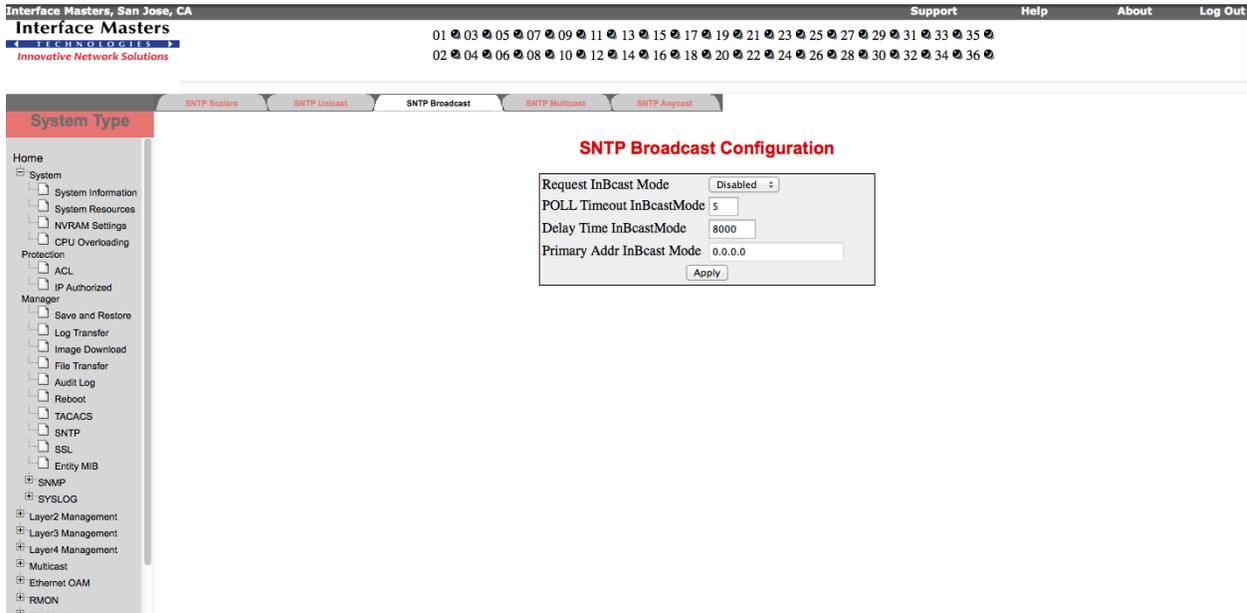


Figure 3-22: SNMP Broadcast Configuration - System Group

2. Configure the parameters described in Table 3-22.

Table 3-18: SNMP Broadcast Configuration

Field	Description
Request InBcast Mode	Specifies the SNMP send request status in Broadcast mode. Options are: <ul style="list-style-type: none"> • Enabled - The SNMP request is sent to the broadcast server to calculate the delay time. • Disabled - The SNMP request is not sent. By default, this is Disabled.
POLL Timeout InBcast Mode	Specifies the number of seconds to wait for a response from a SNMP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds. The default value is 5 seconds.
Delay Time InBcast Mode	Specifies the delay time when there is no response from the broadcast server. This value ranges between 1000 and 15000 microseconds. The default value is 8000 microseconds.
Primary Addr InBcast Mode	Specifies the primary server IP address learnt in Broadcast addressing mode. This is a read-only field. The default address is 0.0.0.0.

3. Click **Apply** for the configuration to take effect.

3.11.4 SNMP Multicast

The **SNMP Multicast Configuration** page allows you to configure the SNMP multicast parameters.

To configure SNMP Multicast Configuration

1. Select **System > SNMP > SNMP Multicast** to open the **SNMP Multicast Configuration** page.

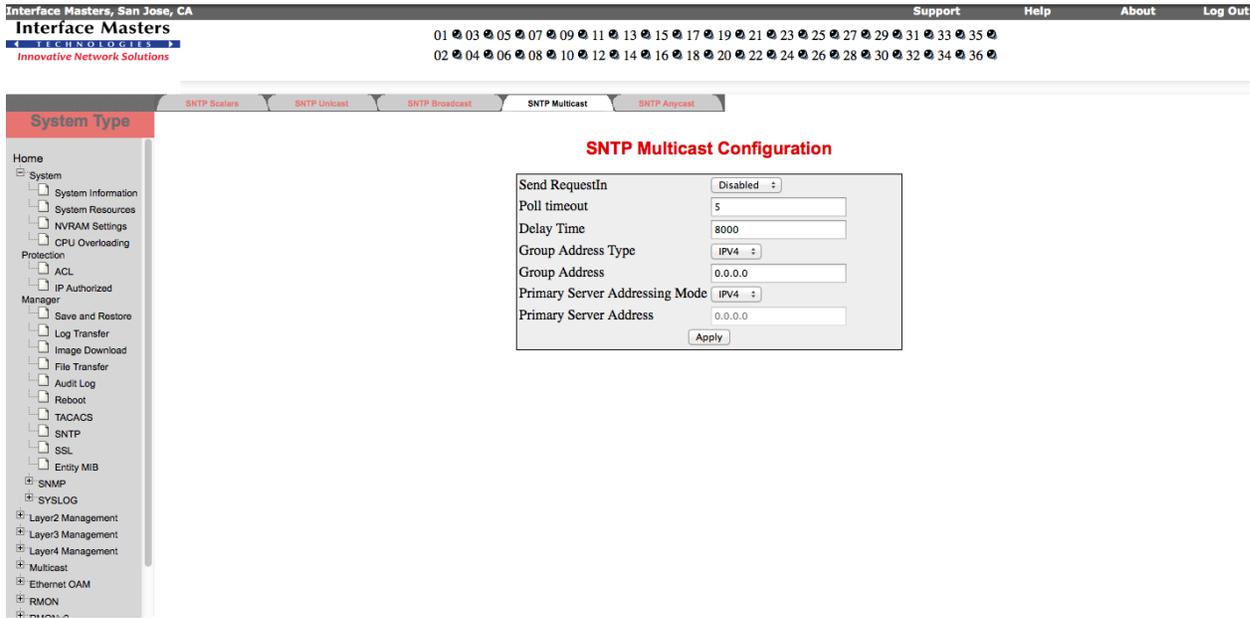


Figure 3-23: SNMP Multicast Configuration - System Group

2. Configure the parameters described in Table 3-19.

Table 3-19: SNMP Multicast Configuration

Field	Description
Send RequestIn	Specifies the SNMP send request status in Multicast mode. Options are: <ul style="list-style-type: none"> • Enabled - The SNMP request is sent to the multicast server to calculate the delay time. • Disabled - The SNMP request is not sent. By default, this is Disabled.
Poll timeout	Specifies the number of seconds to wait for a response from a SNMP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds. The default value is 5 seconds.
Delay Time	Specifies the delay time when there is no response from the multicast server. This value ranges between 1000 and 15000 microseconds. The default value is 8000 microseconds.
Group Address Type	Specifies the multicast group address type that can be configured by the administrator. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6

Field	Description
Group Address	Specifies the multicast group address that can be configured by the administrator.
Primary Server Addressing Mode	Specifies the address type of the primary server learnt in Multicast addressing mode. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
Primary Server Address	Specifies the primary server IP address learnt in Multicast addressing mode. This is a read-only field. The default address is 0.0.0.0.

3. Click **Apply** for the configuration to take effect.

3.12 SNMP

The SNMP is a widely deployed protocol that is commonly used to monitor and manage network devices.

The **SNMP** link opens the **SNMP Agent Control Settings** page that allows you to configure the SNMP Agent settings. The sub links of the SNMP are classified as follows:

- AGENT
- AGENTX

To configure SNMP Agent Control Settings

1. Select **System > SNMP** to open **SNMP Agent Control Settings** page.

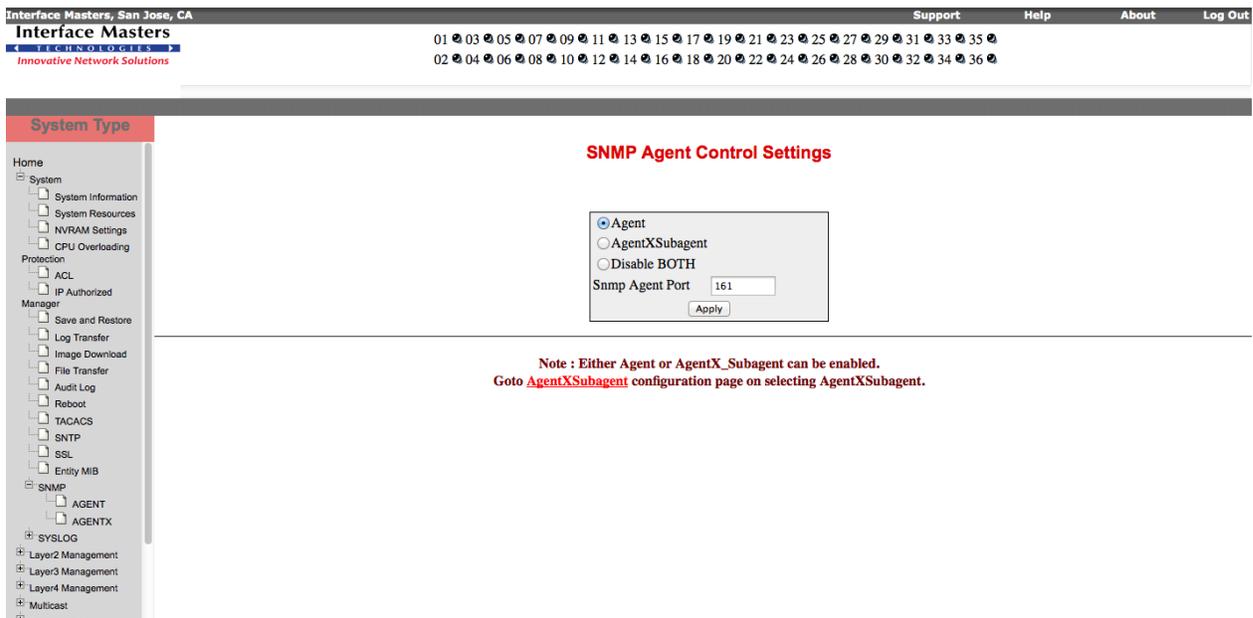


Figure 3-24: SNMP Agent Control Settings – System Group

2. Select Agent or AgentXSubagent or Disable BOTH.

- Specify the port number on which the agent should listen. The default port number is 161.
- Click **Apply** for the configuration to take effect.

3.12.1 AGENT

The **AGENT** link allows you to configure SNMP Agent related configuration through the following links:

- Community
- Group
- Group Access
- View
- Target Address
- TargetParameter
- User
- Trap Manager

By default, the **SNMP Community Settings** page is loaded.

3.12.1.1 Community

The **SNMP Community Settings** page displays the access permissions of the already configured SNMP Managers. This page allows you to add new managers to the table and delete existing managers from the same.

To configure SNMP Community Settings

- Select **System > SNMP > AGENT** to open **SNMP Community Settings** page.

The screenshot shows the 'SNMP Community Settings' page in the Interface Masters web interface. The page has a top navigation bar with 'Support', 'Help', 'About', and 'Log Out' links. Below the navigation bar is a breadcrumb trail: 'System > SNMP > AGENT'. The main content area is divided into two sections: a form for adding new community settings and a table of existing settings.

SNMP Community Settings Form:

- Community Index:
- Community Name:
- Security Name:
- Context Name:
- Transport Tag:
- Storage Type:
- Buttons:

SNMP Community Settings Table:

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

Buttons:

Figure 3-25: SNMP Community Settings - System Group

2. Configure the attributes described in Table 3-20.

Table 3-20: Community Settings

Field Name	Description
Community Index	Specifies the Index to the community table. Default index is NETMAN/PUBLIC.
Community Name	Specifies the community name. Default community name is NETMAN/PUBLIC.
Security Name	Specifies the security name. Default security name is None.
Context Name	Specifies the context name. Default context name is Null.
Transport Tag	Specifies the transport tag. Default transport tag is Null.
Storage Type	<p>Specifies the required Storage type for the User-Group combination. Options are:</p> <ul style="list-style-type: none"> • Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. • Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system. <p>Default storage type is Volatile.</p>

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.2 Group

The **SNMP GROUP Settings** page allows you to map a combination of Security Model and Security Name into a Group Name, which is used to define an access control policy.

To configure SNMP GROUP Settings

1. Select **System > SNMP > AGENT > Group** to open the **SNMP GROUP Settings** page.

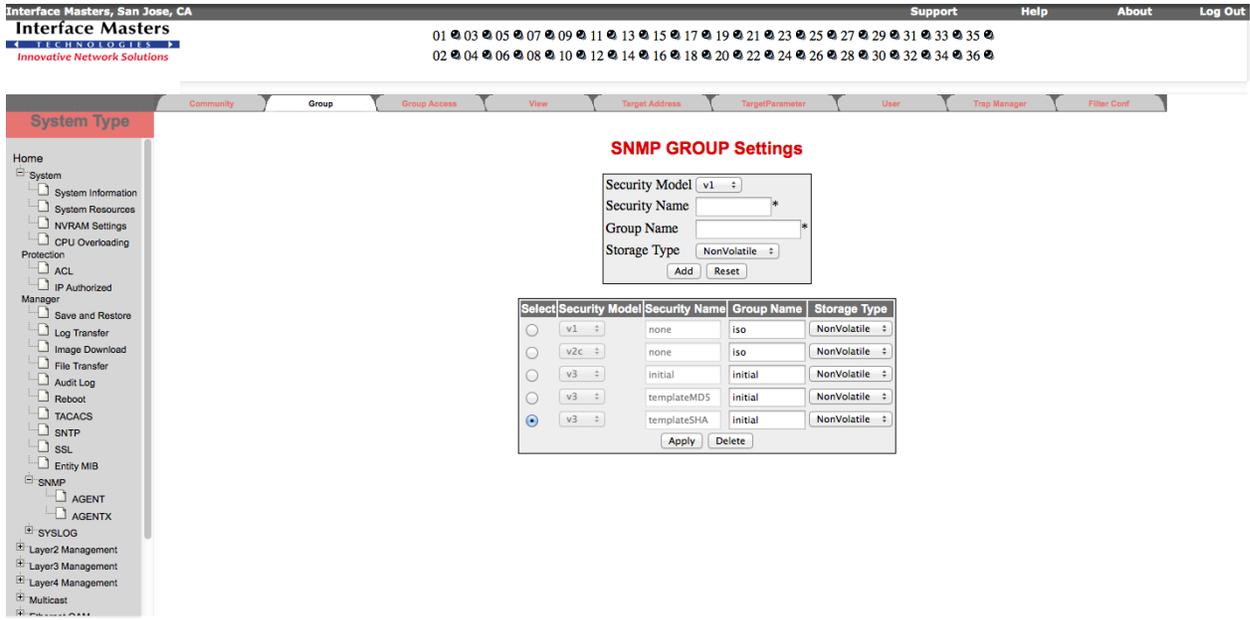


Figure 3-26: SNMP GROUP Settings - System Group

2. Configure the attributes described in Table 3-21.

Table 3-21: Group Settings

Field Name	Description
Security Model	Specifies the version of the SNMP. Options are: <ul style="list-style-type: none"> • v1 • v2c • v3
Security Name	Specifies the security name of the group.
Group Name	Specifies the name of the SNMP group. Default group name is iso/initial.
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> • Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. • Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.3 Group Access

The **SNMP Group Access Settings** page allows you to configure the access rights of groups.



A SNMP Group has to be created prior to the Group Access configuration.

To configure SNMP Group Access Settings

1. Select **System > SNMP > AGENT > Group Access** to open the **SNMP Group Access Settings** page.

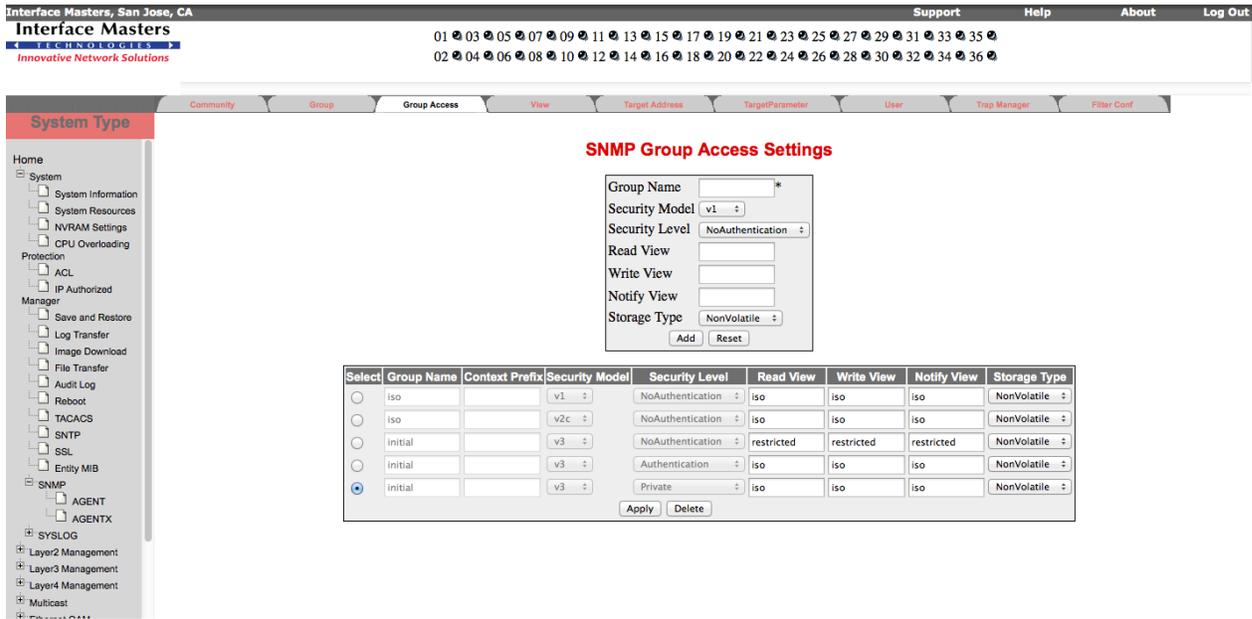


Figure 3-27: SNMP Group Access Settings - System Group

2. Configure the attributes described in Table 3-22.

Table 3-22: SNMP Group Access Settings

Field Name	Description
Group Name	Specifies the name of the group.
Context Prefix	Specifies a string representing a context name or collection of context names.
Security Model	Specifies the version of the SNMP. Options are: <ul style="list-style-type: none"> • v1 • v2c • v3
Security Level	Specifies the version of the SNMP. Options are: <ul style="list-style-type: none"> • NoAuthentication – No authentication. • Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. • Private - Both authentication and privacy.
Read View	Specifies the read view identifier.
Write View	Specifies the write view identifier.
Notify View	Specifies the notify view identifier.

Field Name	Description
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> • Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. • Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.4 View

The **SNMP ViewTree Settings** page allows you to configure SNMP View information.



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

To configure SNMP ViewTree Settings

1. Select **System > SNMP > AGENT > View** to open the **SNMP ViewTree Settings** page.

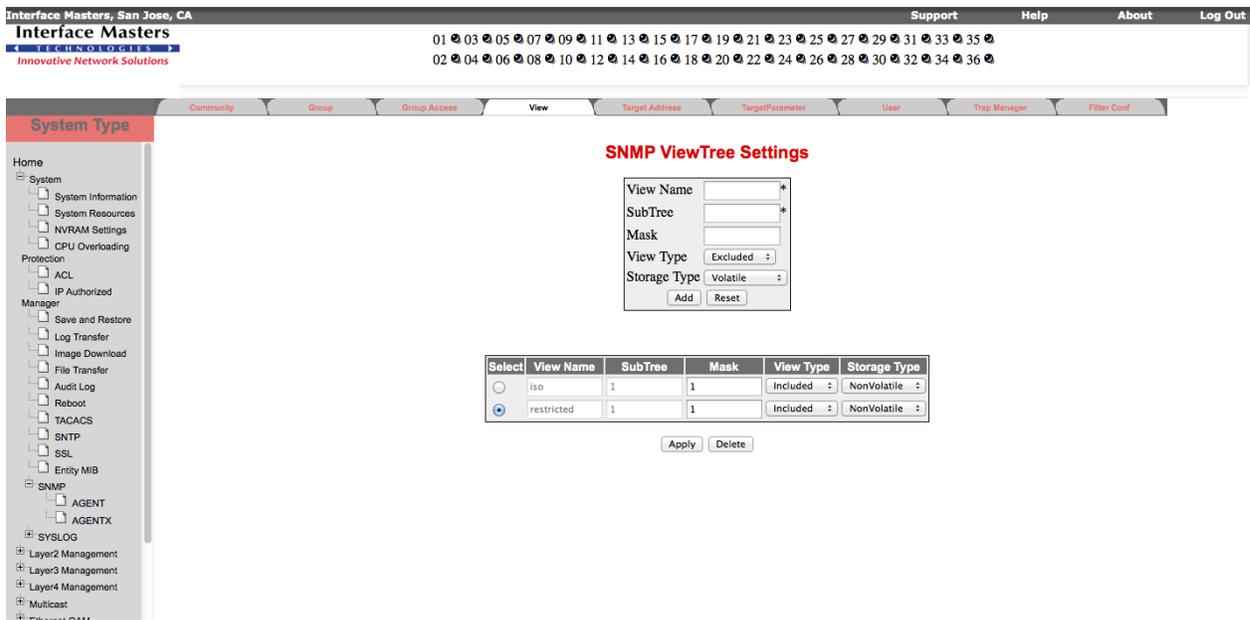


Figure 3-28: SNMP View Tree Settings - System Group

2. Configure the attributes described in Table 3-23.

Table 3-23: SNMP View Tree Settings

Field Name	Description
View Name	Specifies the View Name for which the view details are to be configured.
SubTree	Specifies the Sub Tree value for the particular view.
Mask	Specifies the Mask value for the particular view.
View Type	Specifies the View Type. Options are: <ul style="list-style-type: none"> Included – Allows access to the subtree. Excluded – Denies access to the subtree.
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.5 Target Address

The **SNMP Target Address Settings** page allows you to configure the following information:

To configure SNMP Target Address Settings

1. Select **System > SNMP > AGENT > Target Address** to open the **SNMP Target Address Settings** page.

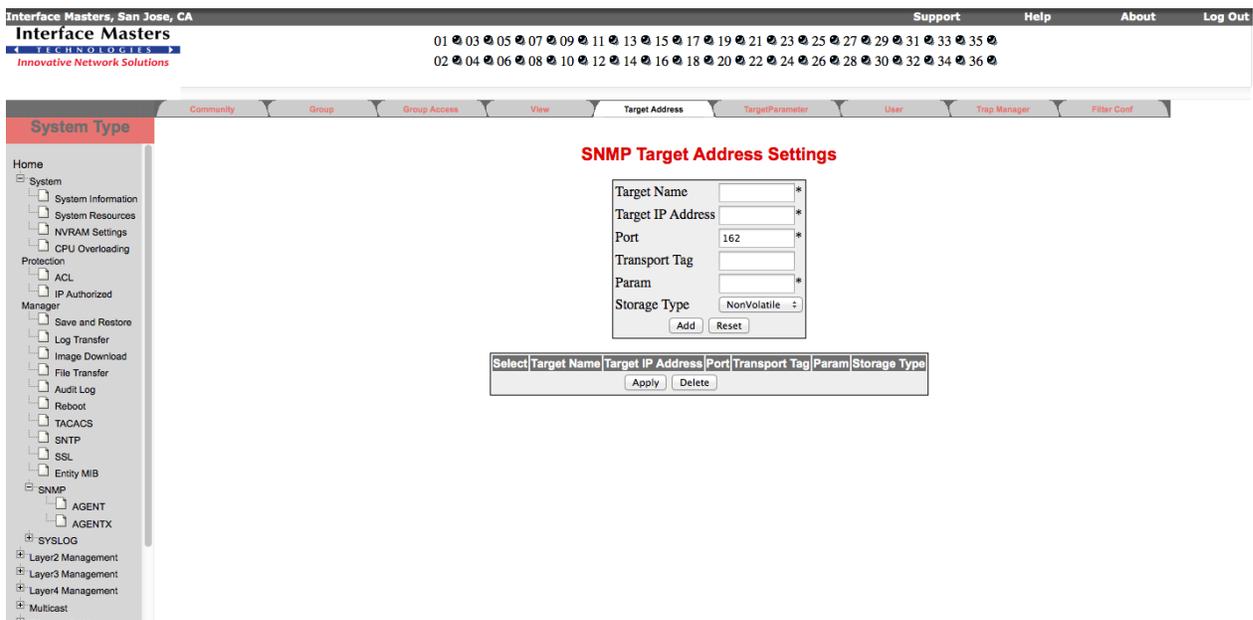


Figure 3-29: SNMP Target Address Settings - System Group

2. Configure the attributes described in Table 3-24.

Table 3-24: SNMP Target Address Settings

Field Name	Description
Target Name	Specifies a unique identifier of the Target.
Target IP Address	Specifies a target address to be used in the generation of SNMP operations.
Transport tag	Selects the target address for a particular operation.
Param	Contains SNMP parameters to be used when generating messages to be sent to transport address.
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> • Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. • Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

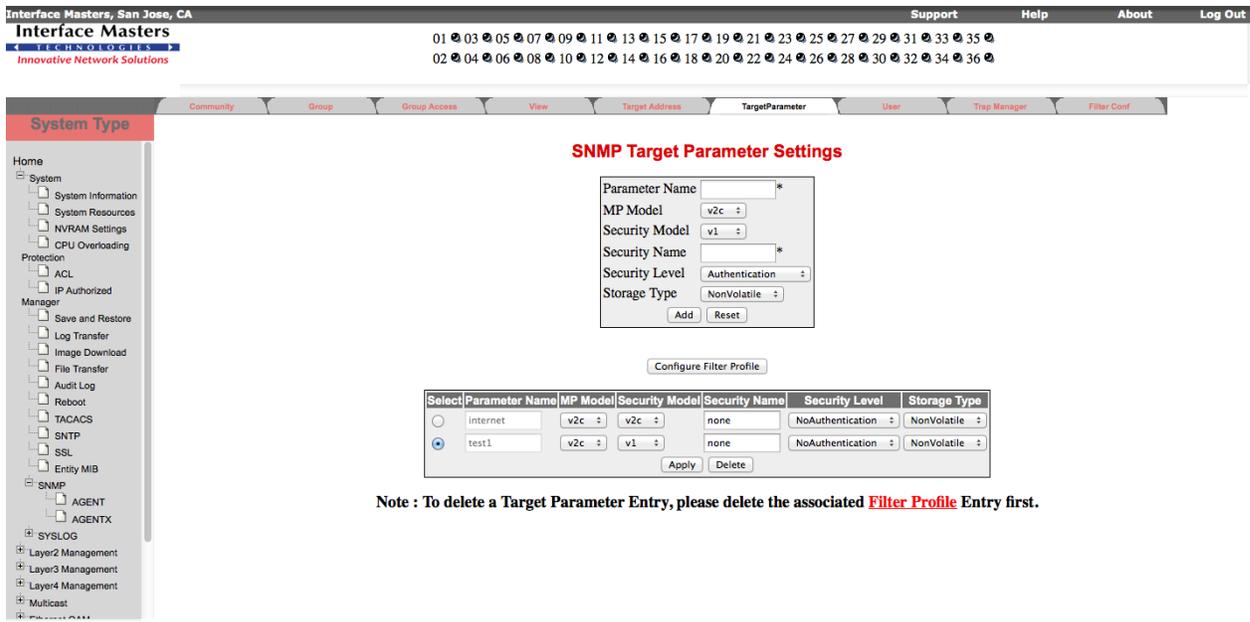
3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.6 TargetParameter

The **SNMP Target Param Settings** page specifies SNMP target information to be used in the generation of SNMP messages.

To configure SNMP Target Param Settings

1. Select **System > SNMP > AGENT > TargetParameter** to open the **SNMP Target Param Settings** page.



Note : To delete a Target Parameter Entry, please delete the associated Filter Profile Entry first.

Figure 3-30: SNMP Target Param Settings - System Group

2. Configure the attributes described in Table 3-25.

Table 3-25: SNMP Target Param Settings

Field Name	Description
Parameter Name	Specifies a unique identifier of the parameter.
MP Model	Specifies the MP model of the SNMP. Options are: <ul style="list-style-type: none"> v1 v2c v3
Security Model	Specifies the version of the SNMP. Options are: <ul style="list-style-type: none"> v1 v2c v3
Security Name	Identifies the current Param Name, on whose behalf SNMP messages will be generated.
Security Level	Specifies the level of security to be used when generating SNMP messages. Options are: <ul style="list-style-type: none"> NoAuthentication – No authentication. Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. Private - Both authentication and privacy.
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. Non Volatile – Storage type is permanent. Saves the configuration to the system.

Field Name	Description
	You can view the Saved configuration on restarting the system.
	<ol style="list-style-type: none"> 3. Click Add to save the entry. If you wish to discard the information you have entered, click Reset. 4. Select the required entry. Modify the parameters and click Apply for the configuration to take effect. 5. Select the required entry and click Delete for the entry to be deleted.

3.12.1.7 User

The **SNMP Security Settings** page specifies a user configured in the SNMP for the User-based Security Model.

To configure SNMP Security Settings

1. Select **System > SNMP > AGENT > User** to open the **SNMP Security Settings** page.

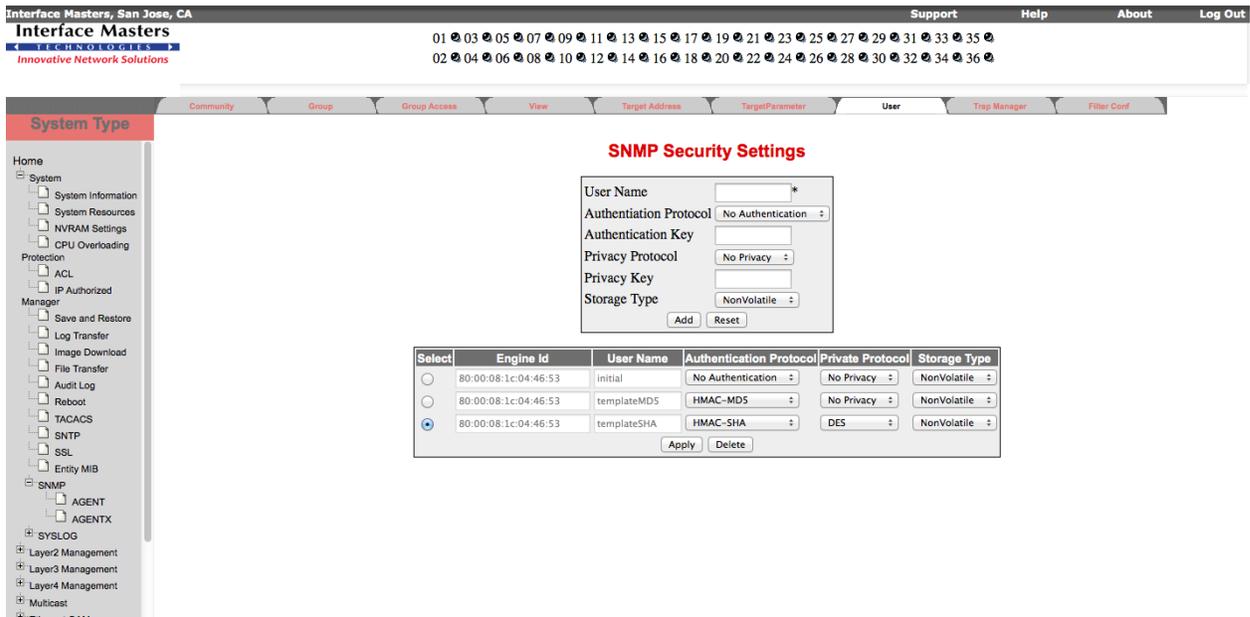


Figure 3-31: SNMP Security Settings - System Group

2. Configure the attributes described in Table 3-26.

Table 3-26: SNMP Security Settings

Field Name	Description
User Name	Specifies the User-based Security Model dependent security ID.
Engine Id	Specifies the administratively unique identifier of an SNMP engine, and is used for identification, not for addressing.
Authentication Protocol	Specifies the type of authentication protocol used for authentication. Options are: <ul style="list-style-type: none"> • No Authentication – No Authentication. • HMAC-MD5 – Message Digest 5 based authentication.

Field Name	Description
	<ul style="list-style-type: none"> HMAC-SHA – Security Hash Algorithm based authentication.
Authentication Key	Specifies the secret authentication key used for messages sent on behalf of this user to/from the SNMP.
Privacy Protocol	Specifies the type of protocol to be is used in this case. Options are: <ul style="list-style-type: none"> No Privacy DES
Privacy Key	Indicates whether messages sent on behalf of a user to/from the SNMP, can be protected from disclosure.
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

3.12.1.8 Trap Manager

The **SNMP TRAP Settings** page allows you to configure set of management targets to receive notifications.

To configure SNMP TRAP Settings

- Select **System > SNMP > AGENT > Trap Manager** to open the **SNMP TRAP Settings** page.

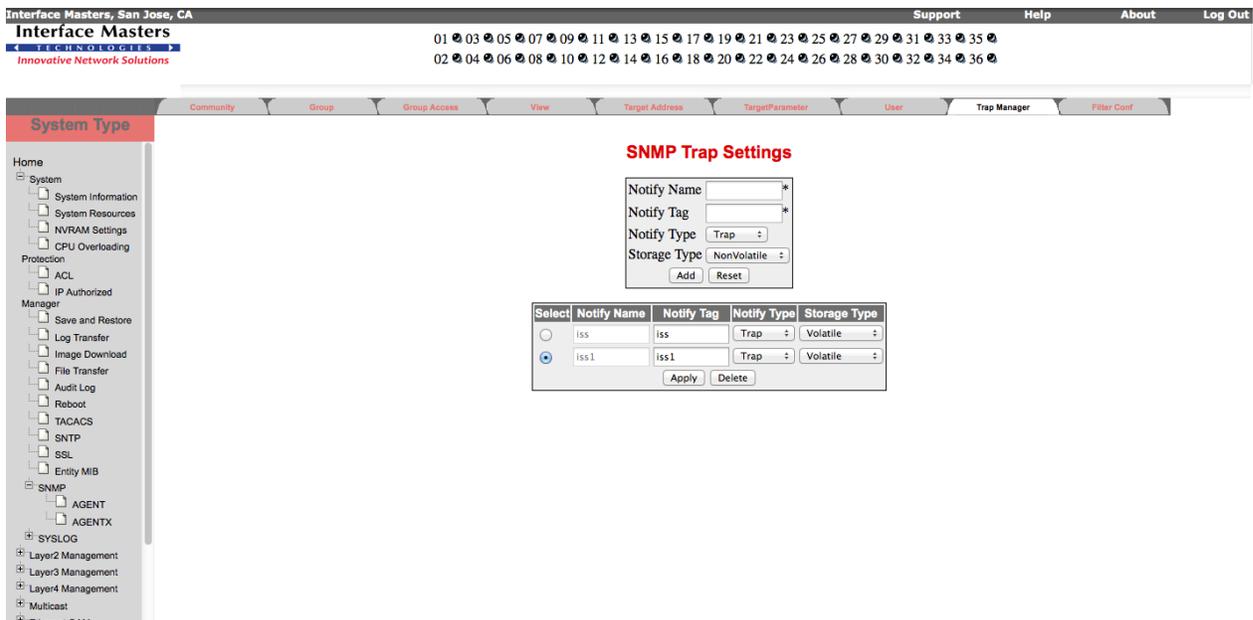


Figure 3-32: SNMP Trap Settings - System Group

2. Configure the attributes described in Table 3-27.

Table 3-27: SNMP Trap Settings

Field Name	Description
Notify Name	Specifies a unique identifier associated with the entry.
Notify Tag	Specifies the notification tag, which is used to select entries in the Target Address Table.
Notify Type	Specifies the notification type. Options are: <ul style="list-style-type: none"> • Inform • Trap
Storage Type	Specifies the required Storage type for the User-Group combination. Options are: <ul style="list-style-type: none"> • Volatile – Storage type is temporary. Erases the configuration setting on restarting the system. • Non Volatile – Storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.12.2 AGENTX

The **SNMP Agentx Subagent Settings** page allows you to configure the following:

To configure SNMP Agentx Subagent Settings

1. Select **System > SNMP > AGENTX** to open the. **SNMP Agentx Subagent Settings** page.

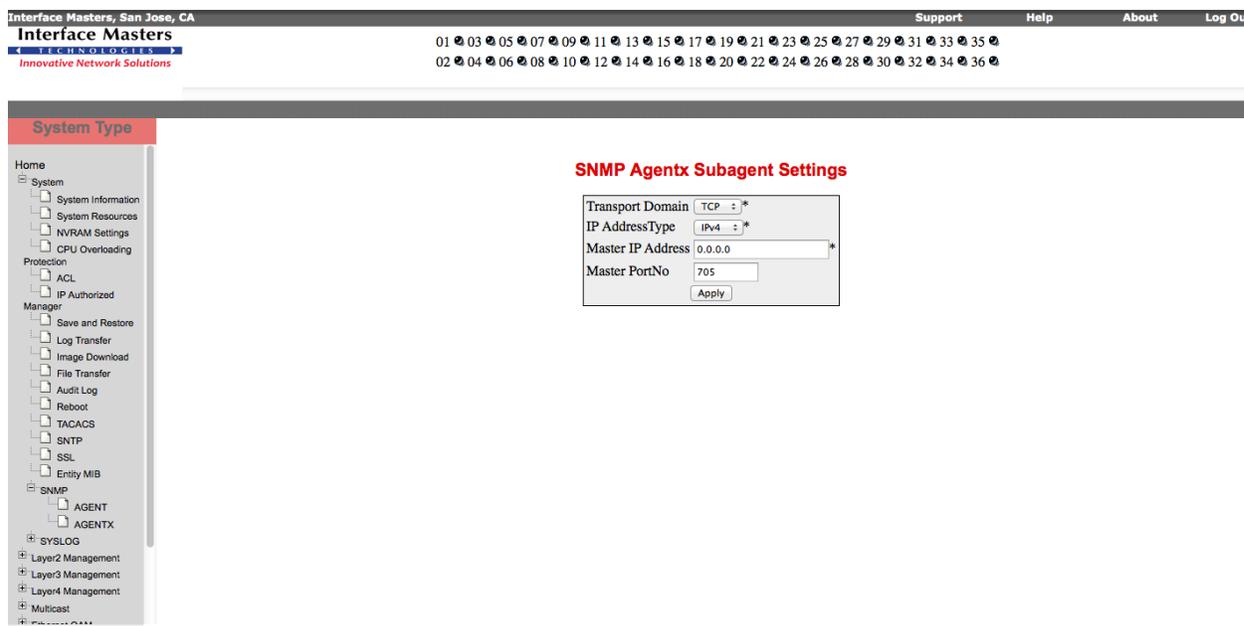


Figure 3-33: SNMP Agentx Subagent Settings – System Group

- Configure the attributes described in Table 3-28.

Table 3-28: SNMP Agentx Subagent Settings

Field Name	Description
Transport Domain	Specifies the transport domain to be used.
IP AddressType	Specifies the address type. Options are: <ul style="list-style-type: none"> IPv4 IPv6
Master IP Address	Specifies the master IP address.
Master PortNo	Specifies the master port number.

- Click **Apply** for the configuration to take effect.

3.13 SYSLOG

Syslog is a protocol used to capture log information for 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.

One of the fundamental qualities of the Syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

The **SYSLOG** link opens the **SYSLOG Settings** page.

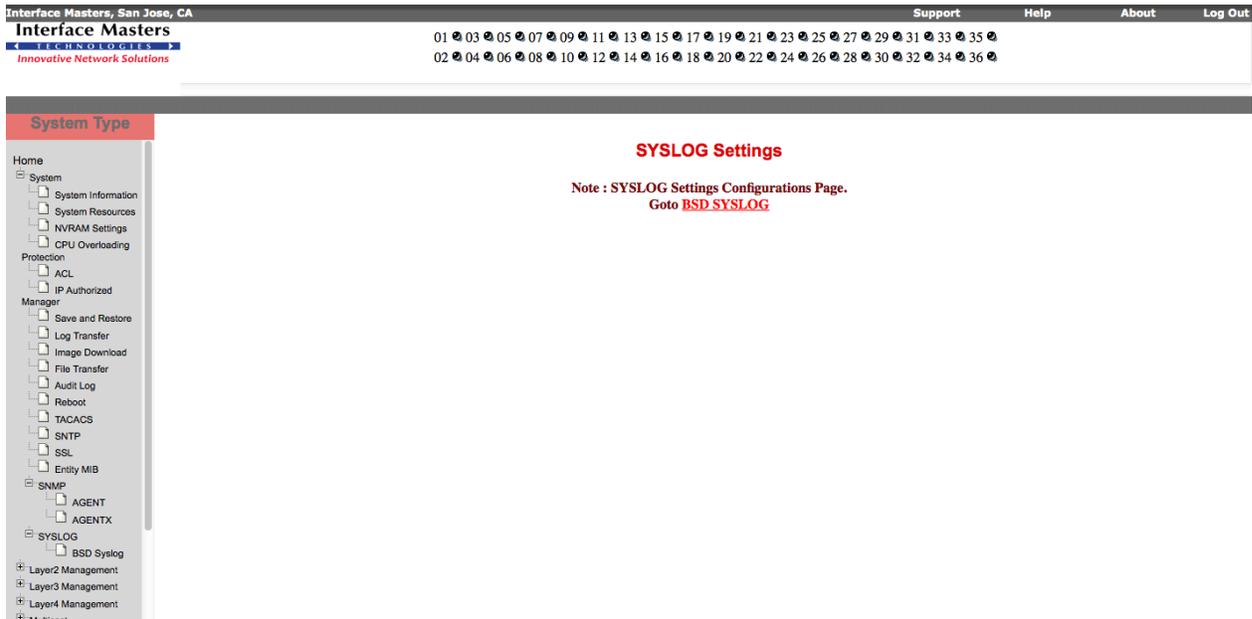


Figure 3-34: SYSLOG Settings – System Group

3.13.1 BSD Syslog

The **BSD Syslog** link allows you to configure BSD Syslog related configuration through the following links:

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

By default, the **BSD Syslog Settings** page is loaded.

3.13.1.1 SYSLOG ScalarsConf

The **BSD Syslog Settings** page allows you to configure the BSD syslog settings.

To configure BSD Syslog Settings

1. Select **System > SYSLOG > BSD Syslog** to open the **BSD Syslog Settings** page.

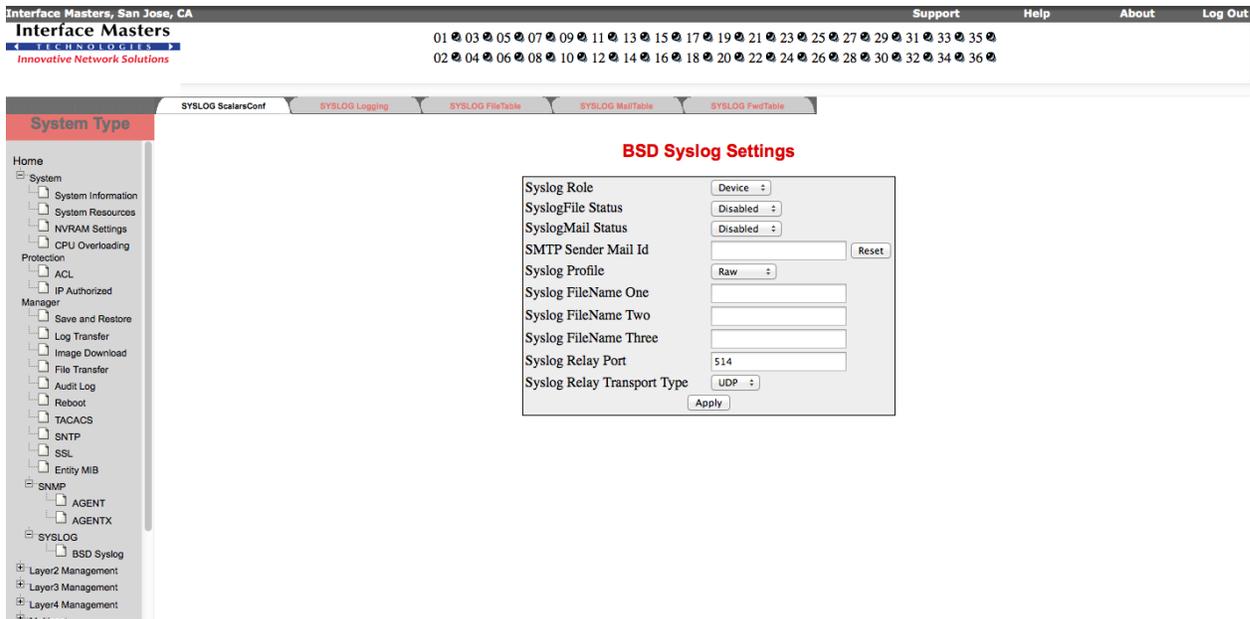


Figure 3-35: BSD Syslog Settings – System Group

2. Configure the attributes described in Table 3-29.

Table 3-29: BSD Syslog Settings

Field Name	Description
Syslog Role	<p>Specifies the syslog role. Options are:</p> <ul style="list-style-type: none"> • Device - Generates and forwards the syslog message. • Relay - Receives, generates and forwards the syslog messages. Checks whether the received packet is as per BSD Syslog format. If not, makes the message to BSD Syslog format and forwards. <p>Default role is Device.</p>
SyslogFile Status	<p>Enables / disables the syslog local storage. Options are:</p> <ul style="list-style-type: none"> • Enabled – Enables the syslog local storage. • Disabled – Disables the syslog local storage. <p>By default, the status is Disabled.</p>
SyslogMail Status	<p>Enables / disables the syslog mail storage. Options are:</p> <ul style="list-style-type: none"> • Enabled – Enables the syslog mail storage. • Disabled – Disables the syslog mail storage. <p>By default, the status is Disabled.</p>
Syslog Profile	<p>Specifies the syslog profile for beep. Options are:</p> <ul style="list-style-type: none"> • Raw - Raw syslog profile. • Cooked - Cooked syslog profile. <p>By default, the beep profile is Raw.</p>
Syslog FileName One	<p>Specifies the first file where the syslog can store the messages locally.</p>
Syslog FileName	<p>Specifies the second file where the syslog can store the messages locally.</p>

Field Name	Description
Two	
Syslog FileName Three	Specifies the third file where the syslog can store the messages locally.

3. Click **Apply** for the configuration to take effect.

3.13.1.2 SYSLOG FileTable

The **BSD Syslog File Table** page allows you to configure the BSD syslog file table settings.

To configure BSD Syslog File Table

1. Select **System > SYSLOG > BSD Syslog > SYSLOG FileTable** to open the **BSD Syslog File Table** page.

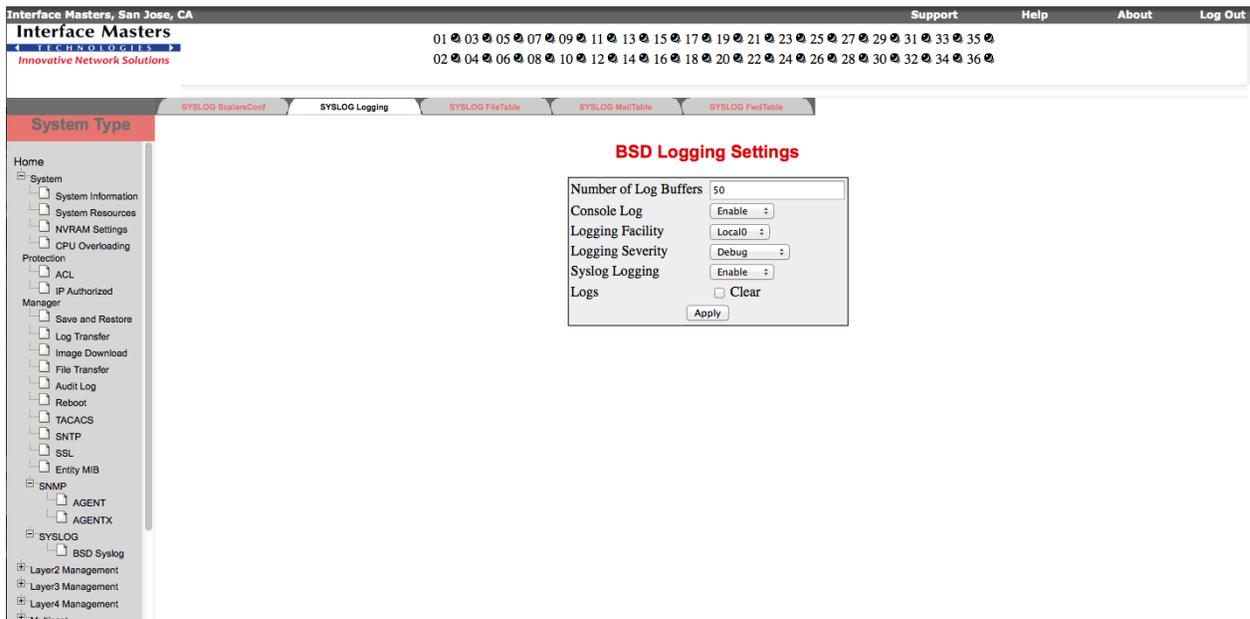


Figure 3-36: BSD Syslog File Table – System Group

2. Configure the attributes described in Table 3-30.

Table 3-30: BSD Syslog File Table

Field Name	Description
File Priority	Specifies the priority for which it should be written in file. This value ranges between 0 and 191.
File Name	Specifies the file name to which the syslog message is written.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry and click **Delete** for the entry to be deleted.

3.13.1.3 SYSLOG MailTable

The **BSD Syslog MailTable** page allows you to configure the BSD syslog mail table settings.

To configure BSD Syslog MailTable

1. Select **System > SYSLOG > BSD Syslog > SYSLOG MailTable** to open the **BSD Syslog MailTable** page.

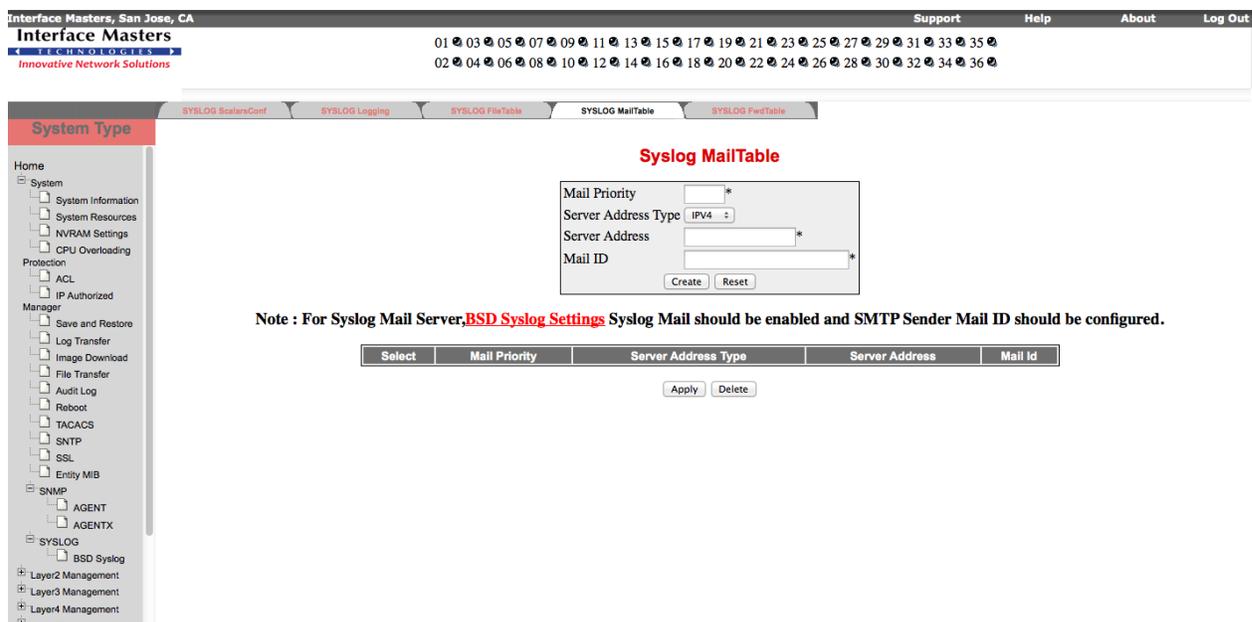


Figure 3-37: BSD Syslog MailTable – System Group

2. Configure the attributes described in Table 3-31.

Table 3-31: BSD Syslog MailTable

Field Name	Description
Mail Priority	Specifies the priority which is to be mailed. This value ranges between 0 and 191.
Server Address Type	Specifies the mail server address type. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
Server Address	Specifies the mail server IP.
Mail ID	Specifies the receiver mail ID.

3. Click **Create** to save the entry. If you wish to discard the information you have entered, click **Reset**.

4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

3.13.1.4 SYSLOG FwdTable

The **Syslog FwdTable** page allows you to configure the syslog forward table settings.

To configure Syslog FwdTable

1. Select **System > SYSLOG > BSD Syslog > SYSLOG FwdTable** to open the **Syslog FwdTable** page.

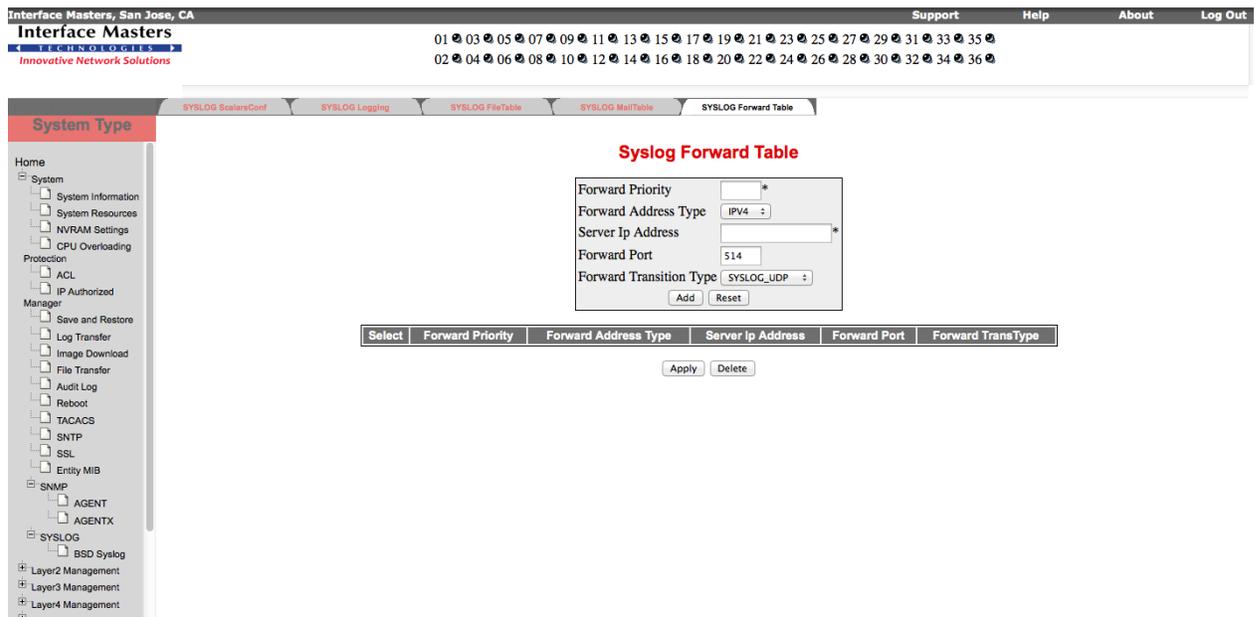


Figure 3-38: Syslog FwdTable – System Group

2. Configure the attributes described in Table 3-32.

Table 3-32: Syslog FwdTable

Field Name	Description
Fwd Priority	Specifies the priority which is to be forwarded to the desired server. This value ranges between 0 and 191.
Forward Address Type	Specifies the address type of the server. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
Server Ip Address	Specifies the server IP to which the syslog is to be forwarded.
Fwd Port	Specifies the port through which it can send the syslog message. This value ranges between 0 and 65535. Default value is 514.
Fwd Transition Type	Specifies the transport type using which it can send syslog message. Options are: <ul style="list-style-type: none"> • SYSLOG_UDP

Field Name	Description
	<ul style="list-style-type: none"> • SYSLOG_TCP • SYSLOG_BEEP <p>The default transition type is SYSLOG_UDP.</p>
	<ol style="list-style-type: none"> 3. Click Add to save the entry. If you wish to discard the information you have entered, click Reset. 4. Select the required entry. Modify the parameters and click Apply for the configuration to take effect. 5. Select the required entry and click Delete for the entry to be deleted.

Chapter

4

Layer2 Management

This chapter describes the configuration of the various features of the Layer-2 interfaces.

The **Layer2 Management** link on the left pane opens the **Layer2 Management** page. This page provides the following links:

- Port Manager
- VLAN
- VLAN SUBNET
- Dynamic VLAN
- MSTP
- RSTP
- LA
- 802.1x
- Filters

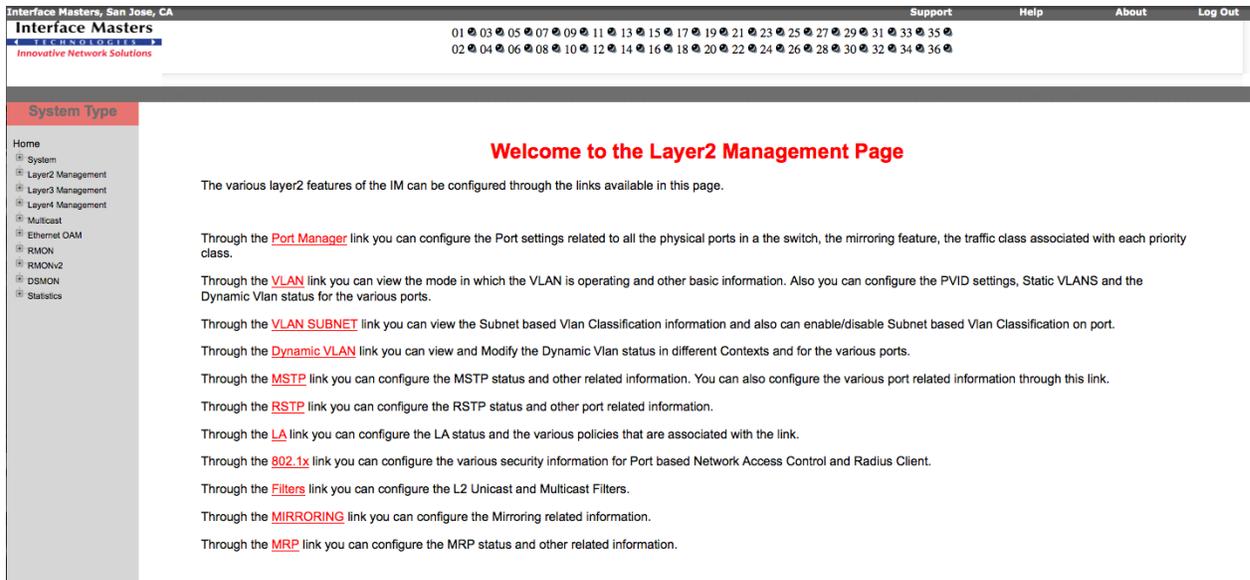


Figure 4-1: Layer2 Management Page

4.1 Port Manager

The **Port Manager** link allows you to configure port related parameters through the following links:

- Basic Settings
- Port Monitoring
- Traffic Class
- Port Control
- Rate Limiting

By default, the **Port Basic Settings** page is loaded.

4.1.1 Basic Settings

The **Port Basic Settings** page displays the general information related to all the physical ports in a switch.

To configure Port Basic Settings

1. Select **Layer2 Management > Port Manager** to open the **Port Basic Settings** page.

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"/>	Ex0/1	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:94
<input type="radio"/>	Ex0/2	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:95
<input type="radio"/>	Ex0/3	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:96
<input type="radio"/>	Ex0/4	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:97
<input type="radio"/>	Ex0/5	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:98
<input type="radio"/>	Ex0/6	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:99
<input type="radio"/>	Ex0/7	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9a
<input type="radio"/>	Ex0/8	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9b
<input type="radio"/>	Ex0/9	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9c
<input type="radio"/>	Ex0/10	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9d
<input type="radio"/>	Ex0/11	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9e
<input type="radio"/>	Ex0/12	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:9f
<input type="radio"/>	Ex0/13	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a0
<input type="radio"/>	Ex0/14	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a1
<input type="radio"/>	Ex0/15	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a2
<input type="radio"/>	Ex0/16	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a3
<input type="radio"/>	Ex0/17	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a4
<input type="radio"/>	Ex0/18	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a5
<input type="radio"/>	Ex0/19	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a6
<input type="radio"/>	Ex0/20	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a7
<input type="radio"/>	Ex0/21	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a8
<input type="radio"/>	Ex0/22	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:a9
<input type="radio"/>	Ex0/23	Down	Down	CustomerBridgePort	0	Hybrid	1500	Enabled	Switch Port	00:00:bd:83:92:aa

Figure 4-2: Port Basic Settings - Layer 2 Group

2. Configure the attributes described in Table 4-1.

Table 4-1: Port Basic Settings

Field	Description
Port	Specifies the Port Number.
Link Status	Specifies the Link State. <ul style="list-style-type: none"> Green arrow – The admin status of the port is up. Red arrow – The admin status of the port is down.
Admin State	Specifies the Admin State of the port. Options are: <ul style="list-style-type: none"> Up – Makes the admin status of the port Up. Down – Makes the admin status of port Down.
Bridge Port Type	Specifies the bridge port type. Options are: <ul style="list-style-type: none"> providerNetworkPort customerNetworkPortPortBased customerNetworkPortStaged customerEdgePort propCustomerEdgePort propCustomerNetworkPort propProviderNetworkPort customerBridgePort None
Default User Priority	Specifies the Default User Priority value. This value ranges between zero and seven. Default value is 0.

Field	Description
Switch Port Mode	Specifies the switch port mode. Options are: <ul style="list-style-type: none"> • Access • Trunk • Hybrid
MTU	Specifies the Maximum Transmittable Unit of the port. This value ranges between 90 and 9202.
Link Up/Down Trap	Specifies the Link Up/Down Trap status. Options are: <ul style="list-style-type: none"> • Enabled – Enables the Link Up/Down Trap status. • Disabled – Disables the Link Up/Down Trap status.

3. Click **Apply** for the configuration to take effect.



You can change any of the parameters mentioned in this page at any time.

4.1.2 Port Monitoring

The **Port Monitoring** page allows you to enable/disable Port Monitoring feature at every port level.

To configure Port Monitoring

1. Select **Layer2 Management > Port Manager > Port Monitoring** to open the **Port Monitoring** page.

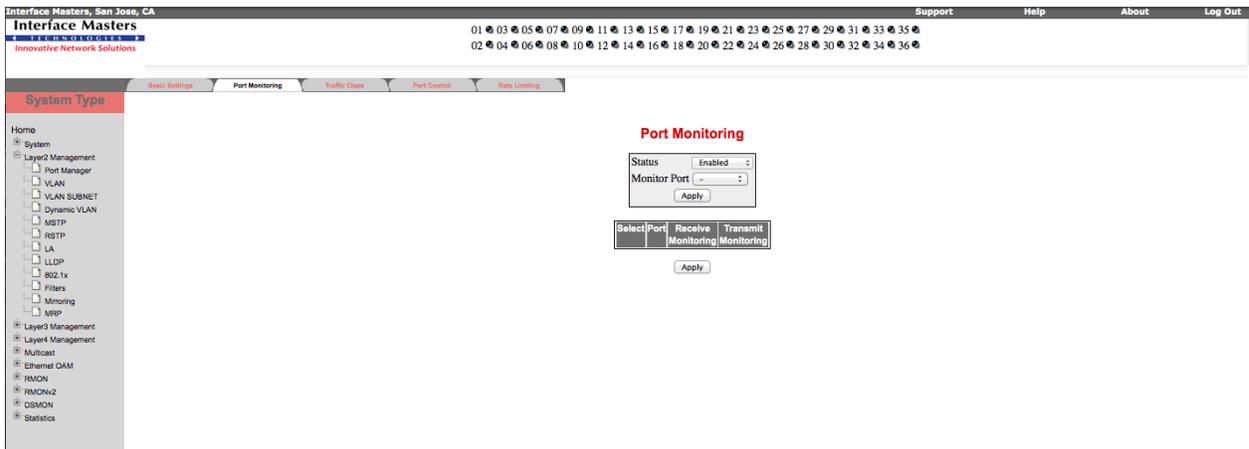


Figure 4-3: Port Monitoring - Layer 2 Group

2. Configure the attributes described in Table 4-2.

Table 4-2: Port Monitoring

Field	Description
Status	Specifies the Port Monitoring status. Options are: <ul style="list-style-type: none"> • Enabled

Field	Description
	<ul style="list-style-type: none"> Disabled By default, the status is disabled.
Monitor Port	Specifies the port number for which the monitoring status is to be changed.
Port	Specifies the port number. The port number ranges between 1 and 65535.
Receive Monitoring	Specifies the monitoring of the Receive packet direction for the port. Options are: <ul style="list-style-type: none"> Enabled Disabled By default, the Receive Monitoring status is disabled.
Transmit Monitoring	Specifies the monitoring of the Transmit packet direction for the port. Options are: <ul style="list-style-type: none"> Enabled Disabled By default, the Transmit Monitoring status is disabled.

3. Click **Apply** for the configuration to take effect.

4.1.3 Traffic Class

The **VLAN Traffic Class Mapping** page allows you to configure the traffic classes associated with each priority class on all ports.

To configure VLAN Traffic Class Mapping

1. Select **Layer2 Management > Port Manager > Traffic Class** to open the **VLAN Traffic Class Mapping** page.

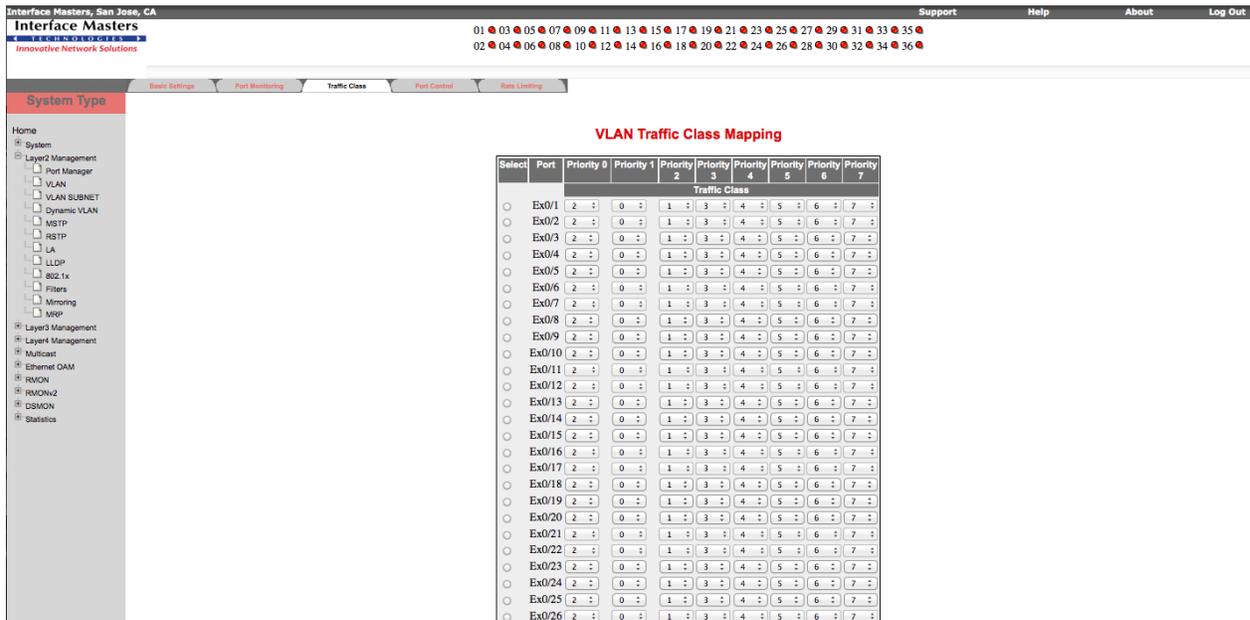


Figure 4-4: VLAN Traffic Class Mapping - Layer 2 Group

2. Configure the attributes described in Table 4-3.

Table 4-3: VLAN Traffic Class Mapping

Field	Description
Port	Specifies the port number. This is a read-only field.
Traffic Class	Specifies the traffic class value for the given priority and port. Traffic Class values range between zero and seven.

3. Click **Apply** for the configuration to take effect.

4.1.4 Port Control

The **Port Control** page allows you to configure the port specific parameters of the device.

To configure Port Control

1. Select **Layer2 Management > Port Manager > Port Control** to open the **Port Control** page.

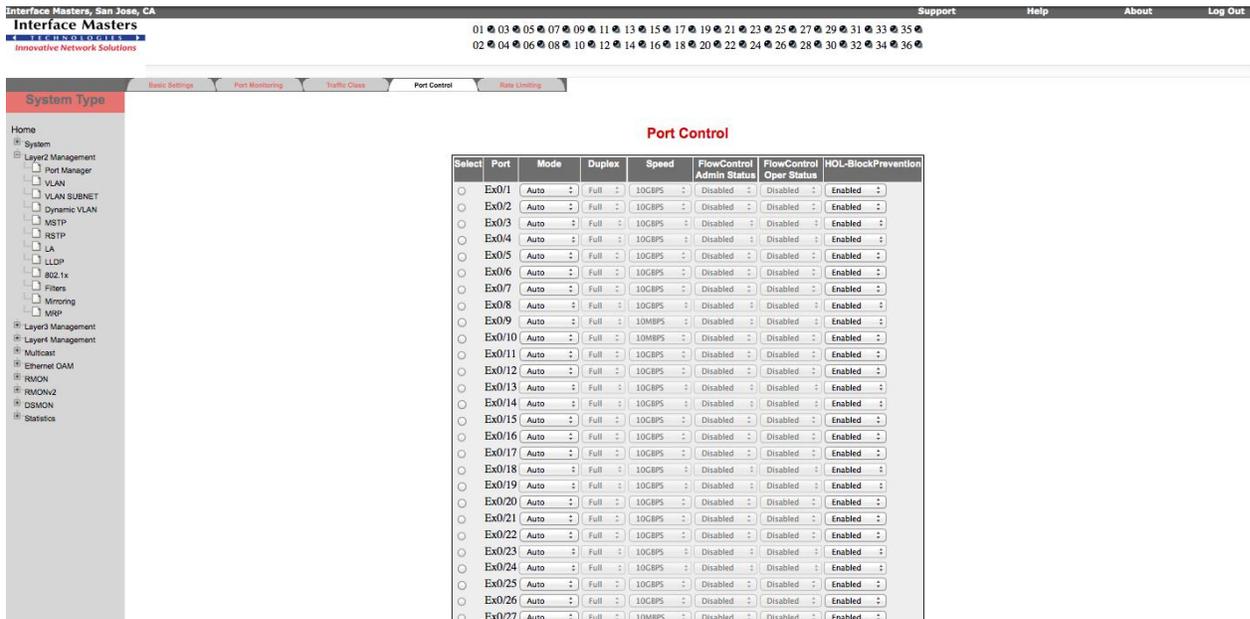


Figure 4-5: Port Control - Layer 2 Group

2. Configure the attributes described in Table 4-4.

Table 4-4: Port Control

Field	Description
Port	Specifies the port number. The port number ranges between 1 and 65535.
Mode	Specifies the mode of negotiation for the port. Options are: <ul style="list-style-type: none"> Auto – Duplex, Speed, Flow Control and HOL Block Prevention cannot be configured. NoNegot – Duplex, Speed, Flow Control and HOL Block Prevention can be

Field	Description
	configured. By default, NoNego mode is selected.
Duplex	Configures the duplex operation on the port. Options are: <ul style="list-style-type: none"> • Full – Port is in full-duplex mode. • Half – Port is in half-duplex mode.
Speed	Specifies the speed of the interface. Options are: <ul style="list-style-type: none"> • 10 MBPS – Sets the port speed as 10 Mbps. • 100 MBPS – Sets the port speed as 100 Mbps. • 1 GB – Sets the port speed as 1Gb.
FlowControl Admin Status	Specifies the Flow Control Admin status for an interface. Options are: <ul style="list-style-type: none"> • Disabled –Flow-control is turned off. • Transmit – Flow control packets are sent to a remote device. • Receive – Flow control packets are received from a remote device. • Both – Flow control packets can be both sent to and received from a remote device.
FlowControl Oper Status	Indicates the Flow Control Operational status for an interface. Options are: <ul style="list-style-type: none"> • Invalid • Disabled –Flow-control is turned off. • Transmit – Flow control packets are sent to a remote device. • Receive – Flow control packets are received from a remote device. • Both – Flow control packets can be both sent to and received from a remote device.
HOL-Block Prevention	Specifies the HOL (Head Of Line)-Block Prevention status. Options are: <ul style="list-style-type: none"> • Enabled – Enables HOL Blocking prevention on a port. • Disabled – Disables HOL Blocking prevention on a port. By default, this is enabled.

3. Click **Apply** for the configuration to take effect.

4.1.5 Rate Limiting

The **Rate Limiting** page allows you to configure Rate Limit Level for the packets on a port per basis.

To configure Rate Limiting

1. Select **Layer2 Management > Port Manager > Rate Limiting** to open the **Rate Limiting** page.

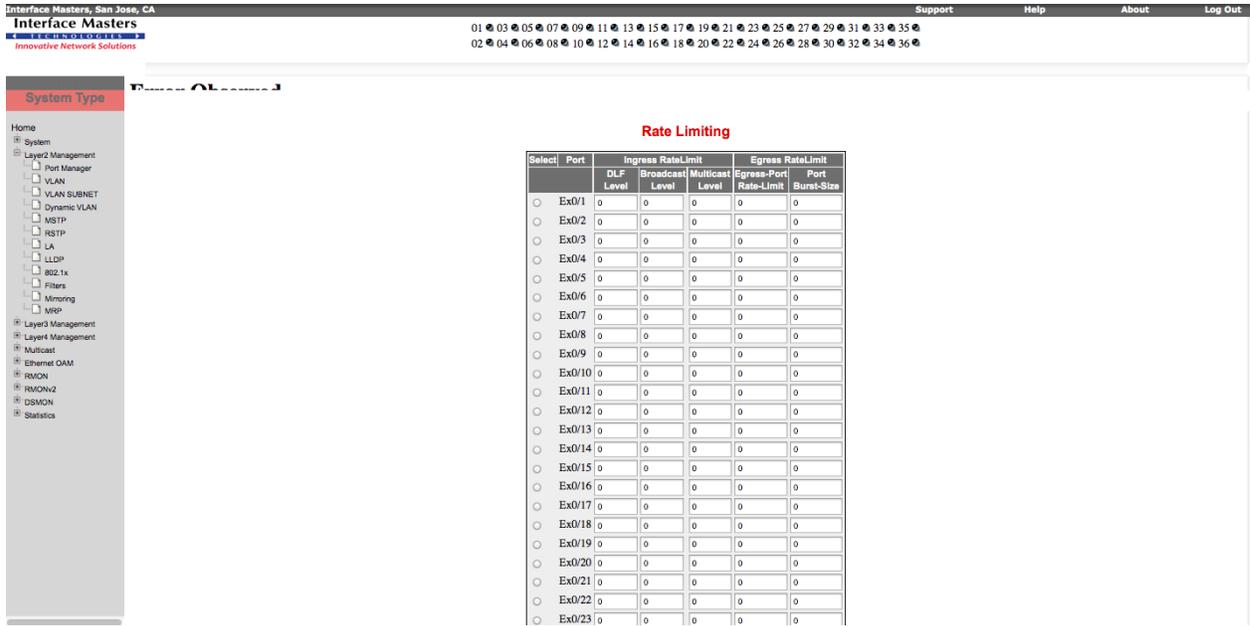


Figure 4-6: Rate Limiting –Layer 2 Group

2. Configure the attributes described in Table 4-5.

Table 4-5: Rate Limiting

Field	Description
Port	Specifies the port number. This is a read-only field.
DLF Level	Specifies the limiting value for the maximum number of DLF (Destination Lookup Failure) Packets that can be transmitted per second over the interface. This value ranges between 0 and 262143. Default value is 0.
Broadcast Level	Specifies the limiting value for the maximum number of broadcast packets that can be transmitted per second over the interface. This value ranges between 0 and 262143. Default value is 0.
Multicast Level	Specifies the limiting value for the maximum number of multicast packets that can be transmitted per second over the interface. This value ranges between 0 and 262143. Default value is 0.
Egress Port Rate Limit	Specifies the Egress Port Rate Limit. This value ranges between 0 and 80000000.
Port Burst Size	Specifies the Port burst packet size. This value ranges between 0 and 80000000.

3. Click **Apply** for the configuration to take effect.

4.2 VLAN

The **VLAN** link allows you to configure the VLAN information through the following links:

- Basic Settings
- Port Settings
- StaticVLANs

- ProtocolGroup
- PortProtocol
- PortMacMAP
- UnicastMac
- Wildcard
- Switchportfiltering

By default, the **VLAN Basic Settings** page is loaded.

4.2.1 Basic Settings⁵

The **VLAN Basic Settings** page allows you to configure the VLAN global configuration information.

To configure VLAN Basic Settings

1. Select **Layer2 Management > VLAN** to open the **VLAN Basic Settings** page.

The screenshot shows the 'VLAN Basic Settings' configuration page. The table below represents the data visible in the configuration interface:

Select	Context	Garp System Control	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
<input checked="" type="radio"/>	0	Start	IVL	Disabled	Disabled	Enabled	Enabled	IVL	300	16128	DOT_1Q_VLAN_MODE	Enabled	Enabled	4094	4094	1

Notes from the screenshot:

- Note 1: To Shutdown GARP, **Dynamic Vlan** & **Dynamic Multicast** should be disabled.
- Note 2: Default VLAN hybrid type can be configured only when learning mode is hybrid.
- Note 3: Dynamic unicast mac limit set for the switch cannot be less than unicast mac limit of vlan and should not exceed the device capability.
- Note 4: Base bridge mode can be set to DOT_1Q_BRIDGE_MODE when GARP, SNOOPING, PNAC, LA, LLDP, MSTP/RSTP modules were shutdown and interfaces other than physical interfaces were deleted.

Figure 4-7: VLAN Basic Settings - Layer 2 Group

2. Configure the attributes described in Table 4-6.

Table 4-6: VLAN Basic Settings

Field	Description
Context	Specifies the context ID. This read-only value ranges between 0 and 65535. The default context ID is 0.
Garp System Control	Specifies the administrative status requested by management for GARP (Generic Attribute Registration Protocol). Options are: <ul style="list-style-type: none"> • Start – Starts GARP in switch. • Shutdown – Shutdown GARP in switch. By default, this is set to Start.

⁵ The two fields - Dynamic VLAN Oper Status and Dynamic Multicast Oper Status are not supported in Enterprise package.

Field	Description
	<input type="checkbox"/> To shutdown GARP, Dynamic VLAN and Dynamic Multicast should be disabled.
Learning Mode	Specifies the type of the VLAN learning mode operational on this switch. Options are: <ul style="list-style-type: none"> • IVL – Independent VLAN learning. • SVL – Shared VLAN learning. • HYBRID – Both Independent and shared VLAN learning. By default, IVL is selected.
Subnet Based On All Ports	Specifies the subnet based on all ports status. Options are: <ul style="list-style-type: none"> • Enabled – Enables the subnet based on all ports. • Disabled - Disables the subnet based on all ports. Default option is Disabled.
MAC Based on All Ports	Specifies the MAC status on all ports. Options are: <ul style="list-style-type: none"> • Enabled – Enables port MAC based classification. • Disabled – Disables port MAC based classification. Default option is Disabled.
Port and Protocol Based on All Ports	Specifies the port protocol based type on all ports. Options are: <ul style="list-style-type: none"> • Enabled – Enables port protocol based classification. • Disabled – Disables port protocol based classification. Default option is Enabled.
Dynamic Vlan Oper Status	Specifies the operational status of the GVRP module. Options are: <ul style="list-style-type: none"> • Enabled – GVRP module is currently enabled in the device. • Disabled – GVRP module is currently disabled in the device. Default option is Enabled.
Dynamic Multicast Oper Status	Specifies the operational status of the GMRP module. Options are: <ul style="list-style-type: none"> • Enabled – GMRP module is currently enabled in the device. • Disabled – GMRP module is currently disabled in the device. Default option is Enabled.
Maximum VLAN ID	Specifies the largest (4094) valid VLAN ID, which the switch can accept. Any number greater than 4094 will be discarded. The default value is 4093.
Maximum Supported VLANs	Specifies the maximum number of VLANs that this device can scale. The default value is 256.
Number of VLANs in the System	Specifies the active number of VLANs configured in the device. By default, one VLAN is configured in the device.

3. Click **Apply** for the configuration to take effect.

4.2.2 Port Settings

The **VLAN Port Settings** page allows you to associate the VLAN ID to the port for Port based VLAN classification. While associating different ports to

VLANs, you can also configure ingress filtering (at the port level) and frame type (accept tagged frame alone or all frames).

To configure VLAN Port Settings

1. Select **Layer2 Management > VLAN > Port Settings** to open the **VLAN Port Settings** page.

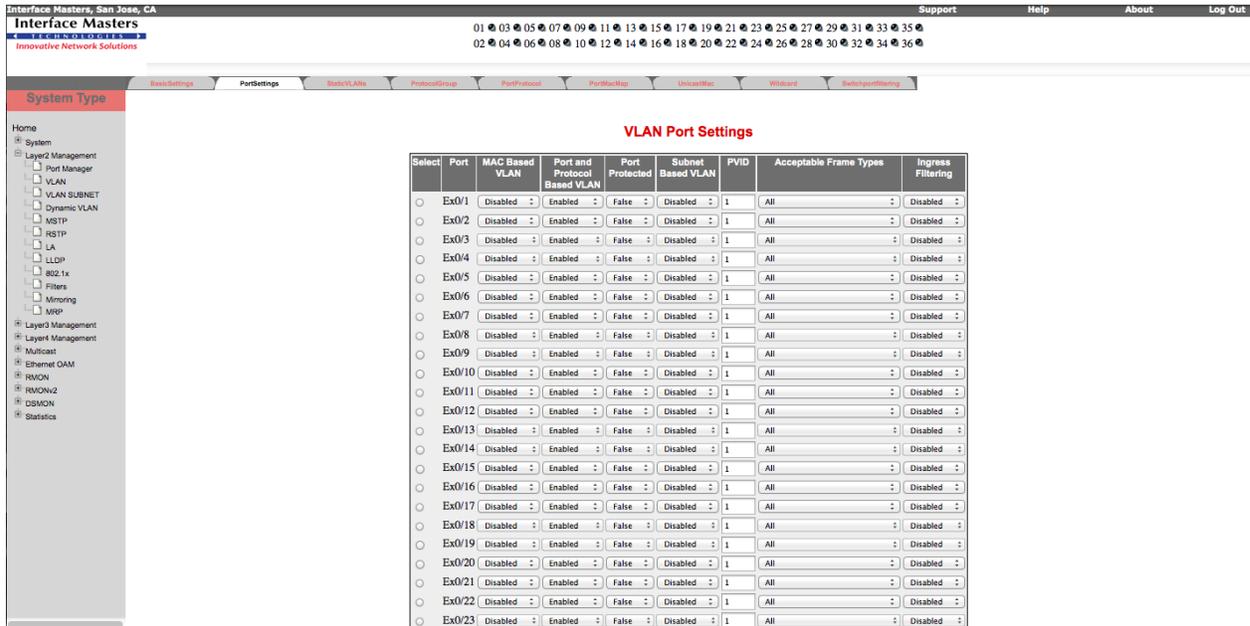


Figure 4-8: VLAN Port Settings - Layer 2 Group

2. Configure the attributes described in Table 4-7.

Table 4-7: VLAN Port Settings

Field	Description
Port	Specifies the port number. This is a read-only value.
MAC Based VLAN	Specifies the MAC based VLAN status on the port. Options are: <ul style="list-style-type: none"> • Enabled – Enables port MAC based VLAN classification. • Disabled – Disables port MAC based VLAN classification. Default option is Enabled.
Port and Protocol Based VLAN	Specifies the port and protocol based VLAN status on the port. Options are: <ul style="list-style-type: none"> • Enabled – Enables port and protocol based VLAN classification. • Disabled – Disables port and protocol based VLAN classification. Default option is Enabled.
PVID	Specifies the VLAN ID assigned to untagged frames or Priority Tagged frames received on the port. This value ranges between 1 and 4094.
Acceptable Frame Types	Specifies the acceptable frame types. Options are: <ul style="list-style-type: none"> • All – Untagged frames or Priority Tagged frames received on the port will be accepted and assigned to the PVID for the port. • Tagged – Untagged frames or Priority Tagged frames received on the port will be

Field	Description
	discarded.
	<ul style="list-style-type: none"> UnTagged and Priority Tagged – Only the Untagged and Priority tagged frames on the port will be received. By default, All is selected.
	<input type="checkbox"/> This field does not affect VLAN independent BPDU (Bridge Protocol Data Unit) frames such as GVRP and STP (Spanning Tree Protocol). It affects VLAN dependent BPDU frames such as GMRP.
Ingress Filtering	Specifies the ingress filtering status. Options are: <ul style="list-style-type: none"> Enabled – Discards the incoming frames for VLANs which do not include the port in its Member set. Disabled – Accepts all incoming frames. By default, this is Disabled.

3. Click **Apply** for the configuration to take effect.

4.2.3 Static VLANs

The **Static VLAN Configuration** page allows you to configure the static VLAN related information.

To configure Static VLAN

1. Select **Layer2 Management > VLAN > StaticVLANs** to open the **Static VLAN Configuration** page.

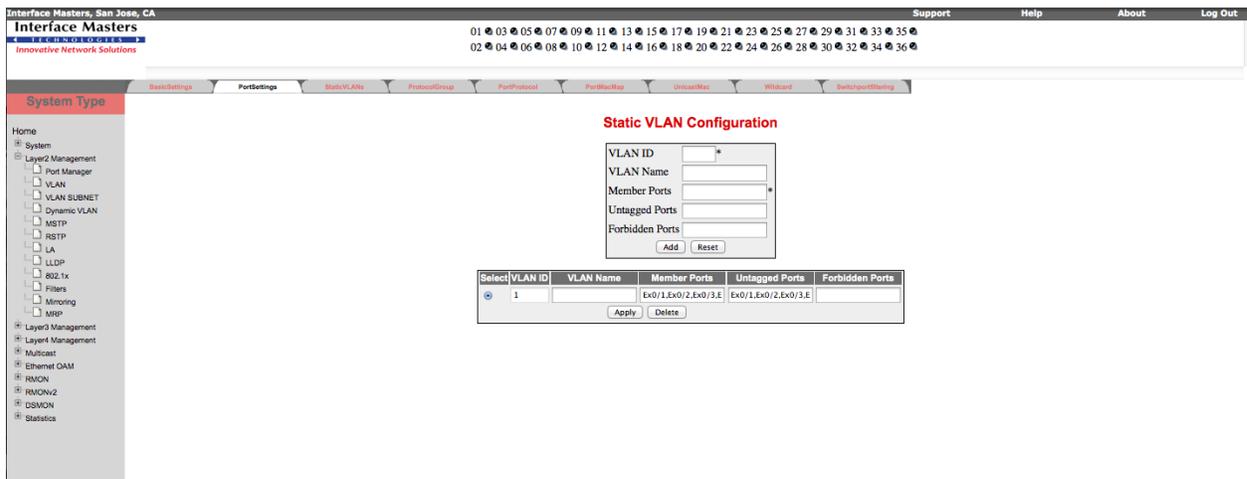


Figure 4-9: Static VLAN Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-8.

Table 4-8: Static VLAN Configuration

Field	Description
VLAN ID	Specifies the VLAN Identifier. This value ranges between 1 and 4094.

Field	Description
VLAN Name	Specifies an administratively assigned string, which is used to identify the VLAN.
Member Ports	Specifies the set of ports which are permanently assigned to the egress list for the VLAN.
Untagged Ports	Specifies the set of ports, which should transmit egress packets for the VLAN as untagged.
Forbidden ports	Specifies the set of ports, which are prohibited by management from being included in the egress list for the VLAN.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.2.4 ProtocolGroup

The **VLAN Protocol Group Settings** page maps the Protocol Templates to the Protocol Group Identifiers.

To configure VLAN Protocol Group Settings

1. Select **Layer2 Management > VLAN > ProtocolGroup** to open the **VLAN Protocol Group Settings** page.

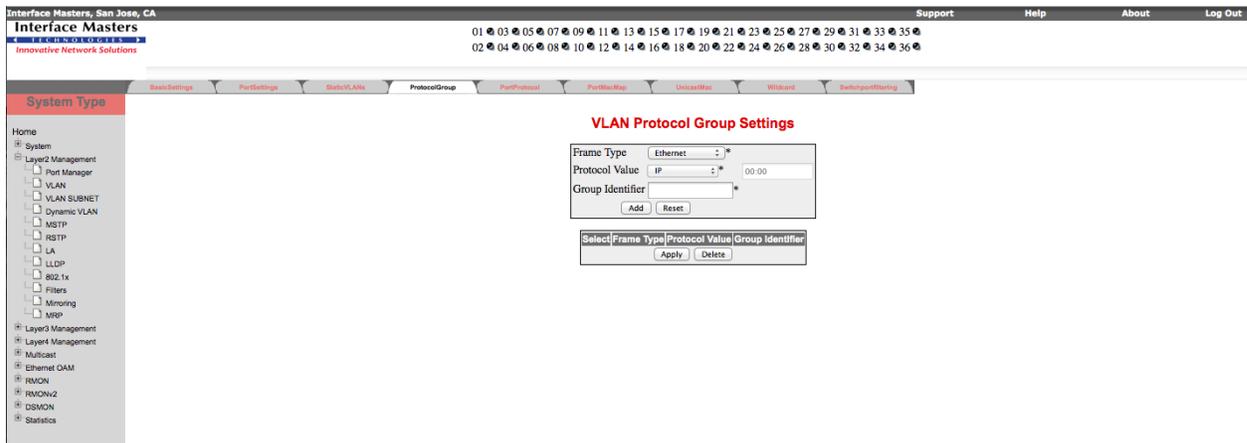


Figure 4-10: VLAN Protocol Group Settings - Layer 2 Group

2. Configure the attributes described in Table 4-9.

Table 4-9: VLAN Protocol Group Settings

Field	Description
Frame Type	Specifies the data-link encapsulation format. Options are: <ul style="list-style-type: none"> Ethernet Snap SNAP802.1H SNAP OTHER LLC OTHER
Protocol Value	Specifies the value of the protocol in a protocol template. Options are: <ul style="list-style-type: none"> IP NOVELL NETBIOS APPLETALK OTHER
Group Identifier	Represents a group of protocols that are associated together when assigning a VID to a frame. This value ranges between 0 and 2147483647.

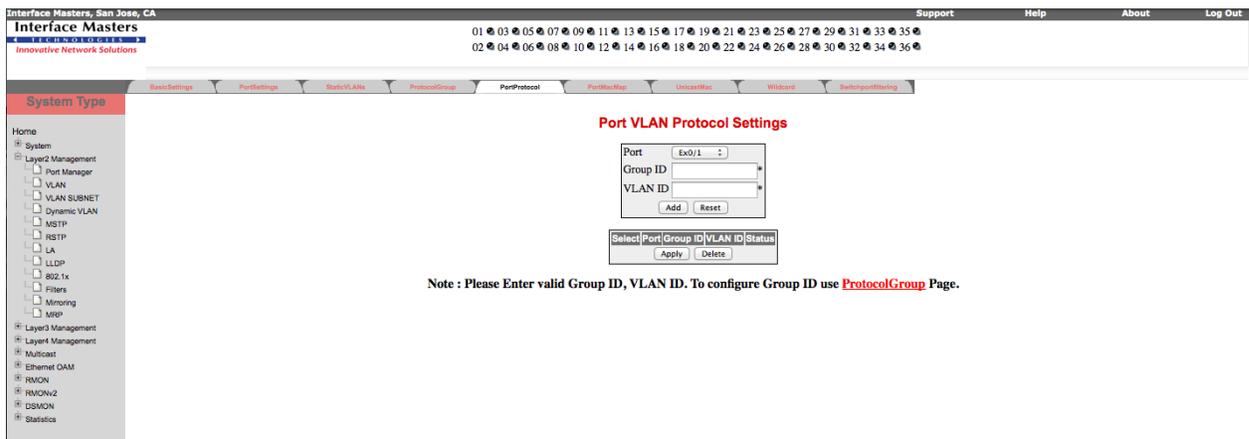
- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry and click **Delete** for the entry to be deleted.

4.2.5 PortProtocol

The **Port VLAN Protocol Settings** page is used for Port and Protocol based VLAN classification.

To configure Port VLAN Protocol Settings

- Select **Layer2 Management > VLAN > PortProtocol** to open the **Port VLAN Protocol Settings** page.



The screenshot shows the 'Port VLAN Protocol Settings' page in the Interface Masters web interface. The page has a navigation menu on the left with options like System, Layer2 Management, and Layer3 Management. The main content area contains a form with the following fields and buttons:

- Port:** A dropdown menu showing 'Ex0/1'.
- Group ID:** A text input field.
- VLAN ID:** A text input field.
- Buttons:** 'Add' and 'Reset' buttons below the input fields.
- Table:** A table with columns 'Select', 'Port', 'Group ID', 'VLAN ID', and 'Status'. Below the table are 'Apply' and 'Delete' buttons.

Below the form, there is a note: "Note : Please Enter valid Group ID, VLAN ID. To configure Group ID use ProtocolGroup Page."

Figure 4-11: Port VLAN Protocol Settings - Layer 2 Group

- Configure the attributes described in Table 4-10.

Table 4-10: Port VLAN Protocol Settings

Field	Description
Port	Specifies the port number.
Group ID	Designates a group of protocols in the Protocol Group Database. This value ranges between 1 and 2147483647.
VLAN ID	Specifies the ID associated with a group of protocols for each port. This value ranges between 1 and 4093.
Status	Specifies the status of the entry. Options are: <ul style="list-style-type: none"> Up Down Under Creation

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

4.2.6 PortMacMAP

The **VLAN Port mac Map** page allows you to configure VLAN-MAC address mapping.

To configure VLAN Port mac Map

- Select **Layer2 Management > VLAN > PortMacMap** to open the **VLAN Port mac Map** page.

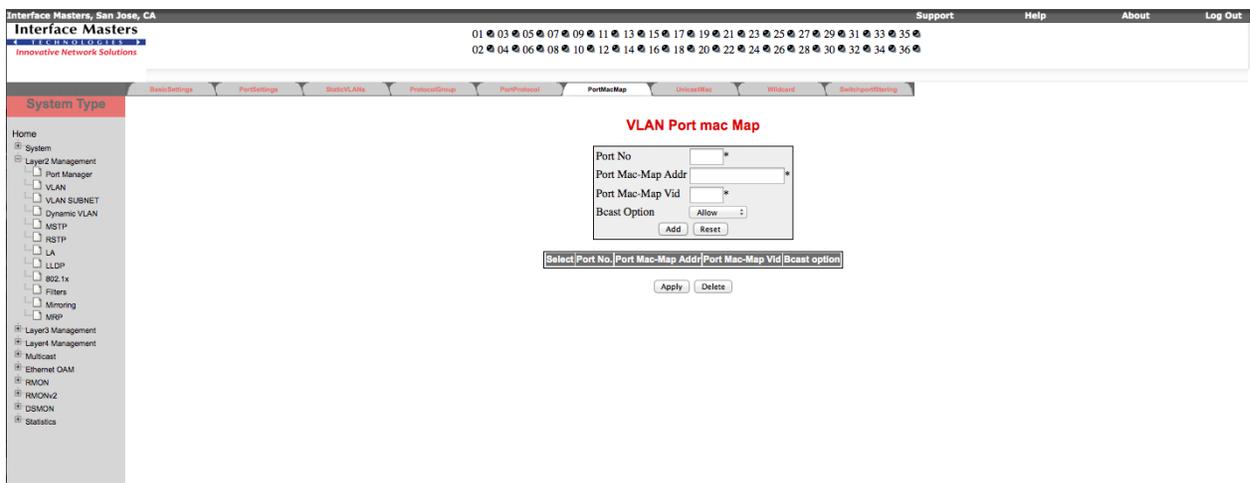


Figure 4-12: VLAN Port MAC Map – Layer 2 Group

- Configure the attributes described in Table 4-11.

Table 4-11: VLAN Port MAC Map

Field	Description
Port No	Specifies the Interface index.
Port Mac-Map Addr	Specifies the MAC address for which the VLAN mapping is present.
Port Mac-Map Vid	Specifies the VLAN to which the MAC address is mapped.
Bcast Option	Specifies the Broadcast option. Options are: <ul style="list-style-type: none"> Allow – Indicates that Broadcast frames with source MAC address as in the MAC VLAN entry will be dropped, if MAC based VLAN is enabled on that port. Discard – Indicates that Broadcast frames with source MAC address as in the MAC VLAN entry will be processed, if MAC based VLAN is enabled on that port. By default, this is set to Allow.

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

4.2.7 UnicastMac

The **VLAN Unicast Mac Settings** page allows you to configure the MAC admin status and the MAC limit for the VLAN.

To configure VLAN Unicast Mac Settings

- Select **Layer2 Management > VLAN > UnicastMac** to open the **VLAN Unicast Mac Settings** page.

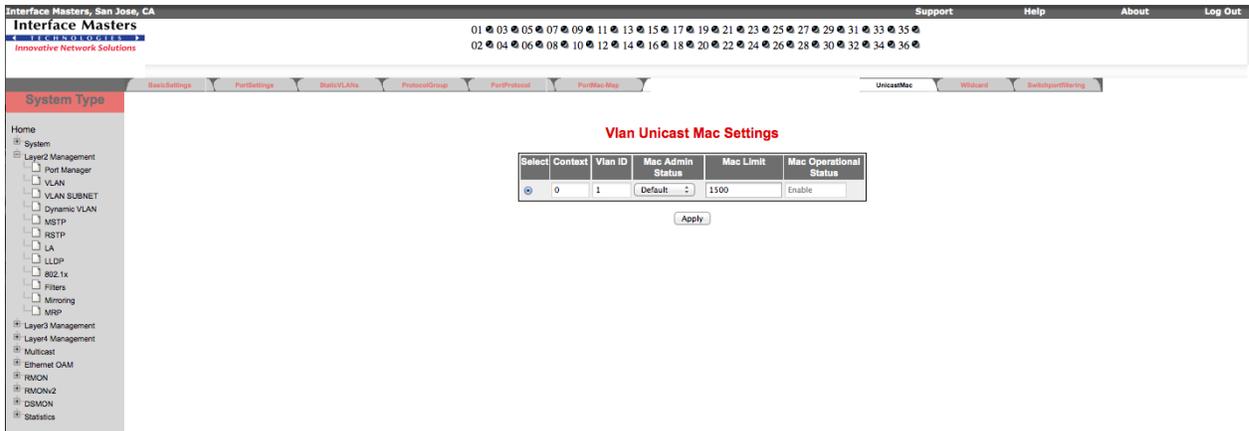


Figure 4-13: VLAN Unicast MAC Settings – Layer 2 Group

- Configure the attributes described in Table 4-12.

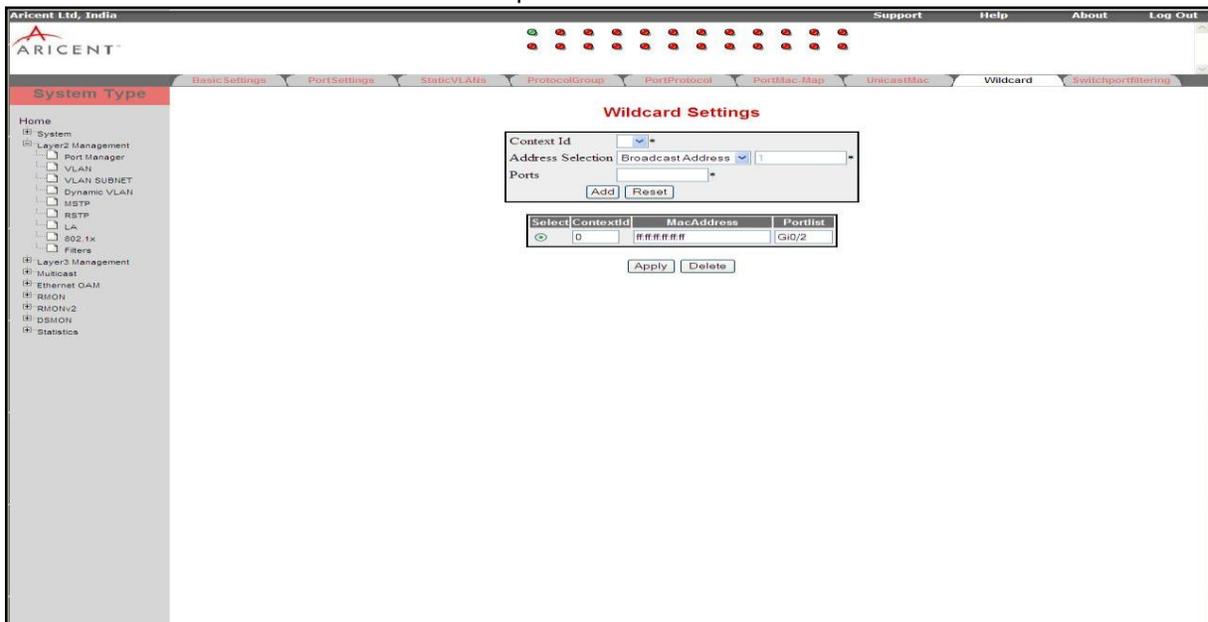
Table 4-12: VLAN Unicast MAC Settings

Field	Description
Context	Specifies the context ID. This is a read-only field
Vlan ID	Specifies the VLAN Identifier. This value ranges between 1 and 4094. This is a read-only field.
Mac Admin Status	Specifies the MAC administration status. Options are: <ul style="list-style-type: none"> Enabled – Enables the MAC administration status. Disabled – Disables the MAC administration status. By default, this is Enabled.
Mac Limit	Specifies the limiting value on the number of distinct unicast MAC addresses learnt in a VLAN. This value ranges between 0 and 950.
Mac Operational Status	Specifies the MAC operational status. Options are: <ul style="list-style-type: none"> Enable –MAC operational status is enabled. Disable – MAC operational status is disabled. <input type="checkbox"/> If the VLAN does not have any member port, then the Mac operational status for that VLAN will always be disabled. Otherwise, the Mac operational status will take value from Mac Admin Status.

3. Click **Apply** for the configuration to take effect.

4.2.8 Wildcard

The **Wildcard Settings** page allows you to configure the MAC address selection and the ports to which frames must be forwarded.



To configure Wildcard Settings

1. Select **Layer2 Management > VLAN > Wildcard** to open the **Wildcard Settings** page.

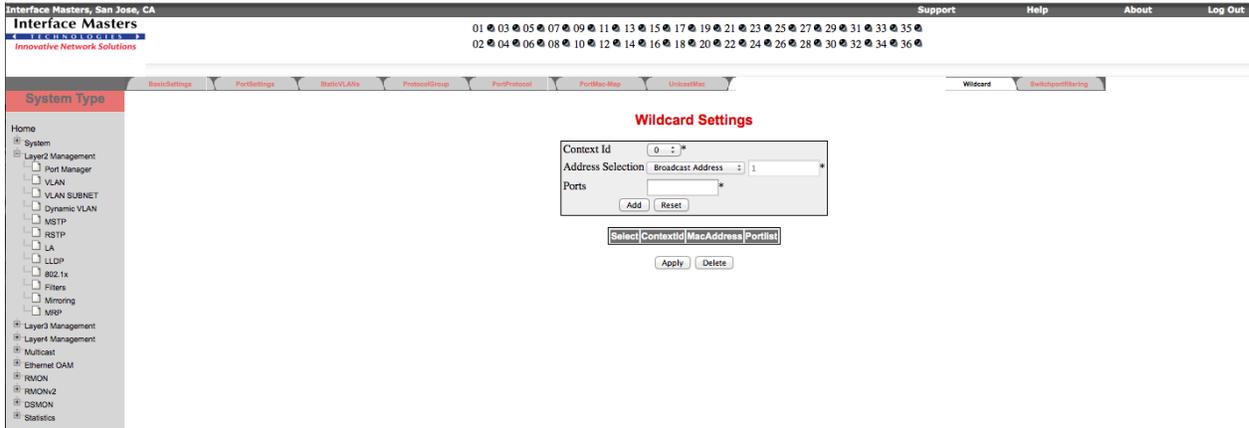


Figure 4-14: Wildcard Settings – Layer 2 Group

2. Configure the attributes described in Table 4-13.

Table 4-13: Wildcard Settings

Field	Description
Context ID	Specifies the context ID.
Address Selection	Specifies the MAC Address selection type. Options are: <ul style="list-style-type: none"> • Broadcast Address • Mac Address
Ports	Specifies the set of ports to which frames must be forwarded.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.2.9 Switchportfiltering

The **SwitchPort VLAN Filtering** page allows you to configure the utility criteria for the port.

To configure SwitchPort VLAN Filtering

1. Select **Layer2 Management > VLAN > Switchportfiltering** to open the **SwitchPort VLAN Filtering** page.

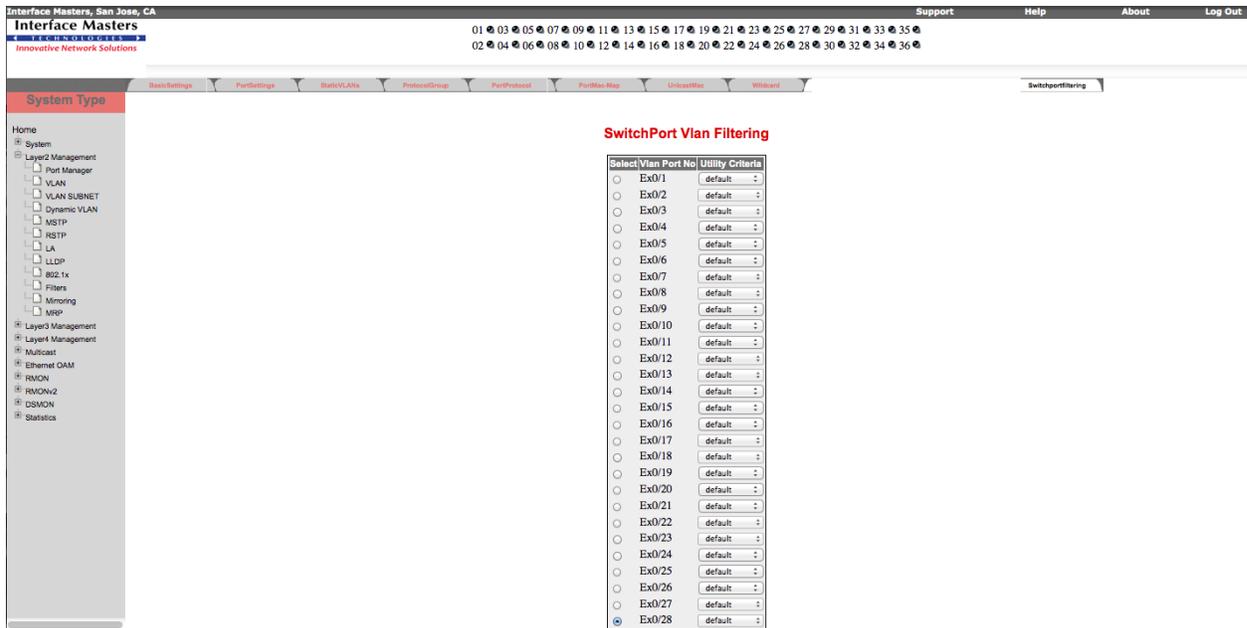


Figure 4-15: SwitchPort VLAN Filtering – Layer 2 Group

- Configure the attributes described in Table 4-14.

Table 4-14: SwitchPort VLAN Filtering

Field	Description
Vlan Port No	Specifies the VLAN port number.
Utility Criteria	Specifies the utility criteria of the port. Options are: <ul style="list-style-type: none"> default – Learning of source MAC from a received packet on the port will be done only if there is atleast one member port in that VLAN. enhanced – Learning of source MAC from a received packet on the port will be done only if the following conditions are satisfied. <ol style="list-style-type: none"> Atleast one VLAN that uses the FID includes the reception Port and atleast one other Port with a Port State of Learning or Forwarding in its member set. The operPointToPointMAC parameter is false for the reception Port or Ingress to the VLAN is permitted through a third Port. By default, this is set to default.

- Click **Apply** for the configuration to take effect.

4.3 VLAN SUBNET

The **VLAN Subnet Port-Map** page allows you to configure the subnet port map information.

To configure VLAN Subnet Port-Map

- Select **Layer2 Management > VLAN > VLAN SUBNET** to open the **VLAN Subnet Port-Map** page.

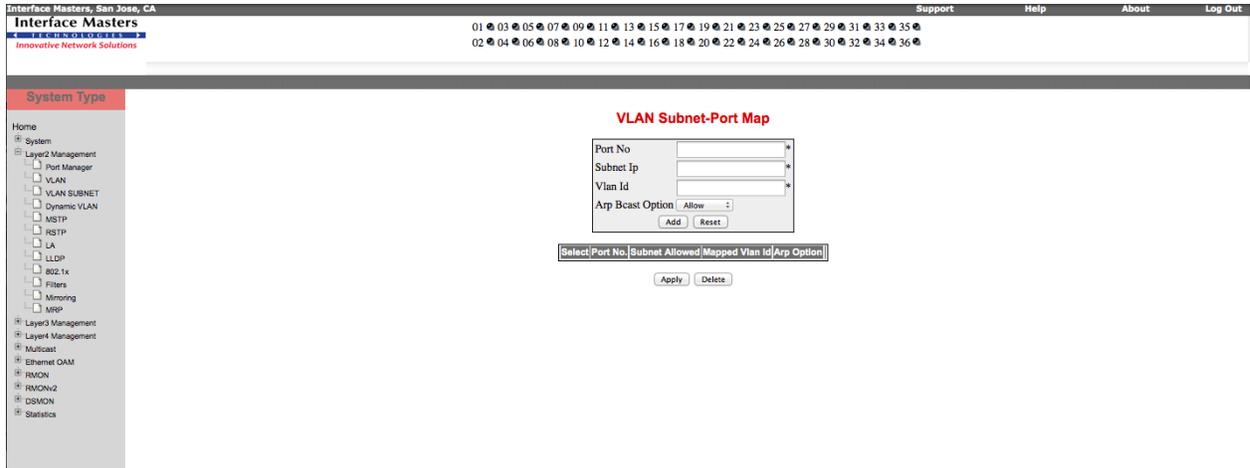


Figure 4-16: VLAN Subnet Port-Map – Layer 2 Group

2. Configure the attributes described in Table 4-15.

Table 4-15: VLAN Subnet Port-Map

Field	Description
Subnet Ip	Specifies the subnet IP address.
Vlan Id	Specifies the VLAN identifier.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.4 Dynamic VLAN

The **Dynamic VLAN** link allows you to configure the Dynamic VLAN information through the following links:

- DynamicVlan
- Port Settings
- GarpTimers

By default, the **Dynamic VLAN Global Configuration** page is loaded.

4.4.1 DynamicVlan

The **Dynamic VLAN Global Configuration** page allows you to configure the dynamic VLAN status.

To configure Dynamic VLAN Global Settings

1. Select **Layer2 Management > DynamicVLAN** to open the **Dynamic VLAN Global Configuration** page.

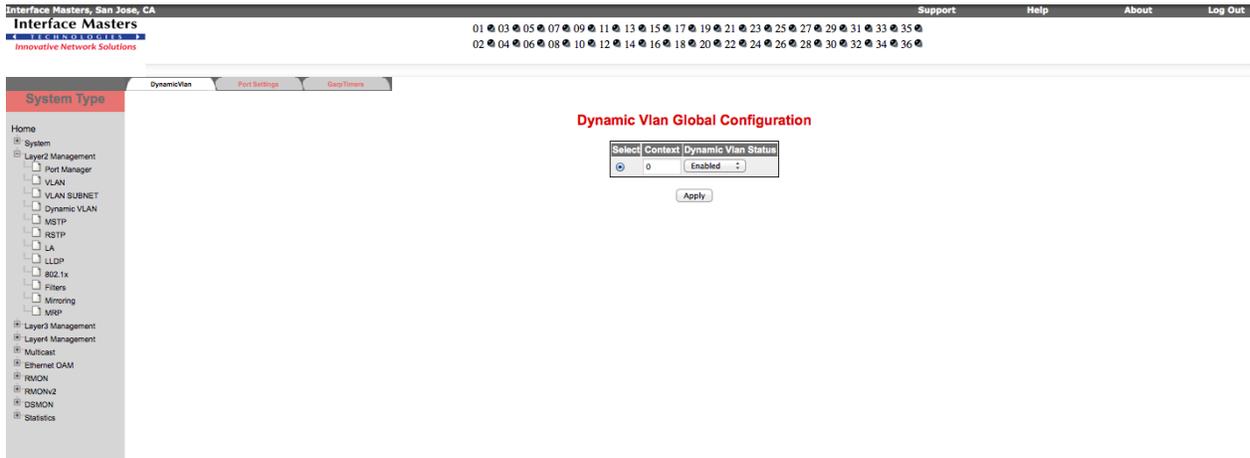


Figure 4-17: Dynamic VLAN Global Configuration – Layer 2 Group

2. Configure the attributes described in Table 4-16.

Table 4-16: Dynamic VLAN Global Configuration

Field	Description
Context	Specifies the Context ID.
Dynamic Vlan Status	Specifies the dynamic VLAN status in the switch. Options are: <ul style="list-style-type: none"> • Enabled – GVRP is enabled on this device on all ports. • Disabled – GVRP is disabled on all ports and all GVRP packets will be forwarded transparently. By default, this is Enabled.

3. Click **Apply** for the configuration to take effect.

4.4.2 Port Settings

The **Dynamic VLAN Port Configuration** page allows you to configure the dynamic VLAN status and the restricted VLAN registration.

To configure Dynamic VLAN Global Settings

1. Select **Layer2 Management > Dynamic VLAN > Port Settings** to open the **Dynamic VLAN Port Configuration** page.

Dynamic Vlan Port Configuration

Select	Port	Dynamic Vlan Status	Restricted VLAN Registration
<input type="radio"/>	Ex0/1	Enabled	Disabled
<input type="radio"/>	Ex0/2	Enabled	Disabled
<input type="radio"/>	Ex0/3	Enabled	Disabled
<input type="radio"/>	Ex0/4	Enabled	Disabled
<input type="radio"/>	Ex0/5	Enabled	Disabled
<input type="radio"/>	Ex0/6	Enabled	Disabled
<input type="radio"/>	Ex0/7	Enabled	Disabled
<input type="radio"/>	Ex0/8	Enabled	Disabled
<input type="radio"/>	Ex0/9	Enabled	Disabled
<input type="radio"/>	Ex0/10	Enabled	Disabled
<input type="radio"/>	Ex0/11	Enabled	Disabled
<input type="radio"/>	Ex0/12	Enabled	Disabled
<input type="radio"/>	Ex0/13	Enabled	Disabled
<input type="radio"/>	Ex0/14	Enabled	Disabled
<input type="radio"/>	Ex0/15	Enabled	Disabled
<input type="radio"/>	Ex0/16	Enabled	Disabled
<input type="radio"/>	Ex0/17	Enabled	Disabled
<input type="radio"/>	Ex0/18	Enabled	Disabled
<input type="radio"/>	Ex0/19	Enabled	Disabled
<input type="radio"/>	Ex0/20	Enabled	Disabled
<input type="radio"/>	Ex0/21	Enabled	Disabled
<input type="radio"/>	Ex0/22	Enabled	Disabled
<input type="radio"/>	Ex0/23	Enabled	Disabled
<input type="radio"/>	Ex0/24	Enabled	Disabled
<input type="radio"/>	Ex0/25	Enabled	Disabled
<input type="radio"/>	Ex0/26	Enabled	Disabled

Dynamic Vlan Port Configuration

Select	Port	Dynamic Vlan Status	Restricted VLAN Registration
<input type="radio"/>	Ex0/1	Enabled	Disabled
<input type="radio"/>	Ex0/2	Enabled	Disabled
<input type="radio"/>	Ex0/3	Enabled	Disabled
<input type="radio"/>	Ex0/4	Enabled	Disabled
<input type="radio"/>	Ex0/5	Enabled	Disabled
<input type="radio"/>	Ex0/6	Enabled	Disabled
<input type="radio"/>	Ex0/7	Enabled	Disabled
<input type="radio"/>	Ex0/8	Enabled	Disabled
<input type="radio"/>	Ex0/9	Enabled	Disabled
<input type="radio"/>	Ex0/10	Enabled	Disabled
<input type="radio"/>	Ex0/11	Enabled	Disabled
<input type="radio"/>	Ex0/12	Enabled	Disabled
<input type="radio"/>	Ex0/13	Enabled	Disabled
<input type="radio"/>	Ex0/14	Enabled	Disabled
<input type="radio"/>	Ex0/15	Enabled	Disabled
<input type="radio"/>	Ex0/16	Enabled	Disabled
<input type="radio"/>	Ex0/17	Enabled	Disabled
<input type="radio"/>	Ex0/18	Enabled	Disabled
<input type="radio"/>	Ex0/19	Enabled	Disabled
<input type="radio"/>	Ex0/20	Enabled	Disabled
<input type="radio"/>	Ex0/21	Enabled	Disabled
<input type="radio"/>	Ex0/22	Enabled	Disabled
<input type="radio"/>	Ex0/23	Enabled	Disabled
<input type="radio"/>	Ex0/24	Enabled	Disabled
<input type="radio"/>	Ex0/25	Enabled	Disabled
<input type="radio"/>	Ex0/26	Enabled	Disabled
<input type="radio"/>	Ex0/27	Enabled	Disabled
<input checked="" type="radio"/>	Ex0/28	Enabled	Disabled

Apply

Figure 4-18: Dynamic VLAN Port Configuration – Layer 2 Group

2. Configure the attributes described in Table 4-17.

Table 4-17: Dynamic VLAN Port Configuration

Field	Description
Port	Specifies the Interface index. This is a read-only field.
Dynamic Vlan Status	Specifies the dynamic VLAN status in the switch. Options are:

Field	Description
	<ul style="list-style-type: none"> Enabled – GVRP is enabled on this device on all ports. Disabled – GVRP is disabled on all ports and all GVRP packets will be forwarded transparently. <p>By default, this is Enabled.</p>
Restricted VLAN Registration	<p>Specifies the restricted VLAN registration status in the switch. Options are:</p> <ul style="list-style-type: none"> Enabled – Enables restricted VLAN registration. That is, the creation of a new dynamic VLAN entry is permitted only if there is a Static VLAN Registration Entry for the VLAN concerned, in which the Registrar Administrative Control value for this port is Normal Registration. Disabled – Disables restricted VLAN registration. <p>By default, this is Disabled.</p>

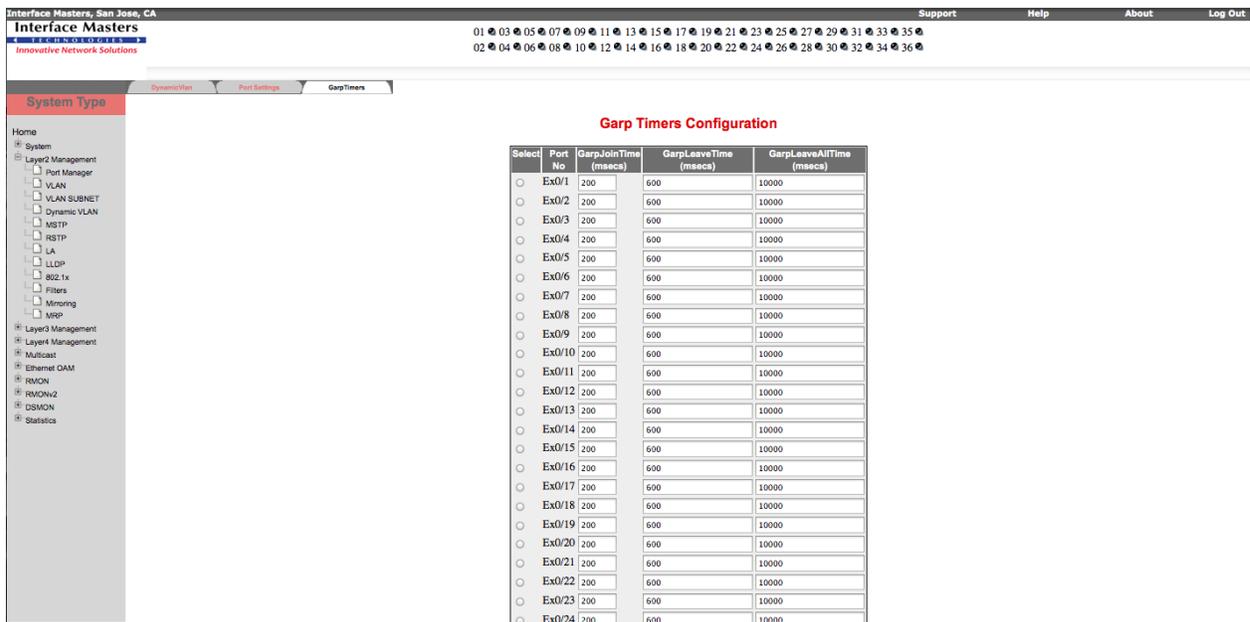
3. Click **Apply** for the configuration to take effect.

4.4.3 GarpTimers

The **Garp Timers Configuration** page allows you to configure the GARP timer parameters.

To configure Garp Timers

1. Select **Layer2 Management > Dynamic VLAN > GarpTimers** to open the **Garp Timers Configuration** page.



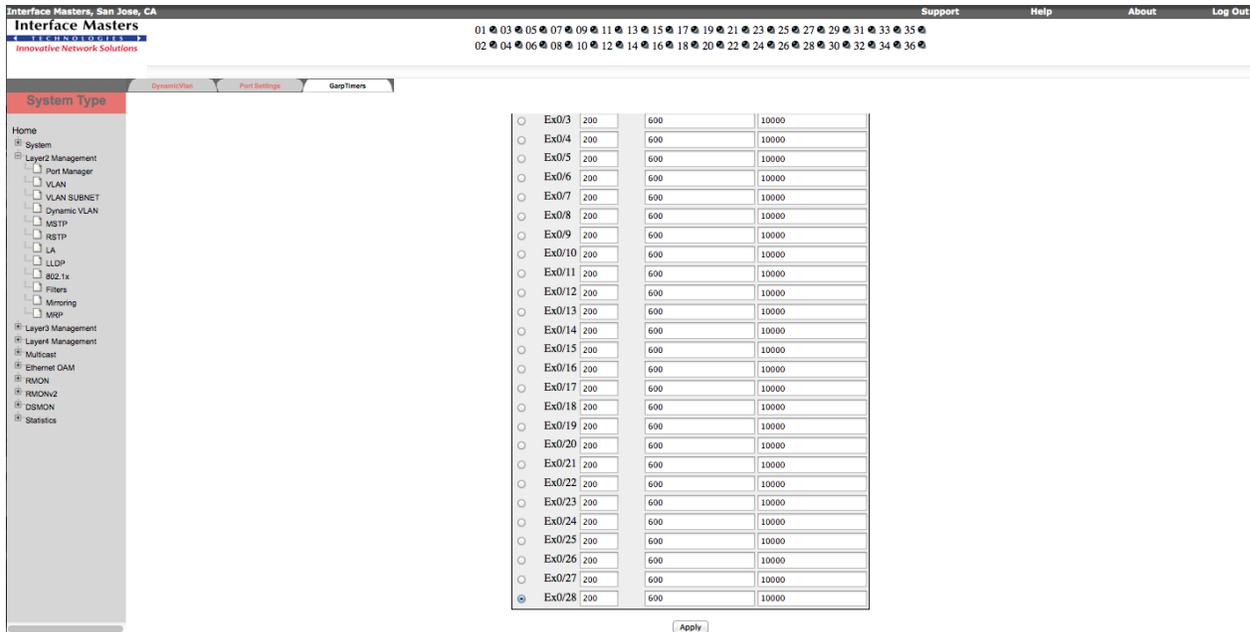


Figure 4-19: Garp Timers Configuration– Layer 2 Group

2. Configure the attributes described in Table 4-18.

Table 4-18: Garp Timers Configuration

Field	Description
Port No	Specifies the Interface index. This is a read-only field.
GarpJoinTime (msecs)	Specifies the GARP Join Time in milliseconds. Default value is 200 milliseconds.
GarpLeaveTime (msecs)	Specifies the GARP Leave Time in milliseconds. Default value is 600 milliseconds.
GarpLeaveAllTime (msecs)	Specifies the GARP Leave All Time in milliseconds. Default value is 10000 milliseconds.

3. Click **Apply** for the configuration to take effect.

4.5 MSTP⁶

The **MSTP** link allows you to configure the MSTP information through the following links:

- Basic Settings

⁶ PVRST feature is supported only in the METRO package.

- Timers
- Port Configuration
- VLAN Mapping
- Port Settings
- CIST Port Status

By default, the **MSTP Basic Settings** page is loaded.

4.5.1 Basic Settings

The **MSTP Global Configuration** page allows you to configure the basic settings of MSTP.

To configure MSTP Global information

1. Select **Layer2 Management > MSTP** to open the **Global Configuration** page.

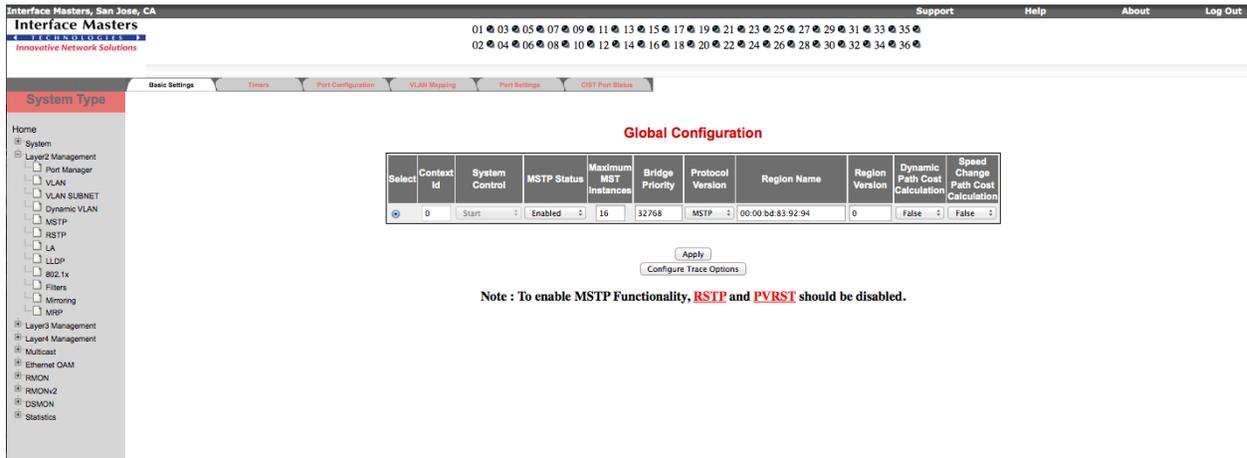


Figure 4-20: MSTP Basic Settings – Layer 2 Group

2. Configure the attributes described in Table 4-19.

Table 4-19: MSTP Basic Settings

Field	Description
Context Id	Specifies the context ID. This ranges between 0 and 65535.
System Control	Specifies the system control status of the MSTP in the switch. Options are: <ul style="list-style-type: none"> • Start – MST will be active in the device on all ports. • Shutdown – MST will be shutdown in the device on all ports.
MSTP Status	Specifies the MSTP module status in the switch. Options are: <ul style="list-style-type: none"> • Enabled – MST is enabled in the device on all ports. • Disabled – MST is disabled in the device on all ports. <input type="checkbox"/> MSTP can be enabled in the device only if the MSTP system control status is set to Start.
Maximum MST	Specifies the maximum number of spanning trees to be allowed.

Field	Description
Instances	This value ranges between 1 and 64.
Bridge Priority	Specifies the Priority value assigned to the bridge that is used to select the root bridge. This value ranges between 0 and 61440. Default value is 32768.
Protocol Version	Specifies the version of Spanning Tree Protocol in which the bridge is currently running. Options are: <ul style="list-style-type: none"> • STP • RSTP • MSTP By default, MSTP is selected.
Region Name	Specifies the name for the Region's configuration. By default, the region name will be the bridge MAC address.
Region Version	Specifies the version number of the configuration to be used. This value ranges between 0 and 65535.
Dynamic Path Cost Calculation	Specifies whether dynamic pathcost calculation is allowed or not. Options are: <ul style="list-style-type: none"> • True – Pathcost is calculated dynamically from the port speed. • False – Pathcost is calculated from the link speed at the time of port creation. By default, this is False.
Speed Change Path Cost Calculation	Specifies whether dynamic pathcost calculation is done for ports for which port speed changes dynamically. Options are: <ul style="list-style-type: none"> • True – Dynamic pathcost calculation is done for ports for which port speed changes dynamically. • False – Dynamic pathcost calculation is not done for ports for which port speed changes dynamically. By default, this is False.



To enable MSTP, RSTP should be disabled.

3. Click **Apply** for the configuration to take effect.

4.5.2 Timers

The **Timers Configuration** page allows you to configure the MSTP Timers information.

To configure Timers

1. Select **Layer2 Management > MSTP > Timers** to open the **Timers Configuration** page.

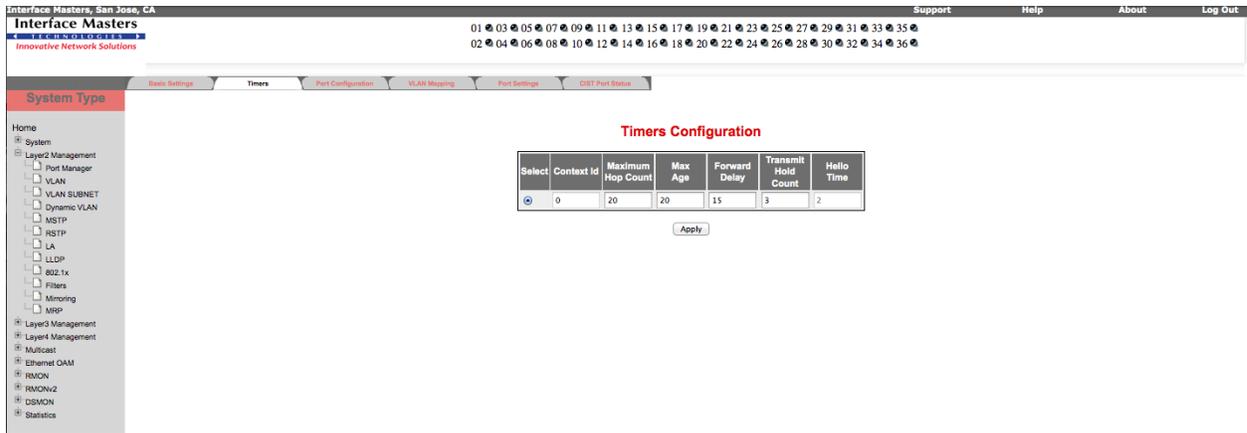


Figure 4-21: MSTP Timers Configuration – Layer 2 Group

- Configure the attributes described in Table 4-20.

Table 4-20: MSTP Timers Configuration

Field	Description
Context Id	Specifies the context ID.
Maximum Hop Count	Specifies the Maximum Hop Count value. That is, the maximum number of bridges that a packet can cross before it is dropped, to avoid infinite looping of the packets. This value ranges between 6 and 40. Default value is 20.
Max Age	Specifies the time period in seconds, for which the information received in the MSTP BPDU is valid. This value ranges between 6 and 40 seconds. Default value is 20 seconds.
Forward Delay	Specifies how fast a port changes its spanning state when moving towards the Forwarding state. This value ranges between 4 and 30 seconds. Default value is 15 seconds.
Transmit Hold Count	Specifies the maximum number of packets that can be sent in a given interval. This is configured to avoid flooding. This value ranges between 1 and 10. Default value is 3.
Hello Time	Specifies the time interval between two successive configuration BPDUs (Bridge Protocol Data Units). This value can be either one or two seconds.

- Click **Apply** for the configuration to take effect.

4.5.3 Port Configuration

The **CIST Settings** page allows you to configure per port related to MSTP.

To configure CIST (Common Internal Spanning Tree) Settings

- Select **Layer2 Management > MSTP > Port Configuration** to open the **CIST Settings** page.

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
<input type="radio"/>	Ex0/1	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/2	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/3	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/4	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/5	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/6	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/7	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/8	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/9	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/10	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/11	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/12	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/13	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/14	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/15	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/16	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/17	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/18	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/19	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/20	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/21	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/22	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False
<input type="radio"/>	Ex0/23	20000	128	Auto	False	Enable	False	2	True	False	False	True	True	False	False

Figure 4-22: CIST Settings - Layer 2 Group

2. Configure the attributes described in Table 4-21.

Table 4-21: CIST Settings

Field	Description
Port	Specifies the port identifier.
Priority	Specifies the port priority used in role selection. This value ranges between 0 and 240. This must be incremented in steps of 16. Default value is 128.
Path Cost	Specifies the contribution of the port to the cost of paths towards the CIST Root, which includes this port. This value ranges between 1 and 200000000.
Point-to-Point Status	Specifies the administrative point-to-point status of the LAN (Local Area Network) segment attached to the port. Options are: <ul style="list-style-type: none"> ForceTrue – Port is always treated as if it is connected to a point-to-point link. ForceFalse – Port is treated as having a shared media connection. Auto – Port is considered to have a point-to-point link, <ol style="list-style-type: none"> if it is an Aggregator and all of its members can be aggregated. If the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
Edge Port	Specifies the administrative value of the Edge Port parameter. Options are: <ul style="list-style-type: none"> True – Port is assumed as an Edge port. False – Port is assumed as a non-Edge port.
MSTP Status	Specifies the MSTP module status in the switch. Options are: <ul style="list-style-type: none"> Enable – MST is enabled in the device on all ports. Disable – MST is disabled in the device on all ports.

Field	Description
	<p>The default value is Enable.</p> <p><input type="checkbox"/> MSTP can be enabled in the device only if the MSTP system control status is set to Start.</p>
Protocol Migration	<p>Specifies the Protocol migration state of the Port. Options are:</p> <ul style="list-style-type: none"> • True • False <p>This is to control the migration among MSTP, RSTP and STP protocols, if the other side of the switch runs a different mode. Migration takes place only if this is set to True.</p>
Hello Time	<p>Specifies the time interval between two successive configuration BPDUs.</p> <p>This value ranges between 1 and 10 seconds.</p>
Auto Edge Status	<p>Specifies the means of detection of a port as an Edge Port. Options are:</p> <ul style="list-style-type: none"> • True – Detection of a port as Edge Port happens automatically. • False – Edge Port feature is disabled.
Restricted Role	<p>Specifies the Restricted role status of the port. Options are:</p> <ul style="list-style-type: none"> • True – Port is not selected as Root Port for the CIST or any MSTI (Multiple Spanning Tree Instance), even if it has the best spanning tree priority vector. It will be selected as an Alternate Port after the Root Port has been selected. • False – Causes lack of spanning tree connectivity. <p>By default, this is set to False.</p>
Restricted TCN	<p>Indicates the Restricted TCN status of the port. Options are:</p> <ul style="list-style-type: none"> • True – Port does not propagate the received topology change notifications and topology changes to other ports. • False – Causes temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. <p>By default, this is set to False.</p>

3. Click **Apply** for the configuration to take effect.

4.5.4 VLAN Mapping

The **VLAN Mapping** page allows you to add /delete VLAN.

To configure VLAN Mapping

1. Select **Layer2 Management > MSTP > VLAN Mapping** to open the **VLAN Mapping** page.

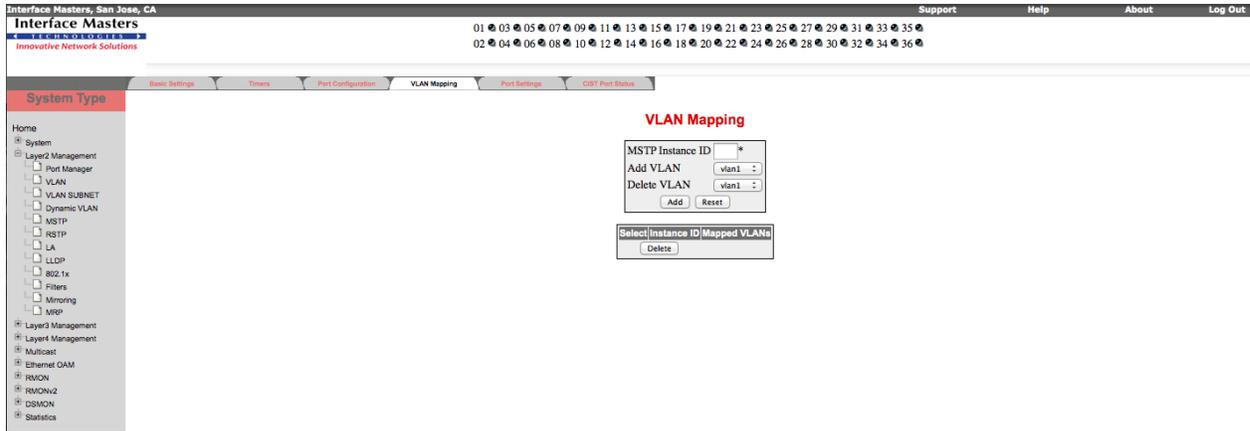


Figure 4-23: VLAN Mapping - Layer 2 Group

- Configure the attributes described in Table 4-22.

Table 4-22: VLAN Mapping

Field	Description
MSTP Instance ID	Specifies the Instance ID, which is the index of the table.
Add VLAN	Specifies the list of VLANs from which the VLAN to be mapped to this instance of the spanning tree can be selected.
Delete VLAN	Specifies the list of VLANs from which the VLAN to be unmapped from this instance of the spanning tree can be selected.
Mapped VLANs	Specifies the list of VLANs mapped to the instance of the spanning tree.

- Click **Add** to save the entry. To discard the information you have entered, click **Reset**.
- Select the required entry and click **Delete** for the entry to be deleted.

4.5.5 Port Settings

The **Port Settings** page allows you to configure port state, priority and cost for a port.

To configure Port Settings

- Select **Layer2 Management > MSTP > Port Settings** to open the **Port Settings** page.

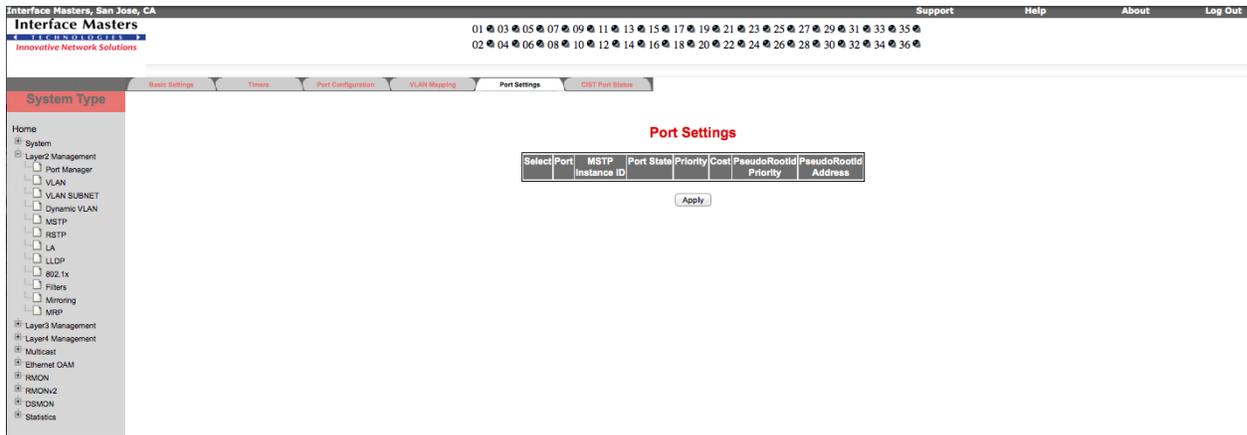


Figure 4-24: Port Settings - Layer 2 Group

- Configure the attributes described in Table 4-23.

Table 4-23: Port Settings

Field	Description
Port	Specifies the interface index of the port on which MSTP is run.
MSTP Instance ID	Specifies the Instance ID, which is the index of the table.
Port State	Specifies the current state of the port. Options are: <ul style="list-style-type: none"> Enabled Disabled
Priority	Specifies the port priority used in role selection. This value ranges between 0 and 240. This value is incremented in steps of 16. Default value is 128.
Cost	Specifies the cost associated with this port, which will be added to the cost of any path that includes this port. This value ranges between 0 and 200000000.

- Click **Apply** for the configuration to take effect.

4.5.6 CIST Port Status

The **MSTP CIST Port Status** page displays the MSTP CIST port specific information.

To view MSTP CIST Port Status

- Select **Layer2 Management > MSTP > CIST Port Status** to open the **Port Settings** page.

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
Ex01	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:01	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex02	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:02	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex03	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:03	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex04	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:04	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex05	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:05	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex06	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:06	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex07	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:07	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex08	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:08	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex09	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:09	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex10	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0a	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex11	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0b	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex12	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0c	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex13	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0d	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex14	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0e	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex15	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:0f	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex16	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:10	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex17	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:11	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex18	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:12	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex19	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:13	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex20	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:14	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex21	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:15	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex22	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:16	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex23	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:17	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex24	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:18	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex25	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:19	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex26	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:1a	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex27	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:1b	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex28	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:1c	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex29	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:1d	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding
Ex30	80:00:00:00:bd:83:92:94	32768	80:00:00:00:bd:83:92:94	80:1e	0	80:00:00:00:bd:83:92:94	32768	0	SharedLan	Disabled	Discarding

Figure 4-25: MSTP CIST Port Status - Layer 2 Group-2

2. The attributes are described in Table 4-24.

Table 4-24: Port Settings

Field	Description
Port	Specifies the port identifier.
Designated Root	Specifies the unique Identifier of the bridge recorded as the Root for the segment to which the port is attached.
Root priority	Specifies the priority of the root in the network for CIST.
Designated Bridge	Specifies the Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.
Designated Port	Specifies the Identifier of the port on the Designated Bridge for this port's segment.
Designated Cost	Specifies the path cost of the Designated Port of the segment connected to this port.
Regional Root	Specifies the unique Identifier of the bridge recorded as the CIST Regional Root Identifier in the configuration BPDUs transmitted.
Regional Root Priority	Specifies the priority of the regional root in the network for this specific MSTI (Multiple Spanning Tree Instance).
Regional Path Cost	Specifies the contribution of this port to the cost of paths towards the CIST Regional Root, which includes this port.
Type	Specifies the operational point-to-point status of the LAN (Local Area Network) segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or Shared media.
Role	Specifies the Ports Current Role as defined by Spanning Tree Protocol. The values are <ul style="list-style-type: none"> disabled

Field	Description
	<ul style="list-style-type: none"> alternate backup root designated
Port State	<p>Specifies the port's current state as defined by application of the Spanning Tree Protocol. The values are</p> <ul style="list-style-type: none"> discarding learning forwarding

4.6 RSTP⁶

The **RSTP** link allows you to configure the RSTP information through the following links:

- Global Settings
- Basic Settings
- Port Settings
- REF_Ref102971948 \h Port Status

By default, the **RSTP Basic Settings** page is loaded.

4.6.1 Global Settings

The **RSTP Global Configuration** page allows you to configure the RSTP basic settings.

To configure RSTP Global information

- Select **Layer2 Management > RSTP** to open the **RSTP Global Configuration** page.

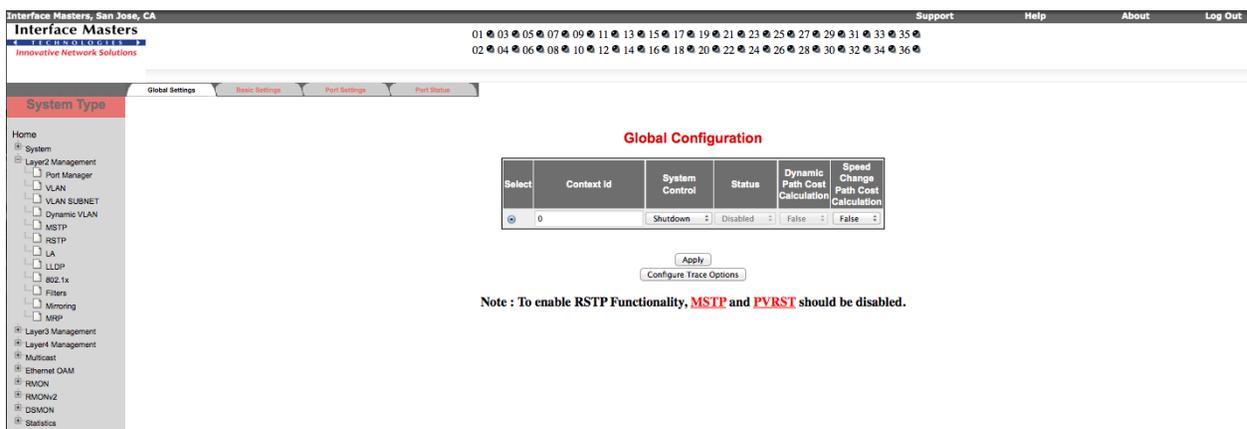


Figure 4-26: RSTP Basic Settings – Layer 2 Group

2. Configure the attributes described in Table 4-25.

Table 4-25: RSTP Basic Settings

Field	Description
Context Id	Specifies the context ID.
System Control	Specifies the system control status of the RSTP in the switch. Options are: <ul style="list-style-type: none"> Start – RSTP will be active in the device on all ports. Shutdown – RSTP will be shutdown in the device on all ports.
Status	Specifies the RSTP module status in the switch. Options are: <ul style="list-style-type: none"> Enabled – RSTP is enabled in the device on all ports. Disabled – RSTP is disabled in the device on all ports. <input type="checkbox"/> RSTP can be enabled in the device only if the RSTP system control status is set to Start.
Dynamic Path Cost Calculation	Specifies whether dynamic path cost calculation is allowed or not. Options are: <ul style="list-style-type: none"> True – Pathcost is calculated dynamically from the port speed. False – Pathcost is calculated from the link speed at the time of port creation. By default, this is set to False.



To enable RSTP, MSTP should be disabled.

3. Click **Apply** for the configuration to take effect.

4.6.2 Basic Settings

The **RSTP Configuration** page allows you to configure the RSTP Timers information.

To configure RSTP

1. Select **Layer2 Management > RSTP > Basic Settings** to open the **RSTP Configuration** page.

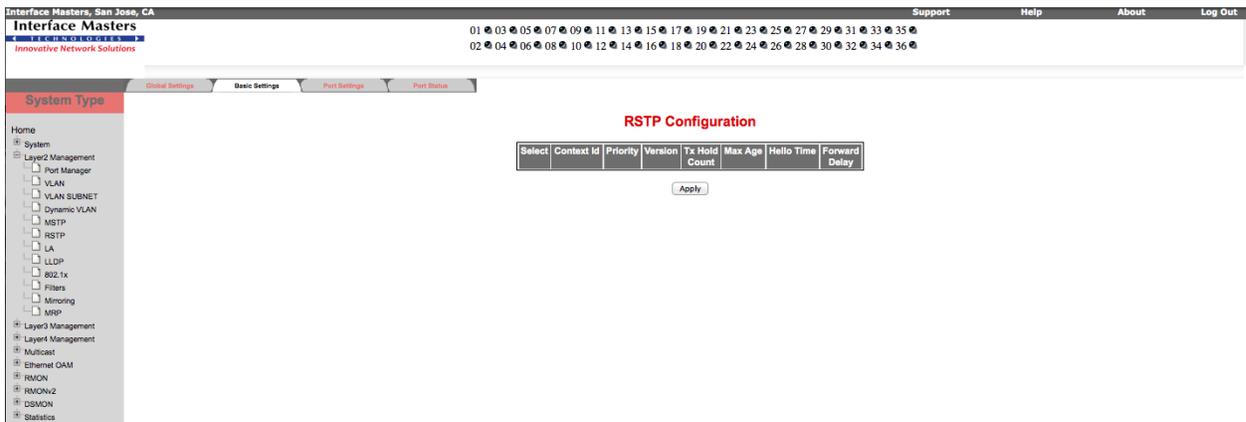


Figure 4-27: RSTP Configuration – Layer 2 Group

2. Configure the attributes described in Table 4-26.

Table 4-26: RSTP Configuration

Field	Description
Context Id	Specifies the context ID, which is operated currently. This value ranges between 0 and 65535.
Priority	Specifies the port priority used in role selection. This value ranges between 0 and 61440. This value is incremented in steps of 4096. Default value is 32768.
Version	Specifies the version of Spanning Tree Protocol, the bridge is currently running. Options are: <ul style="list-style-type: none"> • STP Compatible • RSTP Compatible
Tx Hold Count	Specifies the value used by the Port Transmit state machine to limit the maximum transmission rate. This value ranges between 1 and 10. Default value is 3.
Max Age	Specifies the time period in seconds, for which the information received in RSTP BPDU is valid. This value ranges between 6 and 40 seconds. Default value is 20 seconds.
Hello Time	Specifies the time interval between two successive configuration BPDUs (Bridge Protocol Data Units). This value can be either 1 or 2 seconds.
Forward Delay	Specifies how fast a port changes its spanning state when moving towards the Forwarding state. This value ranges between 4 and 30 seconds. Default value is 15 seconds.

3. Click **Apply** for the configuration to take effect.

4.6.3 Port Settings

The **RSTP Port Status Configuration** page allows you to configure per port related to RSTP.

To configure RSTP Port Status

1. Select **Layer2 Management > RSTP > Port Settings** to open the **Port Status Configuration** page.

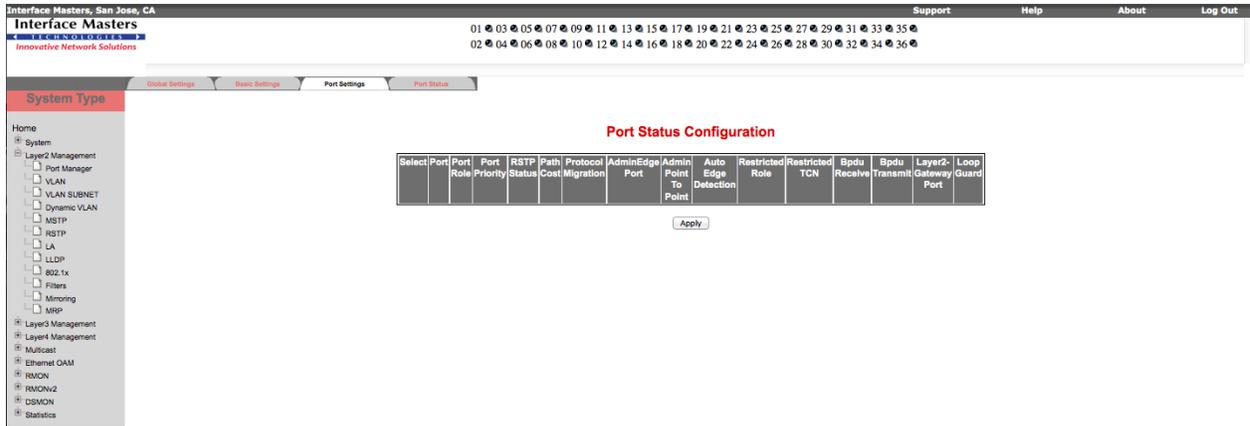


Figure 4-28: RSTP Port Status Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-27.

Table 4-27: RSTP Port Status Configuration

Field	Description
Port	Specifies the port identifier.
Port Role	Indicates the current port role assumed by the port.
Port Priority	Specifies the port priority used in role selection. This value ranges between 0 and 240. This value is incremented in steps of 16. Default value is 128.
RSTP Status	Specifies the RSTP module status in the switch. Options are: <ul style="list-style-type: none"> • Enable – RSTP is enabled in the device on all ports. • Disable – RSTP is disabled in the device on all ports. <input type="checkbox"/> RSTP can be enabled in the device only if the RSTP system control status is set to Start.
Path Cost	Specifies the path cost associated with this port. This value ranges between 1 and 200000000.
Protocol Migration	Specifies the Protocol migration state of the Port. Options are: <ul style="list-style-type: none"> • True • False This is to control the migration among MSTP, RSTP and STP protocols, if the other side of the switch runs a different mode. Migration takes place only if this is set to True.
Admin Edge Port	Specifies the administrative value of the Edge Port parameter. Options are: <ul style="list-style-type: none"> • True – Port is assumed as an Edge port. • False – Port is assumed as a non-Edge port.
Admin Point-to-Point	Specifies the administrative point-to-point status of the LAN segment attached to the port. Options are: <ul style="list-style-type: none"> • ForceTrue – Port is always treated as if it is connected to a point-to-point link. • ForceFalse – Port is treated as having a shared media connection.

Field	Description
	<ul style="list-style-type: none"> Auto – Port is considered to have a point-to-point link, <ol style="list-style-type: none"> if it is an Aggregator and all of its members can be aggregated. If the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
Auto Edge Detection	Specifies the means of detection of a port as an Edge Port. Options are: <ul style="list-style-type: none"> True – Detection of a port as Edge Port happens automatically. False – Edge Port feature is disabled.
Restricted Role	Specifies the Restricted role status of the port. Options are: <ul style="list-style-type: none"> True – Port is not selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. It will be selected as an Alternate Port after the Root Port has been selected. False – Causes lack of spanning tree connectivity. By default, this is set to False.
Restricted TCN	Indicates the Restricted TCN status of the port. Options are: <ul style="list-style-type: none"> True – Port does not propagate the received topology change notifications and topology changes to other ports. False – Causes temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. By default, this is set to False.

- Click **Apply** for the configuration to take effect.

4.6.4 Port Status

The **RSTP Port Status** page displays RSTP port specific information.

To display RSTP Port Status

- Select **Layer2 Management > RSTP > Port Status** to open the **RSTP Port Status** page.

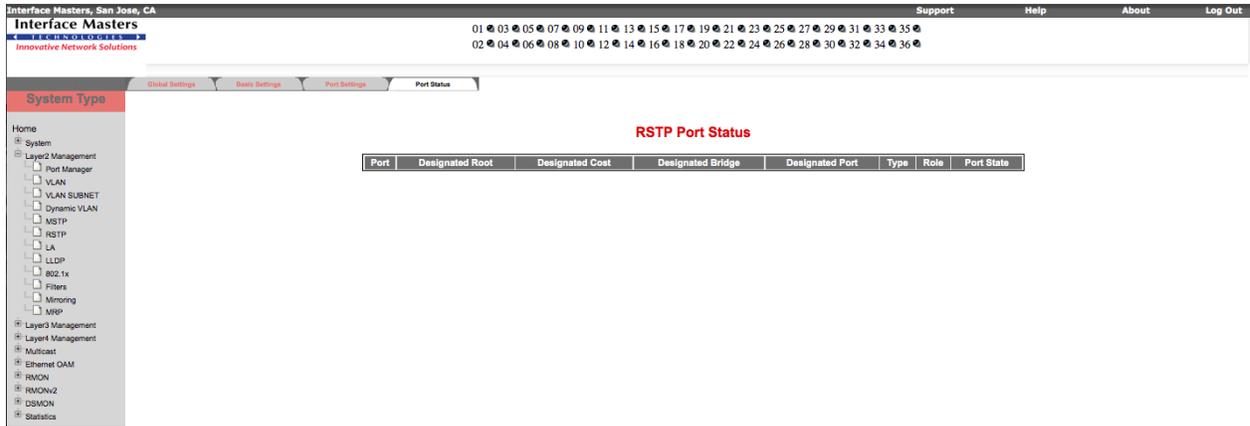


Figure 4-29: RSTP Port Status – Layer 2 Group

2. The attributes are described in Table 4-28.

Table 4-28: RSTP Port Status

Field	Description
Port	Specifies the port identifier.
Designated Root	Specifies the unique Identifier of the Bridge recorded as the Root for the segment to which the port is attached.
Designated Cost	Specifies the path cost of the Designated Port of the segment connected to this port.
Designated Bridge	Specifies the Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.
Designated Port	Specifies the Identifier of the port on the Designated Bridge for this port's segment.
Type	Specifies the operational point-to-point status of the LAN (Local Area Network) segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or Shared media.
Role	Specifies the Ports Current Role as defined by Spanning Tree Protocol.
Port State	Specifies the port's current state as defined by application of the Spanning Tree Protocol.

4.7 LA

The **LA** link allows you to configure the LA information through the following links:

- * MERGEFORMAT Basic Settings
- REF_Ref171760425 \h Interface Settings
- PortChannelSettings
- Port Settings
- Port StateInfo
- Load Balancing

By default, the **LA Basic Settings** page is loaded.

4.7.1 Basic Settings

The **LA Basic Settings** page allows you to configure the basic settings of LA.

To configure LA Basic Settings

1. Select **Layer2 Management > LA** to open the **LA Basic Settings** page.

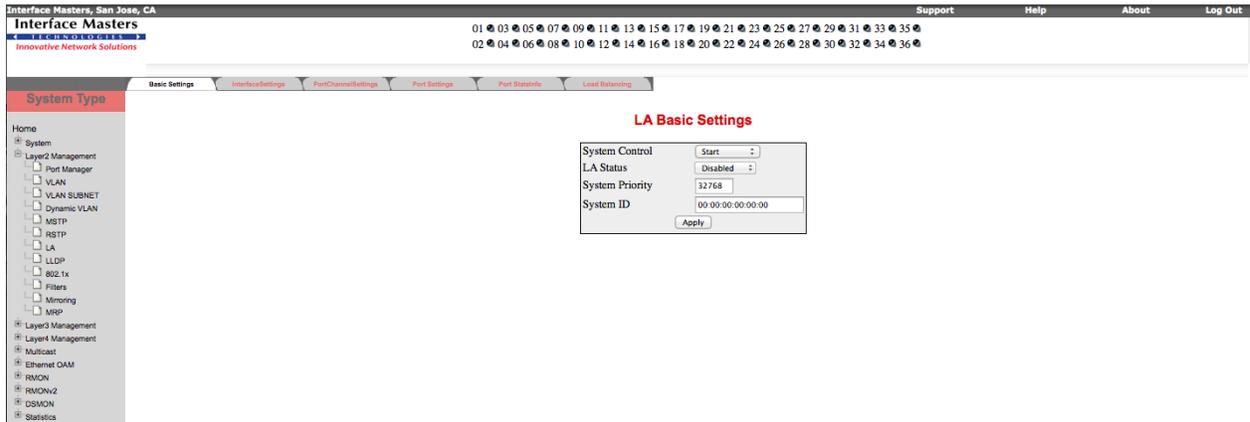


Figure 4-30: LA Basic Settings – Layer 2 Group

2. Configure the attributes described in Table 4-29.

Table 4-29: LA Basic Settings

Field	Description
System Control	Specifies the system control status of the LA in the switch. Options are: <ul style="list-style-type: none"> • Start – Resources required by LA module are allocated and the LA module starts running. • Shutdown – All resources used by LA module is released to the system and the LA module is shut down..
LA Status	Specifies the LA module administrative status. Options are: <ul style="list-style-type: none"> • Enabled – Enables LA in the switch. • Disabled – Disables LA in the switch. By default, this is Disabled.
System Priority	Specifies the priority value associated with the Actor's system ID. This value ranges between 0 and 65535. Default value is 32768.
System ID	Specifies a 6-octet read-write MAC address value used as a unique identifier for the system.

3. Click **Apply** for the configuration to take effect.

4.7.2 Interface Settings

The **Port Channel Interface Basic Settings** page allows you to configure the LA Port Channel Interface Basic Settings.

To configure Port Channel Interface Basic Settings

1. Select **Layer2 Management > LA > Interface Settings** to open the **Port Channel Interface Basic Settings** page.

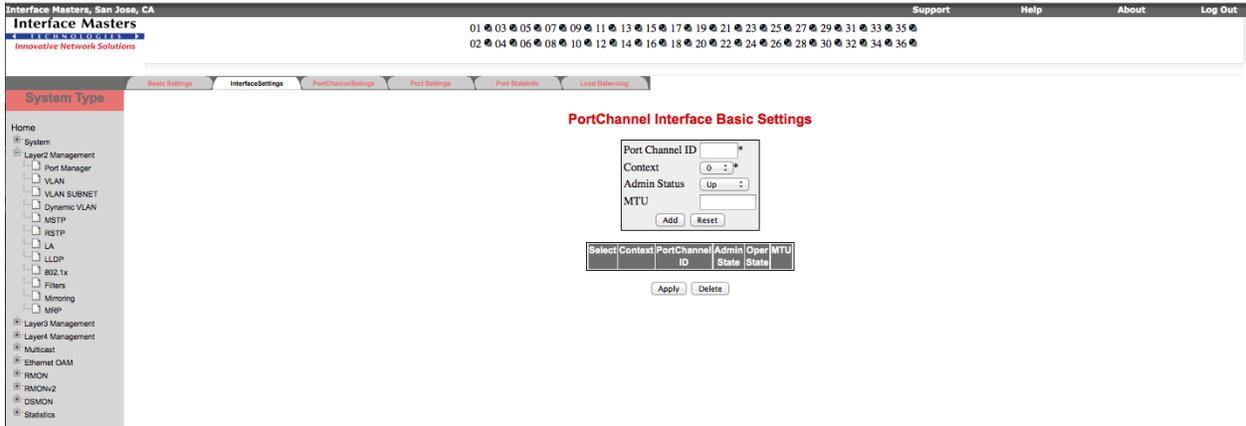


Figure 4-31: LA Port Channel Interface Basic Settings – Layer 2 Group

2. Configure the attributes described in Table 4-30.

Table 4-30: LA Port Channel Interface Basic Settings

Field	Description
Port Channel ID	Specifies the Port-Channel Identifier. This value ranges between 1 and 65535.
Context	Specifies the Context to which the Port channel is associated.
Admin Status	Specifies the Admin Status of the port-channel. Options are: <ul style="list-style-type: none"> • Up • Down
Oper State	Specifies the operational status of the port channel. This is a read-only field. Options are: <ul style="list-style-type: none"> • Up • Down
MTU	Specifies the Maximum Transmission Unit of the Port-channel. This value ranges between 90 and 9202.

3. Click Add to save the entry. If you wish to discard the information you have entered, click Reset.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.7.3 PortChannelSettings

The **LA Port Channel Settings** page allows you to edit the Port Channel configuration. The first table is meant for creating Port Channel interfaces

while the second table is for editing/deleting the existing Port Channel configuration.

To configure LA Port Channel Settings

1. Select **Layer2 Management > LA > PortChannelSettings** to open the **LA Port Channel Settings** page.

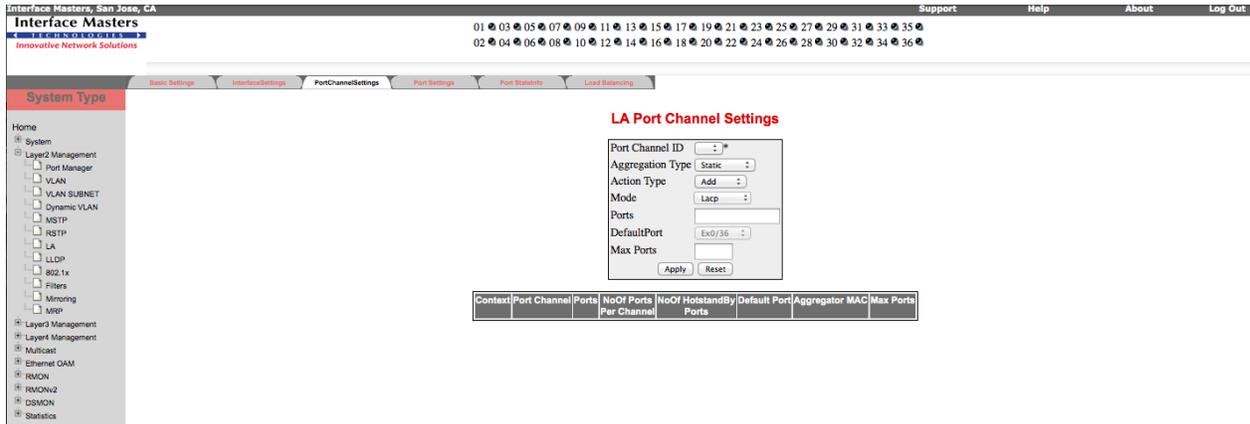


Figure 4-32: LA Port Channel Settings – Layer 2 Group

2. Configure the attributes described in Table 4-31.

Table 4-31: LA Port Channel Settings

Field	Description
Port Channel ID	Specifies the identifier of the port channel interface.
Aggregation Type	<p>Specifies whether the port chooses its aggregator dynamically or it is configured statically. Options are:</p> <ul style="list-style-type: none"> • Static – The port is involved only in static aggregation, that is, the port can be a member of only the aggregation to which it is configured. • Dynamic – The port participates in dynamic aggregation selection, that is, the port will be a part of best aggregation selected based on System ID and Admin key. <p>Default Aggregation Type is Static.</p> <p><input type="checkbox"/> This is set to Dynamic, once the port is configured as a default port of a port channel.</p>
Context	Specifies the Context to which the Port channel is associated.
Action Type	<p>Specifies whether the Port should be added or deleted for the port channel. Options are:</p> <ul style="list-style-type: none"> • Add • Delete
Mode	<p>Specifies the various Port Modes. Options are:</p> <ul style="list-style-type: none"> • LACP – Places the port into passive negotiation state, in which the port waits for its peer to initiate negotiation. • Manual – Forces the port to enable channeling. • Disable – Disables channeling.

Field	Description
Ports	Specifies the interface indices that must be configured to be members of the Port Channel.
Default Port	Specifies the default port when the port is configured to participate in dynamic aggregator selection.
MAC Selection	<p>Specifies the mode by which the MAC address for the Port Channel is assigned. Options are:</p> <ul style="list-style-type: none"> • Dynamic – Port channel MAC address is chosen as MAC address of an active port in the Port channel. • Force – Port channel MAC address configured through Admin MAC address is used. <p>Default MAC Selection is Dynamic.</p>
Force MAC	Specifies the MAC Address that is assigned to the Port channel. For this, the MAC selection mode must be Force.
No Of Ports Per Channel	Indicates the number of ports that are bundled per port channel.
No Of HotstandBy Ports	Indicates the number of ports that are in standby state per port channel.

3. Click **Apply** for the configuration to take effect. If you wish to discard the information you have entered, click **Reset**.

4.7.4 Port Settings

The **LA Port Settings** page allows you to configure the LA properties at per-port level.

To configure LA Port Settings

1. Select **Layer2 Management > LA > Port Settings** to open the **LA Port Settings** page.

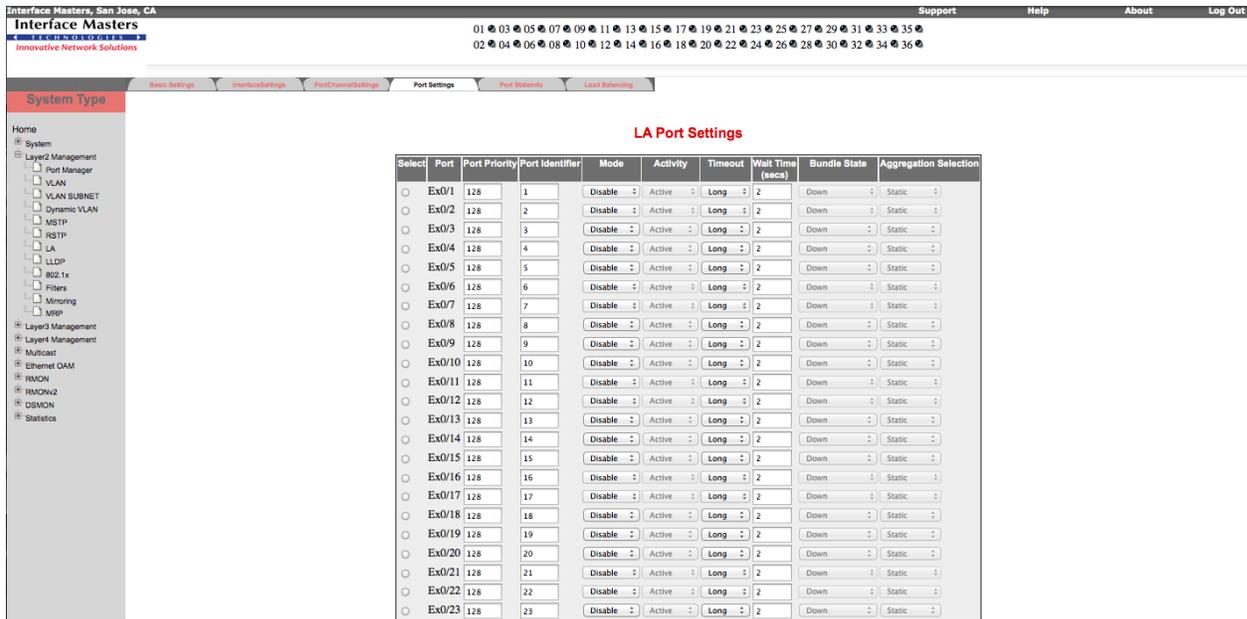


Figure 4-33: LA Port Settings – Layer 2 Group

2. Configure the attributes described in Table 4-32.

Table 4-32: LA Port Settings

Field	Description
Port	Specifies the Interface Index.
Port Priority	Specifies the Priority value of the Port.
Port Identifier	Specifies the Port Identity Number.
Mode	Specifies the various Port Modes. Options are: <ul style="list-style-type: none"> Lacp – Places the port into passive negotiation state, in which the port waits for its peer to initiate negotiation. Manual – Forces the port to enable channeling. Disable – Disables channeling.
Activity	Specifies the Port LACP Activity. Options are: <ul style="list-style-type: none"> Active Passive
Timeout	Specifies the time within which LACP PDUs must be received on a port to avoid timing out of the Aggregated Link. Options are: <ul style="list-style-type: none"> Long – The ports will time out of the Port channel in 90 seconds. Short –The ports will time out of the Port channel in 3 seconds.
Wait Time (secs)	Specifies the waiting time for a port after receiving Partner information and before entering aggregation. This value ranges between 0 and 10 seconds. Default value is 2 seconds.
Bundle State	Indicates the current state of the port with respect to Link Aggregation. Options are: <ul style="list-style-type: none"> Up In Bundle – The Port is an active member of the Port channel. Up Individual – The Port is not a member of any Port channel but its Oper-Status

Field	Description
	is Up. <ul style="list-style-type: none"> Standby – The Port is a member of the Port channel but is currently in standby state. Down – The Ports Oper-Status is Down.
Aggregation Selection	Specifies whether the port chooses its aggregator dynamically or it is configured statically. Options are: <ul style="list-style-type: none"> Static – The port is involved only in static aggregation, that is, the port can be a member of only the aggregation to which it is configured. Dynamic – The port participates in dynamic aggregation selection, that is, the port will be a part of best aggregation selected based on System ID and Admin key. Default Aggregation Type is Static. <input type="checkbox"/> This is set to Dynamic, once the port is configured as a default port of a port channel.

3. Click **Apply** for the configuration to take effect.

4.7.5 Port StateInfo

The **LA Port StateMachine Information** page displays the mapping between the Port channel, the Port and the aggregation state.

To view LA Port StateMachine Information

- Select **Layer2 Management > LA > Port StateInfo** to open the **LA Port StateMachine Information** page.

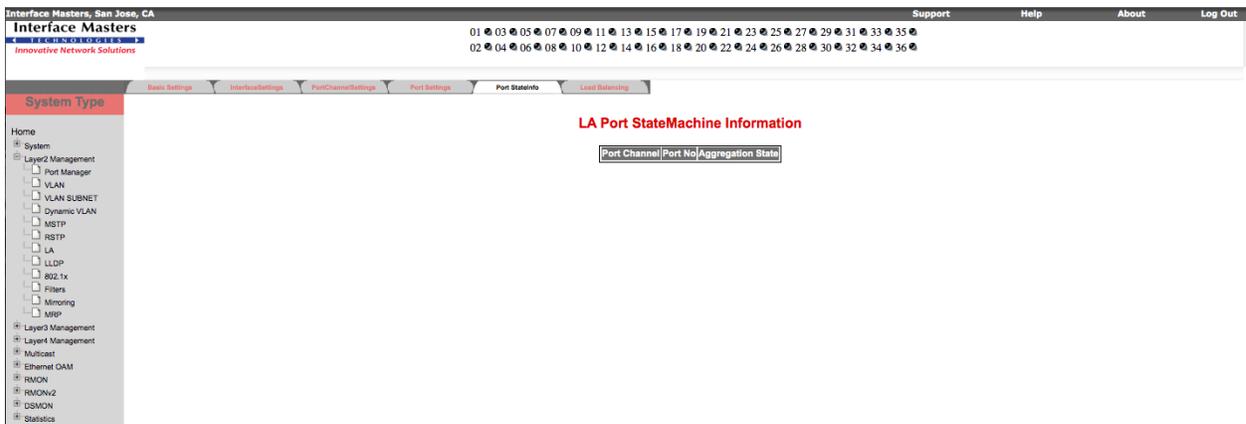


Figure 4-34: LA Port StateMachine Information – Layer 2 Group

- The attributes are described in Table 4-33.

Table 4-33: LA Port StateMachine Information

Field	Description
Port Channel	Specifies the identifier of the port channel interface.

Field	Description
Port No	Specifies the port number.
Aggregation State	Specifies the aggregation state of the port.

4.7.6 Load Balancing

The **LA Load Balancing Policy** page allows you to choose the selection policy for load distribution on the aggregated links.

To configure LA Load Balancing Policy

1. Select **Layer2 Management > LA > Load Balancing** to open the **LA Load Balancing Policy** page.

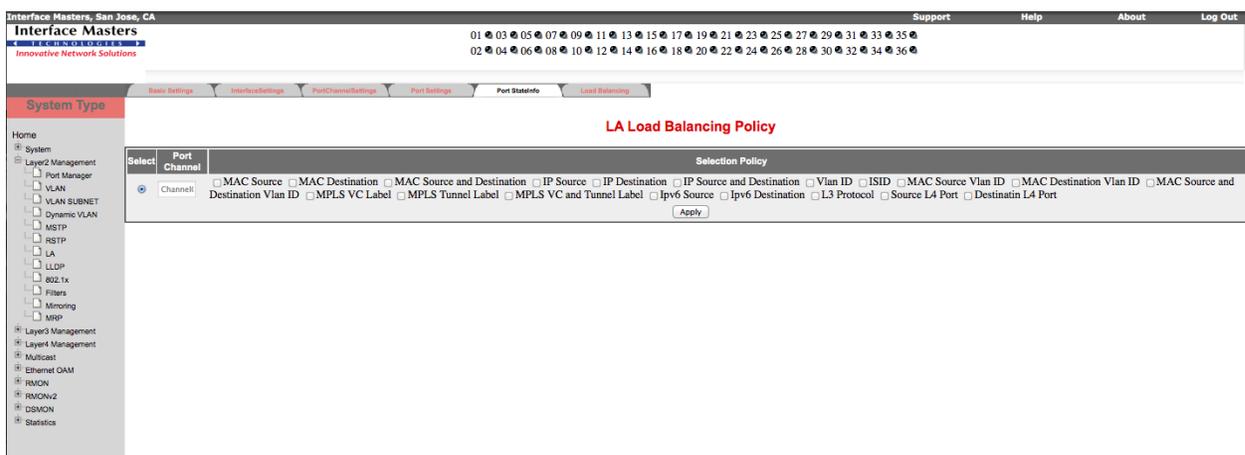


Figure 4-35: LA Load Balancing Policy - Layer 2 Group

2. Select the required selection policy. It can be any one of the following:
 - MAC Source
 - MAC Destination
 - MAC Source and Destination
 - IP Source
 - IP Destination
 - IP Source and Destination
 - VLAN ID
3. Click **Apply** for the configuration to take effect.

4.8 802.1x

The **802.1x** link allows you to configure the 802.1x information through the following links:

- Basic Settings
- Port Settings
- Timers
- Local AS
- Radius Settings
- MacSession Info

By default, the **802.1x Basic Settings** page is loaded.

4.8.1 Basic Settings

The **802.1x Basic Settings** page allows you to configure the basic settings of 802.1x.

To configure 802.1x Basic Settings

1. Select **Layer2 Management > 802.1x** to open the **802.1x Basic Settings** page.

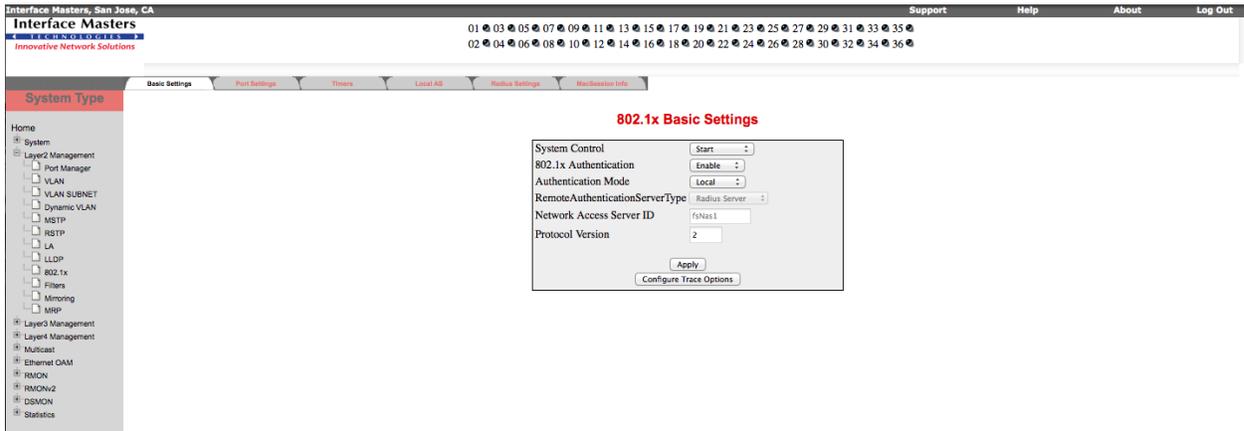


Figure 4-36: 802.1x Basic Settings - Layer 2 Group

2. Configure the attributes described in Table 4-34.

Table 4-34: 802.1x Basic Settings

Field	Description
System Control	Specifies the system control status of the PNAC module in the system. Options are: <ul style="list-style-type: none"> • Start – Resources required by PNAC module are allocated and PNAC module starts running. • Shutdown – All resources used by PNAC module is released to the system and the PNAC module is shut down.
802.1x Authentication	Specifies the status of 802.1x based port security feature in the switch. Options are:

Field	Description
	<ul style="list-style-type: none"> Enable – Enables 802.1x based port security feature in the switch. Disable – Disables 802.1x based port security feature in the switch.
Authentication Mode	Specifies the Authentication Server Location. Options are: <ul style="list-style-type: none"> Remote Local
RemoteAuthenticationServerType	Specifies the Remote Authentication Server Type. Options are: <ul style="list-style-type: none"> Radius Server Tacacs Server
Network Access Server ID	Specifies the Authenticator ID, which originates the Access-Request Packets.
Protocol Version	Specifies the Version Number of the Protocol.

3. Click **Apply** for the configuration to take effect.

4.8.2 Port Settings

The **802.1x Port Settings** page allows you to configure the security information at the individual port levels.

To configure 802.1x Port Settings

1. Select **Layer2 Management > 802.1x > Port Settings** to open the **802.1x > Port Settings** page.

The screenshot displays the '802.1x Port Settings' configuration page. The interface includes a navigation sidebar on the left with options like 'System Type', 'Layer2 Management', and 'Layer3 Management'. The main content area features a table with the following columns: Select, Port, Port Control, Authentication Mode, Auth PortStatus, Supp PortStatus, Access Control, Configured Control Direction, Operational Control Direction, AuthSM State, SuppSM State, Restart Authentication, Authentication Retry Count, Reauth, and Authentication Max Start. Each row represents a port configuration, showing values such as 'ForceAuthorized', 'Port Based', 'Authorized', 'Unauthorized', 'INACTIVE', 'Both', 'Both', 'Initialize', 'Disconnected', 'False', '2', and 'Disabled'.

Figure 4-37: 802.1x Port Settings - Layer 2 Group

2. Configure the attributes described in Table 4-35.

Table 4-35: 802.1x Port Settings

Field	Description
Port	Specifies the index of the port.
Port Control	Specifies the control values of the Authenticator Port. Options are: <ul style="list-style-type: none"> • ForceAuthorized – Allows all the traffic through this port. • ForceUnauthorized – Blocks all the traffic through this port. • Auto – Imposes 802.1x authentication process in this port.
Access Control	Specifies the Access Control status for the port. Options are: <ul style="list-style-type: none"> • INACTIVE – The port uses only the Authenticator authorization state to restrict access to the port and not the the Supplicant authorization state. • ACTIVE – The port applies both the Supplicant authorization state and Authenticator authorization state. By default, this is INACTIVE.
Auth Port Status	Specifies the current status of the Authenticator Port. Options are: <ul style="list-style-type: none"> • Authorized • Unauthorized
Supp Port Status	Specifies the current status of the Supplicant PAE state machine. Options are: <ul style="list-style-type: none"> • Authorized • Unauthorized
Authentication Mode	Specifies the configuration for selecting the authentication mode. Options are: <ul style="list-style-type: none"> • Port Based • Mac Based
Configured Control Direction	Specifies the current value of the administrative controlled directions parameter for the port. Options are: <ul style="list-style-type: none"> • Both • In
Operational Control Direction	Specifies the current value of the operational controlled directions parameter for the port. Options are: <ul style="list-style-type: none"> • Both • In
Auth SM State	Specifies the state of the Authenticator State Machine. Options are: <ul style="list-style-type: none"> • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuth

Field	Description
	<ul style="list-style-type: none"> ForceUnauth
SuppSMState	Specifies the state of the Supplicant State Machine. Options are: <ul style="list-style-type: none"> Disconnected Logoff Connecting Authenticating Authenticated Acquired Held ForceAuth ForceUnauth
Restart Authentication	Specifies the initialization control for the port to restart authentication. Options are: <ul style="list-style-type: none"> True – Causes the Port to be initialized. False – Reverts to False once initialization is complete.
Authentication Retry Count	Specifies the maximum number of authentication requests that can be sent from the authenticator before getting response from the supplicant. This value ranges between 1 and 10. Default value is 2.
Reauth	Enables / disables re-authentication mechanism on the port. Options are: <ul style="list-style-type: none"> Enabled Disabled By default, this is Disabled.

- Click **Apply** for the configuration to take effect.

4.8.3 Timers

The **802.1x Timer Configuration** page allows you to configure the Timer parameters at the individual port level.

To configure 802.1x Timer

- Select **Layer2 Management > 802.1x > Timers** to open the **802.1x Timer Configuration** page.

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"/>	Ex0/1	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/2	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/3	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/4	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/5	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/6	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/7	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/8	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/9	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/10	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/11	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/12	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/13	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/14	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/15	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/16	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/17	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/18	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/19	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/20	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/21	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/22	60	30	3600	30	30	60	30	30
<input type="radio"/>	Ex0/23	60	30	3600	30	30	60	30	30

Figure 4-38: 802.1x Timer Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-36.

Table 4-36: 802.1x Timer Configuration

Field	Description
Port	Specifies the index of the port.
Quiet Period (secs)	Specifies the duration for which the authenticator will be silent and will not attempt to acquire a supplicant. This value ranges between 0 and 65535 seconds. Default value is 60 seconds.
Transmit Period (secs)	Specifies the Time Period used by the Authenticator State machine to define when the EAPOL PDU is to be transmitted. This value ranges between 1 and 65535 seconds. Default value is 30 seconds.
Re-authentication Period (secs)	Specifies the time between periodic re-authentication of the supplicant. This value ranges between 1 and 65535 seconds. Default value is 3600 seconds.
Supplicant Timeout	Specifies the amount of time the switch waits for a response before retransmitting the request to the client, when relaying a request from the authentication server to the client. This value ranges between 1 and 65535 seconds. Default value is 30 seconds.
Server Timeout	Specifies the amount of time the switch waits for a reply before retransmitting the response to the server, when relaying a response from the client to the authentication server. This value ranges between 1 and 65535 seconds. Default value is 30 seconds.
Held Period	Specifies the amount of time the client will wait before re-attempting a failed 802.1X authentication. This value ranges between 1 and 65535 seconds. Default value is 60.
Auth Period	Specifies the time interval for resending 802.1X request messages after not receiving a response.

Field	Description
	This value ranges between 1 and 65535 seconds. Default value is 30 seconds.
Start Period	Specifies the time interval for resending Start messages.
	This value ranges between 1 and 65535 seconds. Default value is 30 seconds.

3. Click **Apply** for the configuration to take effect.

4.8.4 Local AS

The **Local Authentication Server Configuration** page allows you to configure the Local Authentication Server information.

1. Select **Layer2 Management > 802.1x > Local AS** to open the **Local Authentication Server Configuration** page.

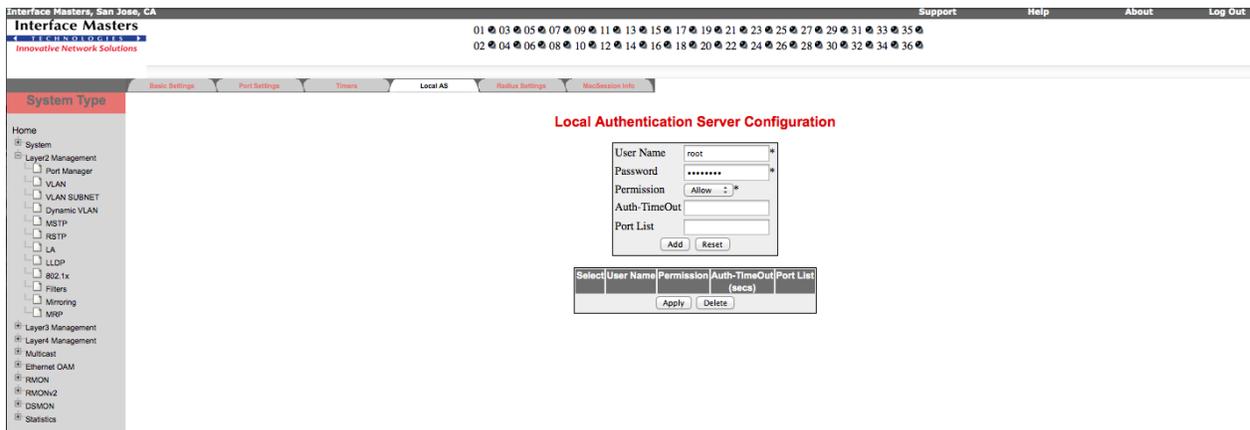


Figure 4-39: Local Authentication Server Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-37.

Table 4-37: Local Authentication Server Configuration

Field	Description
User Name	Specifies the identity of the user, seeking authentication. This field is a string of size not more than 20 printable characters.
Password	Specifies the password specific to the user name. This field is a string of size not more than 20 printable characters.
Permission	Specifies the allowance and denial of access. Options are: <ul style="list-style-type: none"> • Allow - Authentication request is allowed over the set of ports in the Port List. • Deny - Authentication request is not allowed over the set of ports in the Port List.
Auth-TimeOut (secs)	Specifies the Authentication Timeout in seconds. This value ranges between 1 and 7200 seconds.
Port List	Represents the complete set of ports of the authenticator to which the user is allowed or denied access, based on permission .

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.8.5 Radius Settings

The **Radius Server Configuration** page allows you to configure the Radius Server information.

To configure Radius Server

1. Select **Layer2 Management > 802.1x > Radius Settings** to open the **Radius Server Configuration** page.

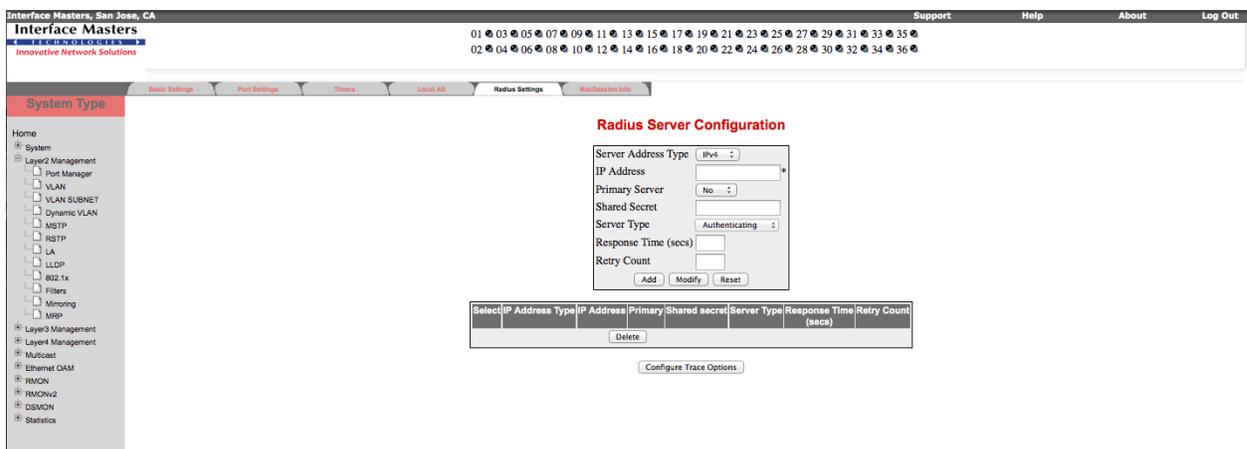


Figure 4-40: Radius Server Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-38.

Table 4-38: Radius Server Configuration

Field	Description
Server Address Type	Specifies the Radius server address type. Options are: <ul style="list-style-type: none"> • IPV4 - Internet Protocol Version 4 • IPV6 - Internet Protocol Version 6
IP Address	Specifies the IP Address of the Radius Server.
Primary Server	Specifies whether the server is a primary server or not. Only one server can be configured as the primary server. Options are: <ul style="list-style-type: none"> • Yes • No

Field	Description
Shared Secret	Specifies the secret string, which is to be shared between the Radius Server and the Radius Client.
Server Type	Specifies the RADIUS server type. Options are: <ul style="list-style-type: none"> • Authenticating • Accounting • Both
Response Time (secs)	Specifies the maximum time within which the Radius Server has to respond for a request from the Radius Client. This value ranges between 1 and 120 seconds.
Retry Count	Specifies the maximum number of times a radius request is to be re-transmitted before getting response from the Radius Server. This value ranges between 1 and 254.
Server ID	Specifies the unique identifier of the Radius Server Entry. This value ranges between 1 and 10.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.8.6 MacSession Info

The **MAC Session Info** page displays the MAC Session information details.

To view MAC Session Info

1. Select **Layer2 Management > 802.1x > MacSession Info** to open the **MAC Session Info** page.

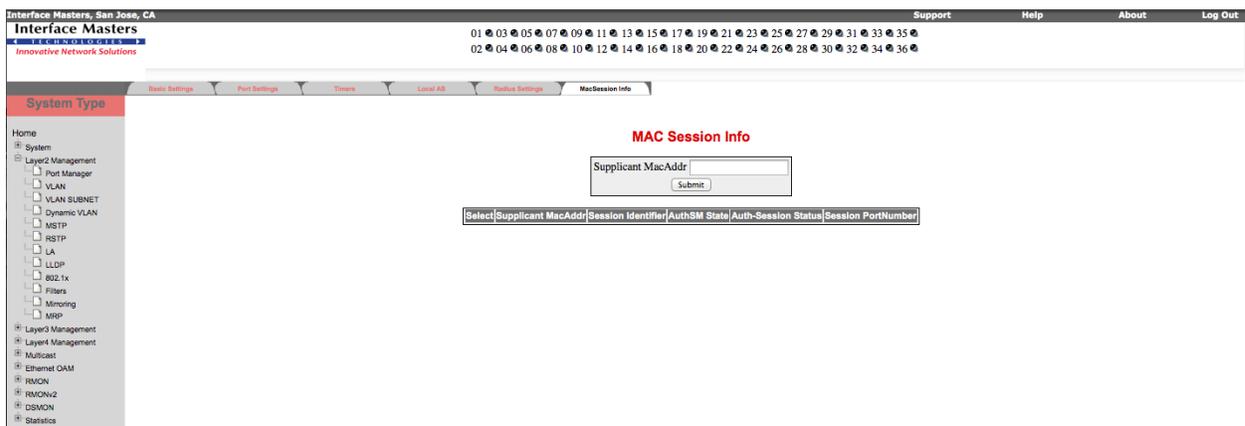


Figure 4-41: Mac Session Info - Layer 2 Group

2. Configure the attributes described in Table 4-39.

Table 4-39: Mac Session Info

Field	Description
Supplicant MacAddr	Specifies the Supplicant MAC Address.
Session Identifier	Specifies the Session Identifier of the supplicant.
AuthSM State	Specifies the state of the Authenticator State Machine.
Auth Session Status	Specifies the Authentication Session Status.
Session PortNumber	Specifies the port number through which a particular Session MAC address is learnt.

- Click **Submit** to view the MAC Session information.

4.9 Filters

The **Filters** link allows you to configure Layer 2 packet filtering through the following links:

- Unicast Filters
- Multicast Filters
- Multicast Forwarding

By default, the **L2 Unicast Filter Configuration** page is loaded.

4.9.1 Unicast Filters

The **L2 Unicast Filter Configuration** page allows you to configure the filter for controlling the unicast packets that the switch needs to process.

To configure L2 Unicast Filter

- Select **Layer2 Management > Filters** to open the **L2 Unicast Filter Configuration** page.

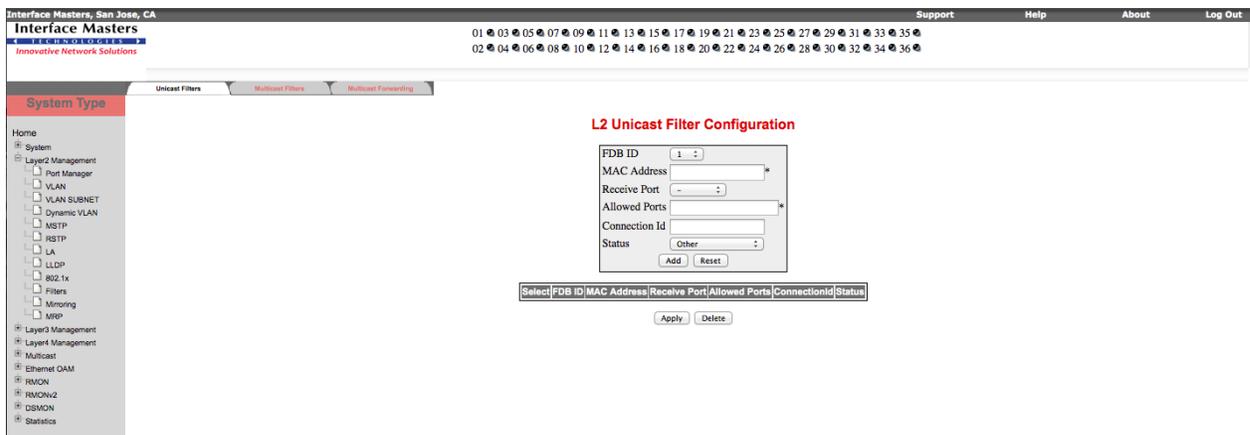


Figure 4-42: L2 Unicast Filter Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-40.

Table 4-40: L2 Unicast Filter Configuration

Field	Description
FDB ID	Specifies the FDB (Forwarding Database) ID.
MAC Address	Specifies the destination MAC address of the received packet.
Receive Port	Specifies the port on which the packet is received.
Allowed Ports	Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) can be forwarded.
Status	Specifies the configuration types. Options are: <ul style="list-style-type: none"> Other – Currently in use, but the conditions under which it will remain so differ from the following values. Permanent – Entry resides even after restart of the switch. DeleteOnReset – Deletes the entry on restart. DeleteOnTimeout – Deletes the entry on expiry of the ageing timer.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.9.2 Multicast Filters

The **L2 Multicast Filter Configuration** page allows you to configure the filter for controlling the multicast packets that the switch needs to process.

To configure L2 Multicast Filter

1. Select **Layer2 Management > Filters > Multicast Filters** to open the **L2 Multicast Filter Configuration** page.

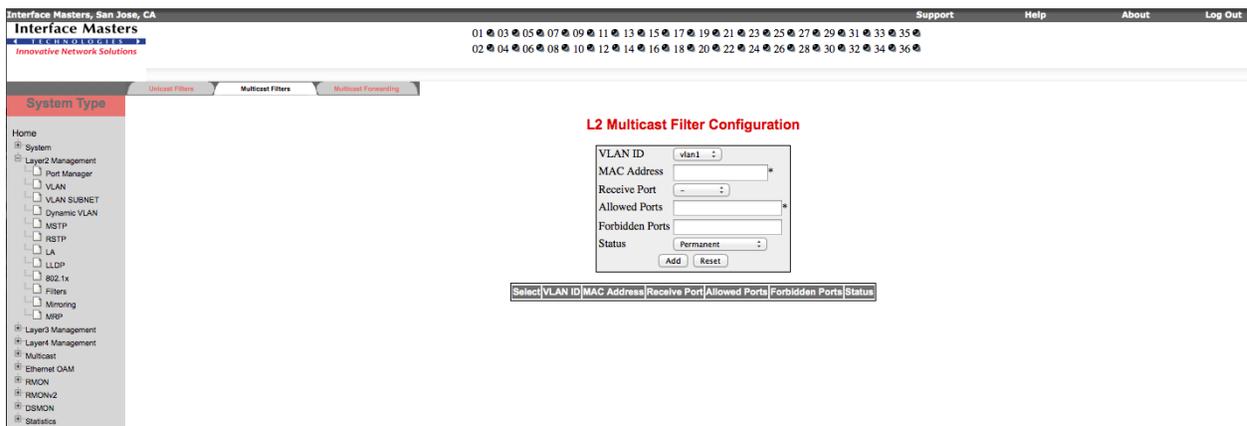


Figure 4-43: L2 Multicast Filter Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-41.

Table 4-41: L2 Multicast Filter Configuration

Field	Description
VLAN ID	Specifies the VLAN ID.
MAC Address	Specifies the destination MAC address of the received packet.
Receive Port	Specifies the port on which the packet is received.
Allowed Ports	Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) can be forwarded.
Forbidden Ports	Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) must not be forwarded.
Status	Specifies the configuration types. Options are: <ul style="list-style-type: none"> • Other – Currently in use, but the conditions under which it will remain so differ from the following values. • Permanent – Entry resides even after restart of the switch. • DeleteOnReset – Deletes the entry on restart. • DeleteOnTimeout – Deletes the entry on expiry of the ageing timer.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

4.9.3 Multicast Forwarding

The **Forward Ports Configuration** page allows you to configure the ports for Multicast Forwarding.

To configure Forward Ports

1. Select **Layer2 Management > Filters > Multicast Forwarding** to open the **Forward Ports Configuration** page.

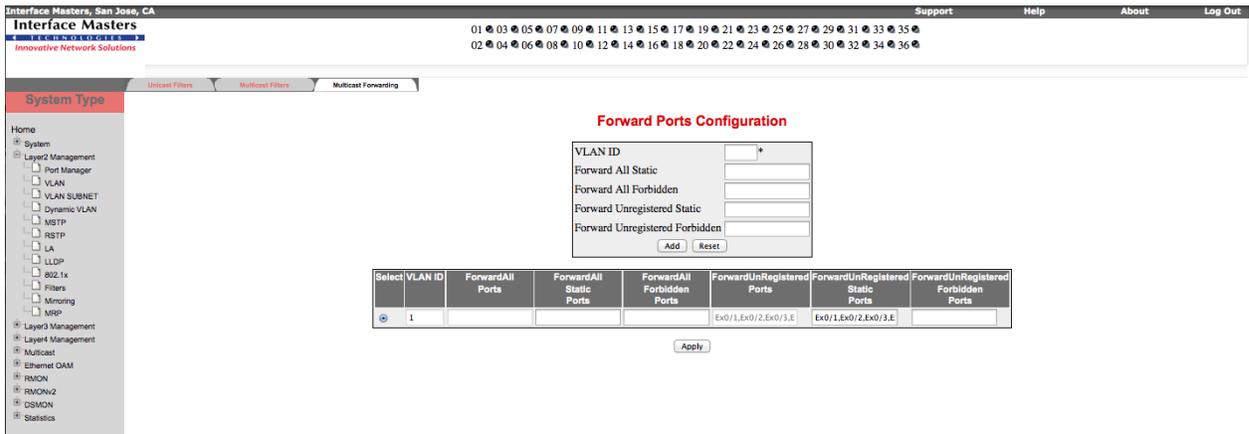


Figure 4-44: Forward Ports Configuration - Layer 2 Group

2. Configure the attributes described in Table 4-42.

Table 4-42: Forward Ports Configuration

Field	Description
VLAN ID	Specifies the VLAN ID.
Forward All Ports	Specifies the forward all static ports as well as forward all learnt ports. This is a read-only field.
Forward All Static ports	Specifies all the static ports to allow Multicast forwarding.
Forward All Forbidden ports	Specifies all the forbidden ports to deny Multicast forwarding.
Forward Unregistered Ports	Specifies the forward unregistered static ports as well as forward unregistered learnt ports. This is a read-only field.
Forward Unregistered Static ports	Specifies all the unregistered static ports to allow Multicast forwarding.
Forward Unregistered Forbidden ports	Specifies all the unregistered forbidden ports to deny Multicast forwarding.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.

Chapter

5

Layer-3 Management

This chapter describes the configuration of the various features of the Layer-3 interface.

The **Layer-3 Management** link on the left pane opens the **Layer 3 Management** page. This page provides the following links:

- IP
- DHCP Server
- DHCP Relay
- **Error! Reference source not found.**

Interface Masters, San Jose, CA

Interface Masters

Support Help About Log Out

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

System Type

Home

- System
- Layer2 Management
- Layer3 Management
 - IP
 - RARP
 - DHCP Server
 - DHCP Relay
 - RIP
 - OSPF
 - ISIS
 - BGP
 - BGP4
 - RRD
 - VRRP
- Layer4 Management
- Multicast
- Ethernet OAM
- RMON
- RMON2
- DSMON
- Statistics

Welcome to the Layer3 Management Page

The various layer3 features of the IM can be configured through the links available in this page.

Through the [IP](#) link you can configure the Routes and also create VLAN interfaces.

[DHCP](#) can be enabled through the DHCP Server link. You can configure the pool of addresses to be assigned to the DHCP Client from here.

[DHCP Relay](#) link helps you to configure the DHCP Relay status and other related information.

[RIP](#) link enables you to configure the RIP feature. RIP neighbours and other related information can also be configured through this link.

Through the [OSPF](#) link you can configure the OSPF status, Area configuration, the various interfaces associated with it and also create virtual interfaces.

Through the [ISIS](#) link you can configure the Instance list, Summary-Address Table, IPRA Table, Circuit Entry Table, Circuit Level Table.

Through the [BGP](#) link you can configure the Neighbour list, Multi-Exit Discriminators, Filters and Route Aggregation.

Through the [BGP4](#) link you can configure the confederation, RFD, community filters, community route set status, community routes, extended community filters, extended community route set status, extended community routes.

Through the [RRD](#) link you can enable the RRD status and also configure the filters, BGP, RIP, OSPF related information.

Through the [VRRP](#) link you can configure VRRP for a particular interface.

Figure 5-1: Layer 3 Management Page

5.1 IP

The **IP** link enables to perform the IP related configuration through the following links:

- Vlan Interface
- IPv4 AddrConf
- IP route
- LoopBack Settings

By default, the **VLAN Interface Basic Settings** page is loaded.

5.1.1 Vlan Interface

The **VLAN Interface Basic Settings** page allows you to configure the basic settings of the VLAN interface.

To configure VLAN Interface Basic Settings

1. Select **Layer3 Management > IP** to open the **VLAN Interface Basic Settings** page.

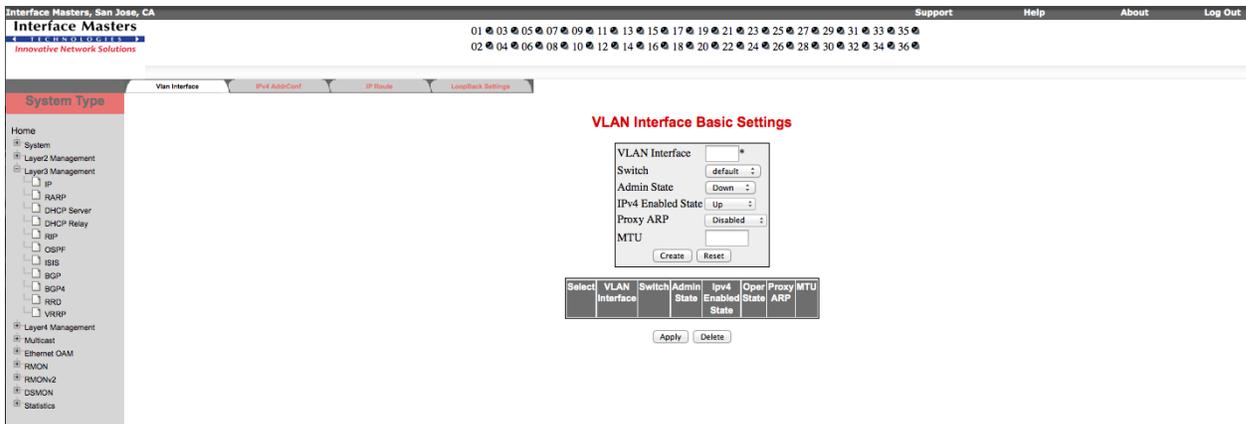


Figure 5-2: VLAN Interface Basic Settings - - Layer 3 Group

2. Configure the attributes described in Table 5-1.

Table 5-1: VLAN Interface Basic Settings

Field	Description
VLAN Interface	Specifies the VLAN ID that is to be created. This ranges between 1 and 4094.
Switch	Specifies the name of the switch context.
Admin State	Specifies the Admin Status of the VLAN interface. Options are: <ul style="list-style-type: none"> • Up • Down
IPv4 Enabled State	Specifies whether IPv4 is enabled (up) or disabled (down) on the interface. Options are: <ul style="list-style-type: none"> • Up

Field	Description
	<ul style="list-style-type: none"> Down
Oper State	<p>Specifies the Operational Status of the VLAN interface. This is a read-only field. Options are:</p> <ul style="list-style-type: none"> Up Down
Proxy ARP	<p>Specifies the Proxy ARP admin status for the interface. Options are:</p> <ul style="list-style-type: none"> Enabled – Proxy ARP feature is enabled. Disabled – Proxy ARP feature is disabled. <p>By default, Proxy ARP is disabled.</p>
MTU	<p>Specifies the Maximum Transmission Unit.</p> <p>This value ranges between 90 and 9202.</p>

- Click **Create** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

5.1.2 IPv4 AddrConf

The **IPv4 Interface Settings** page allows you to configure the settings of the IPv4 interface.

To configure IPv4 Interface Settings

- Select **Layer3 Management > IP > IPv4 AddrConf** to open the **IPv4 Interface Settings** page.

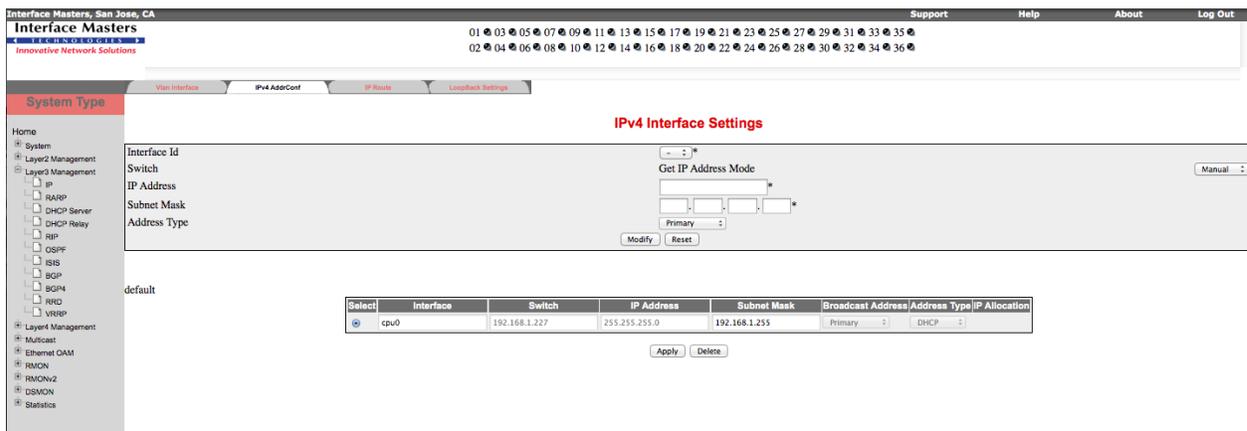


Figure 5-3: IPv4 Interface Settings- Layer 3 Group

- Configure the attributes described in Table 5-2.

Table 5-2: IPv4 Interface Settings

Field	Description
Interface VLAN Id	Specifies the index of the VLAN interface.
Switch	Specifies the name of the switch context.
IP Address	Specifies the IP Address of the interface.
Subnet Mask	Specifies Subnet Mask for the provided IP Address.
Broadcast Address	Indicates the Broadcast address for the specified IP address. This is a read-only field.
Address Type	Specifies the type of address. Options are: <ul style="list-style-type: none"> • Primary • Secondary The default address type is Secondary.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry, modify the parameters and click **Apply**. In the pop-up window, click **OK** for the configuration to take effect or click **Cancel** if you wish to cancel the modification.
5. Select the required entry and click **Delete**. In the pop-up window, click **OK** for the entry to be deleted or click **Cancel** if you wish to cancel the deletion.

5.1.3 IP route

The **IP Route Configuration** page allows you to configure IP route information.

To configure IP Route

1. Select **Layer3 Management > IP > IP route** to open the **IP Route Configuration** page.

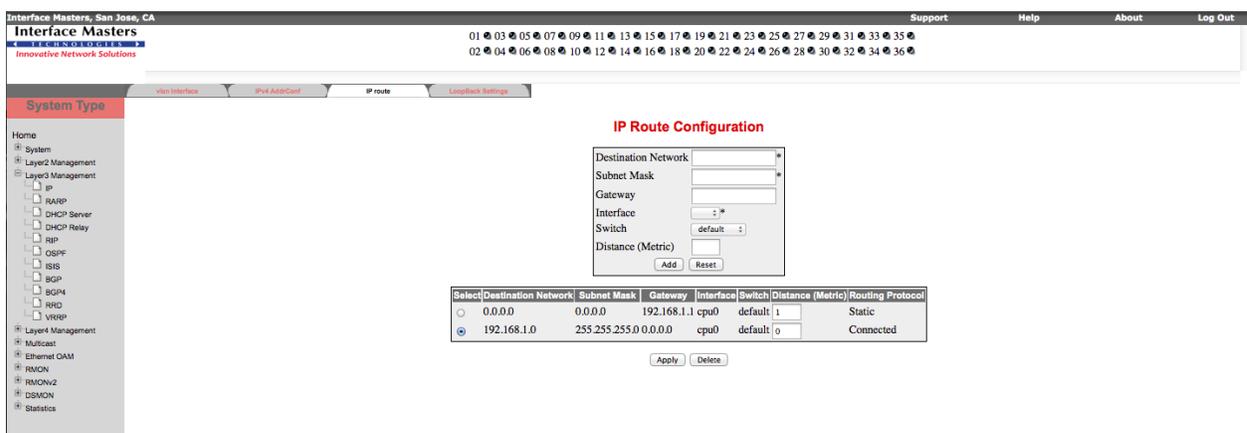


Figure 5-4: IP Route Configuration - Layer 3 Group

- Configure the attributes described in Table 5-3.

Table 5-3: IP Route Configuration

Field	Description
Destination Network	Specifies the Network Address for which the route is being added.
Subnet Mask	Specifies the subnet mask for the Destination Network address.
Gateway	Specifies the Next Hop gateway to reach the Destination Network.
Interface	Specifies the outgoing interface through which the Destination Network is reachable.
Switch	Specifies the name of the switch context.
Distance (Metric)	Specifies the Metric value of the destination. This value ranges between 1
Routing Protocol	Indicates the routing protocol through which the route was learnt, if the route is not a directly connected network or a static route. This cannot be configured.

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
- Select the required entry and click **Delete** for the entry to be deleted.

5.1.4 LoopBack Settings

The **LoopBack Basic Settings** page allows you to configure the basic loopback settings.

To configure LoopBack Basic Settings

- Select **Layer3 Management > IP > LoopBack Settings** to open the **LoopBack Basic Settings** page.

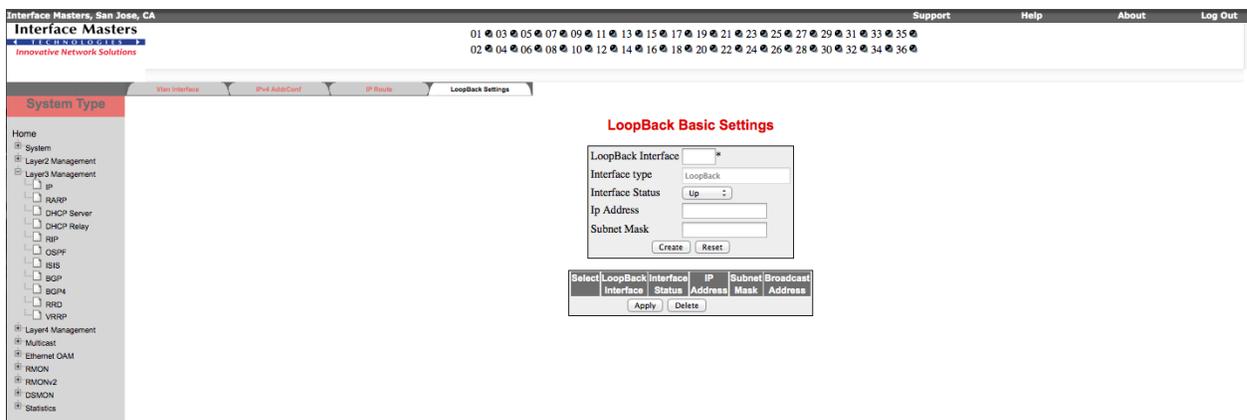


Figure 5-5: LoopBack Basic Settings - Layer 3 Group

2. Configure the attributes described in Table 5-4.

Table 5-4: LoopBack Basic Settings

Field	Description
LoopBack Interface	Specifies the Loopback Interface that is to be created.
Interface type	Specifies the interface type as Loopback. This field is not configurable.
Interface Status	Specifies the Interface Status. Options are: <ul style="list-style-type: none"> • Up • Down
Ip Address	Specifies the IP Address for the Loopback interface.
Subnet Mask	Specifies the Subnet mask for the given IP Address.
Broadcast Address	Specifies the Broadcast address for the specified IP address. This is a read-only field.

3. Click **Create** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

5.2 DHCP Server

The **DHCP Server** link allows you to manage the DHCP server in the switch through the following links:

- Basic Settings
- Pool Settings

By default, the **DHCP Basic Settings** page is loaded.

5.2.1 Basic Settings

The **DHCP Basic Settings** page allows you to configure the basic DHCP settings.

To configure DHCP Basic Settings

1. Select **Layer3Management > DHCP Server** to open the **DHCP Basic Settings** page.

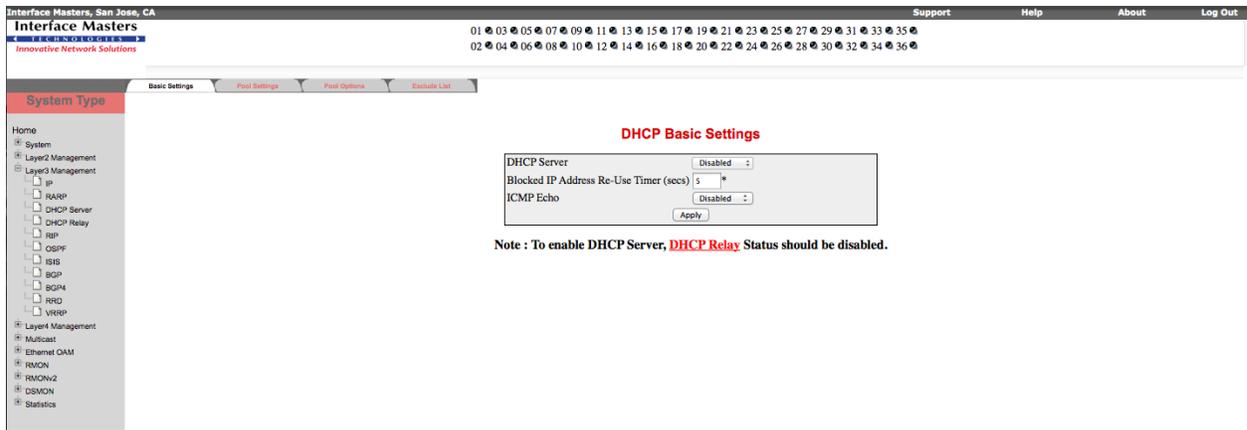


Figure 5-6: DHCP Basic Settings - Layer 3 Group

- Configure the attributes described in Table 5-5.



To enable DHCP Server, DHCP Relay Status should be disabled.

Table 5-5: DHCP Basic Settings

Field	Description
DHCP-Server	Specifies the DHCP server status in the router. Options are: <ul style="list-style-type: none"> Enabled – Enables the DHCP server in the router. Disabled – Disables the DHCP server in the router.
Blocked IP Address Re-Use Timer (secs)	Specifies the Reuse timeout value in seconds that is used by DHCP. This value ranges between 1 and 120 seconds. Default value is 5 seconds.
ICMP Echo	Specifies the status of ICMP (Internet Control Message Protocol) Echo feature. <ul style="list-style-type: none"> Enabled – Enables the ICMP Echo feature. Disabled – Disables the ICMP Echo feature. By default, this is Disabled.

- Click **Apply** for the configuration to take effect.

5.2.2 Pool Settings

The **DHCP Pool Settings** page allows you to configure the IP address pool that can be used by the DHCP server to allocate IP addresses.

To configure DHCP Pool Settings

- Select **Layer3Management > DHCP Server > Pool Settings** to open the **DHCP Pool Settings** page.

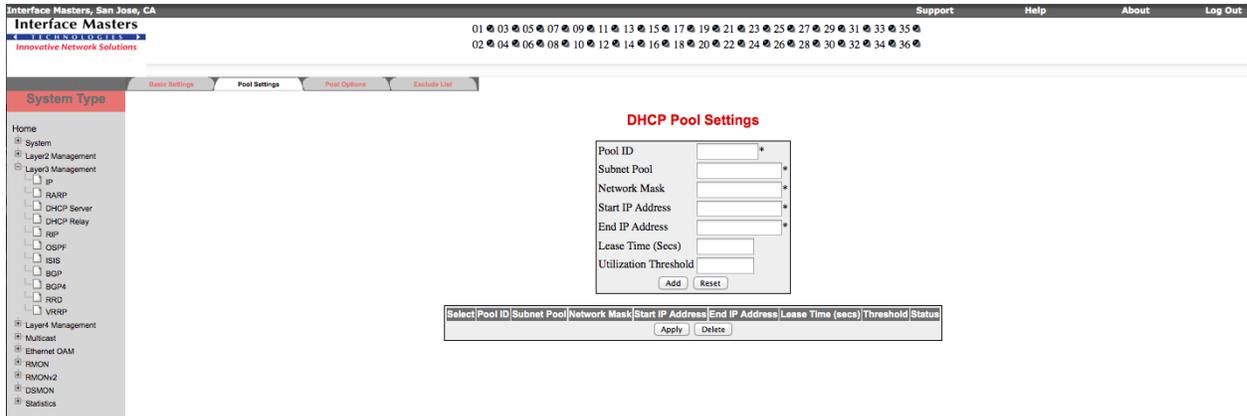


Figure 5-7: DHCP Pool Settings - Layer 3 Group

2. Configure the attributes described in Table 5-6.

Table 5-6: DHCP Pool Settings

Field	Description
Pool ID	Specifies the pool Id to index among the different subnet pools configured. The range of the pool ID is between 1 and 2147483647.
Subnet Pool	Specifies the subnet of the IP address in the pool.
Network Mask	Specifies the subnet mask of the IP address in the pool.
Start IP Address	Specifies the first IP address in the address pool that is used for dynamic allocation by the DHCP server.
End IP Address	Specifies the last IP address in the address pool that is used for dynamic allocation by the DHCP server.
Lease Time (Secs)	Specifies the time interval for which the IP address is valid. This value ranges between 1 and 2147483647.
Utilization threshold	Specifies the DHCP Pool utilization threshold value in percentage. The utilization threshold ranges between 0 and 100 percentage. Default value is 75 percentage.
Status	Specifies the status of the entry.

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

5.3 DHCP Relay

The **DHCP Relay** link allows you to manage the DHCP Relay in the switch through the following pages:

- Basic Settings
- Interface Conf

By default, the **DHCP Relay Configuration** page is loaded.

5.3.1 Basic Settings

The **DHCP Relay Configuration** page allows you to configure basic DHCP Relay information.

To configure DHCP Relay Settings

1. Select **Layer3Management > DHCP Relay** to open the **DHCP Relay Configuration** page.

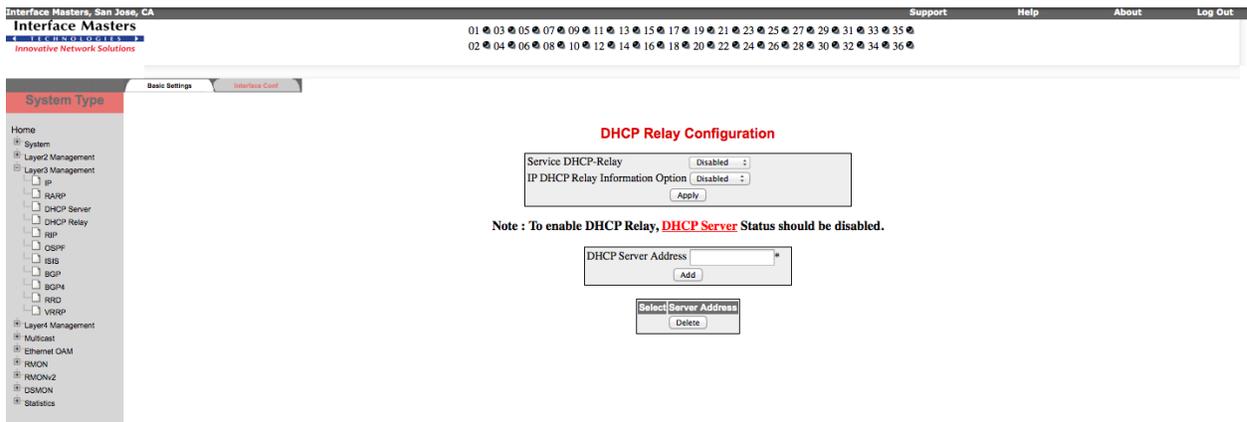


Figure 5-8: DHCP Relay Configuration - Layer 3 Group

2. Configure the attributes described in Table 5-7.



To enable DHCP Relay, DHCP Server Status should be disabled.

Table 5-7: DHCP Relay Configuration

Field	Description
Service DHCP-Relay	Specifies the DHCP relay status in the switch. Options are: <ul style="list-style-type: none"> • Enabled – Enables the DHCP relay status in the switch. • Disabled – Disables the DHCP relay status in the switch. By default, this is Disabled.
IP DHCP Relay Information Option	Specifies the controlling status of the processing related to the Relay Agent Information options. <ul style="list-style-type: none"> • Enabled – Enables the controlling status of the processing related to the Relay Agent Information options.

Field	Description
	<ul style="list-style-type: none"> Disabled – Disables the controlling status of the processing related to the Relay Agent Information options. <p>By default, this is Disabled.</p>
DHCP Server Address	Indicates the IP address of the DHCP Server to which the Relay Agent needs to forward the packets from the client.

3. Click **Apply** for the configuration to take effect.
4. Click **Add** to save the entry in the configuration table.
5. Select the required entry and click **Delete** for the entry to be deleted.

5.3.2 Interface Conf

The **DHCP Relay Interface Configuration** page allows you to configure the interface settings of the DHCP Relay.

To configure DHCP Relay Interface Settings

1. Select **Layer3Management > DHCP Relay > Interface Conf** to open the **DHCP Relay Interface Configuration** page.

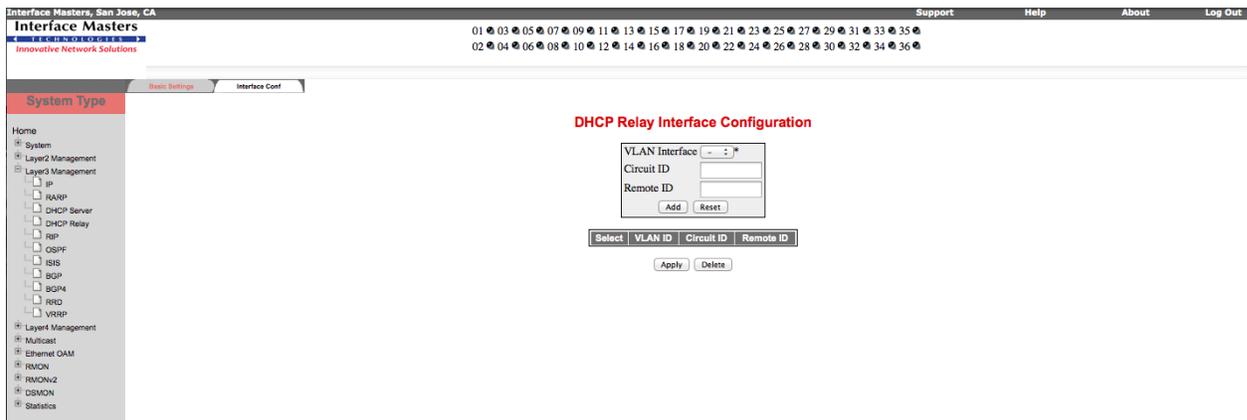


Figure 5-9: DHCP Relay Interface Configuration - Layer 3 Group

2. Configure the attributes described in Table 5-8.

Table 5-8: DHCP Relay Interface Configuration

Field	Description
VLAN Interface	Specifies the VLAN Interface.
Circuit ID	Specifies the Circuit ID that is to be configured for this interface. This value ranges between 1 and 2147483647. The minimum value configurable for circuit-id is system's maximum default interfaces + 1.
Remote ID	Specifies the Remote ID that is to be configured for this interface.

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

Chapter

6

Multicast

This chapter describes the Multicast protocols involved in transmitting a message to a set of selected multiple recipients. There are various multicast protocols such as IGS, IGMP, PIM, DVMRP, MLDS, GMRP, and so on.

The **Multicast** link on the left pane opens the **Multicast** page. This page provides the following links:

- IGMP Snooping
- **Error! Reference source not found.**
- Dynamic Multicast
- TAC

The screenshot shows the Interface Masters web user manual interface. At the top, there is a navigation bar with "Interface Masters, San Jose, CA" on the left and "Support", "Help", "About", and "Log Out" on the right. Below this is a breadcrumb trail: "01 > 03 > 05 > 07 > 09 > 11 > 13 > 15 > 17 > 19 > 21 > 23 > 25 > 27 > 29 > 31 > 33 > 35 > 02 > 04 > 06 > 08 > 10 > 12 > 14 > 16 > 18 > 20 > 22 > 24 > 26 > 28 > 30 > 32 > 34 > 36". The main content area is titled "System Type" and contains a "Welcome to the Multicast Page" message. Below the welcome message, there are several paragraphs of text, each starting with "Through the" followed by a link name in red: "IGS", "Dynamic multicast", "IGMP", "PIM", and "TAC". On the left side of the page, there is a navigation menu with a tree structure. The "Multicast" folder is expanded, showing sub-items: "IGMP Snooping", "Dynamic Multicast", "IGMP", "PIM", and "TAC". Other folders in the menu include "Home", "System", "Layer2 Management", "Layer3 Management", "Layer4 Management", "Ethernet OAM", "RMON", "RMON2", "DSMON", and "Statistics".

Figure 6-1: Multicast Management - Layer 3 Group

6.1 IGMP Snooping

IGMP is the protocol which 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.

The **IGMP Snooping** link provides the following links to configure IGS:

- Basic Settings
- Timer
- VlanConfiguration
- InterfaceConfiguration
- RouterPortConf
- RouterPorts
- FwdInformation
- McastReceiverInfo

By default, the **IGMP Snooping Configuration** page is loaded.

6.1.1 Basic Settings

The **IGMP Snooping Configuration** page allows you to configure the basic settings of IGS.

To configure IGS Basic Settings

1. Select **Multicast > IGMP Snooping** to open the **IGMP Snooping Configuration** page.

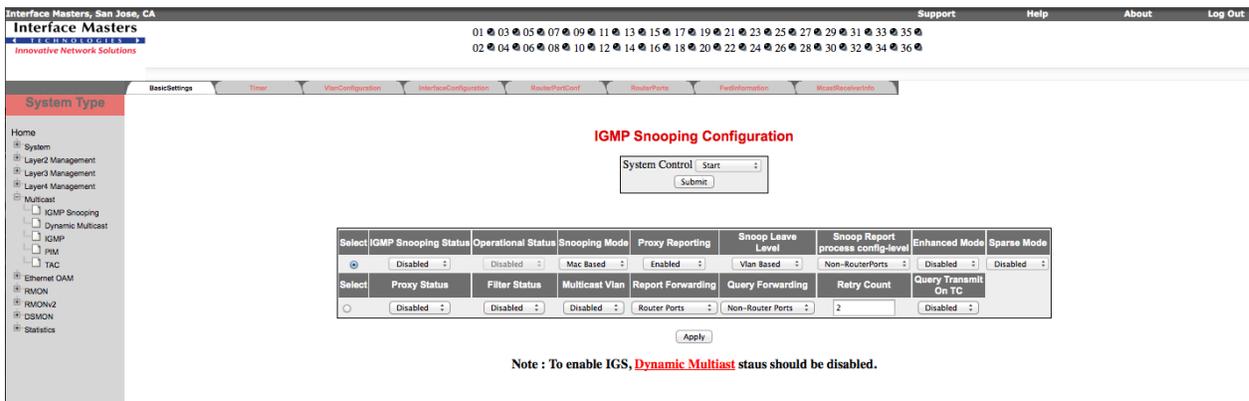


Figure 6-2: IGMP Snooping Configuration - Multicast Group

2. Configure the attributes described in Table 6-1.



To configure IGS, Dynamic Multicast status must be disabled.

Table 6-1: Enabling IGS

Field	Description
System Control	<p>Specifies the System Control status of IGS in the switch. Options are:</p> <ul style="list-style-type: none"> Start - Resources required by the IGS module is allocated and the module starts running. Shutdown - All the resources are released back to the system and the module stops running. <p>By default, the System Control status is Start.</p>

3. Click **Apply** to run the module.

Table 6-2: IGS Basic Settings

Field	Description
IGMP Snooping Status	<p>Specifies the Global status of IGS in the switch. Options are:</p> <ul style="list-style-type: none"> Enabled - IGS is enabled in all the existing VLAN interfaces. Disabled - IGS is disabled in all the existing VLAN interfaces. <p>By default, IGS global status is Disabled.</p>
Operational Status	<p>Specifies the Operational status of the IGS in the switch. Options are:</p> <ul style="list-style-type: none"> Enabled - Indicates that the IGS module is currently enabled in the system. Disable - Indicates that the IGS module is currently disabled in the system.
Proxy Reporting	<p>Specifies the Proxy Reporting status in the switch. Options are:</p> <ul style="list-style-type: none"> Enabled - Switch generates reports and forwards them to the router based on the available host information. Disabled - Switch forwards all v3 reports and a single V2 report to the router. <p>By default, Proxy-reporting status is Enabled in the system.</p>
Snooping Mode	<p>Specifies the IGMP snooping mode. Options are:</p> <ul style="list-style-type: none"> IP based - The hardware supports programming of S, G and *, G entries. MAC based - The hardware supports only MAC based multicast tables. <p>This configuration takes effect only on system reboot.</p> <p>By default, Snooping Mode is set to MAC Based</p>
Snoop Leave Level	<p>Specifies whether leave processing mechanism must be configured at the VLAN level or at port level. Options are:</p> <ul style="list-style-type: none"> Vlan Based – Configures the leave mechanism at the Vlan level Port Based – Configures the leave mechanism at port level. <p>By default, Snoop leave level is Vlan based</p>
Enhanced Mode	<p>Specifies the operating status of snooping module. Options are</p> <ul style="list-style-type: none"> Enabled – The snooping module operates in enhanced mode. Disabled – The snooping module operates in default mode. <p>By default, Enhanced mode is Disabled.</p>

Field	Description
Proxy Status	<p>Specifies the status of the Proxy in the system. Options are:</p> <ul style="list-style-type: none"> • Enabled – Enables proxy in the system • Disabled – Disables proxy in the system. <p><input type="checkbox"/> Proxy status can be enabled only if Proxy-reporting is disabled</p>
Filter Status	<p>Specifies the filter status. Options are:</p> <ul style="list-style-type: none"> • Enabled – Enables the IGS filtering feature • Disabled – Disables the IGS filtering feature <p>By default, Filter Status is Disabled</p>
Multicast Vlan	<p>Specifies the multicast Vlan status. Options are:</p> <ul style="list-style-type: none"> • Enabled – Enables the multicast Vlan feature • Disabled – Disables the multicast Vlan feature <p>By default, Multicast Vlan Status is Disabled.</p>
Report Forwarding	<p>Specifies whether the report must be forwarded on all ports or only on router ports. Options are:</p> <ul style="list-style-type: none"> • Router Ports – Forwards reports only on router ports • All Ports – Forwards reports on all ports <p>By default, Router Ports is selected.</p>
Retry Count	<p>Specifies the maximum number of group specific queries sent on a port on reception of an IGMPv2 leave message.</p> <p>This values range between one and five. Default value is 2 seconds.</p> <p><input type="checkbox"/> When the switch receives leave message on a port, it sends group specific query to check if there are any other interested receivers for the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the maximum retry count exceeds the RetryCount, then the port will be deleted from the multicast group membership information in the forwarding database and received leave message will be forwarded onto the router ports if there are no interested receivers for the group.</p>
Query Transmit on TC	<p>Specifies whether IGMP Snooping queries are transmitted whenever topology changes. Options are:</p> <ul style="list-style-type: none"> • Enabled • Disabled

4. Click **Apply** for the configuration to take effect.

6.1.2 Timer

The **IGMP Snooping Timer Configuration** page allows you to configure IGS Timer related information.

To configure IGS Timer Settings

1. Select **Multicast > IGMP Snooping > Timer** to open the **IGMP Snooping Timer Configuration** page.

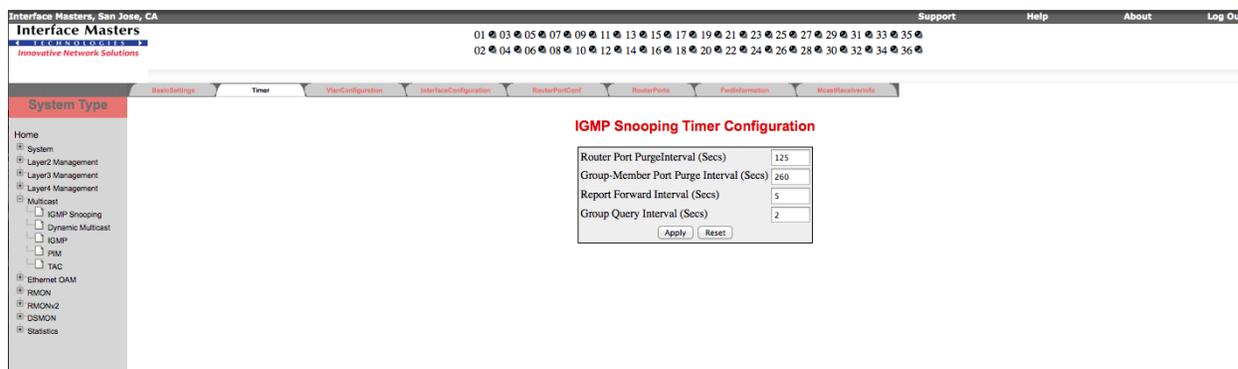


Figure 6-3: IGS Timer Settings - Multicast Group

- Configure the attributes described in Table 6-3.

Table 6-3: IGS Timer Settings

Field	Description
Router Port Purge Interval (Secs)	<p>Specifies the time interval after which the learnt router port will be purged. This value ranges between 60 and 600 seconds. Default value is 125 seconds.</p> <p><input type="checkbox"/> For each router port learnt, the timer runs for the configured port purge time interval. When the timer expires, the learnt router port entry is purged. However, if control messages are received from the router before the timer expiry, then the timer is restarted.</p>
Group-Member Port Purge Interval (Secs)	<p>Specifies the time interval after which a port gets deleted, if IGMP reports are not received on a port. This value ranges between 130 and 1225 seconds. Default value is 260 seconds.</p> <p><input type="checkbox"/> For each port on which report has been received, this timer runs for the configured time. This timer will be restarted whenever a report message is received from a host on the specific port. If the timer expires, then, the learnt port entry will be purged from the multicast group.</p>
Report Forward Interval (Secs)	<p>Specifies the time interval within which the next report messages for the same multicast group will not be forwarded. This value ranges between 1 and 25 seconds. Default value is 5 seconds.</p> <p><input type="checkbox"/> This timer is used when proxy-reporting is disabled; the switch then has to suppress multiple IGMPv2 report messages for the same group from being forwarded to the router. The Report Forward Timer is used per multicast group. This timer is started as soon as a report message for that group is forwarded out. Within this ReportForwardInterval if another report for the same group arrives, then that report will not be forwarded</p>
Group Query Interval (Secs)	<p>Specifies the interval within which the switch sends a group specific query on a port when an IGMPv2 leave message is received. This value ranges between two and five seconds. Default value is 2 seconds.</p>

- Click **Apply** for the configuration to take effect. To discard the values entered, click **Reset**.

6.1.3 VlanConfiguration

The **IGMP Snooping Vlan Configuration** page allows you to configure IGMP Snooping on specific VLANs.

To configure IGS VLAN

1. Select **Multicast > IGMP Snooping > VlanConfiguration** to open the **IGMP Snooping Vlan Configuration** page.

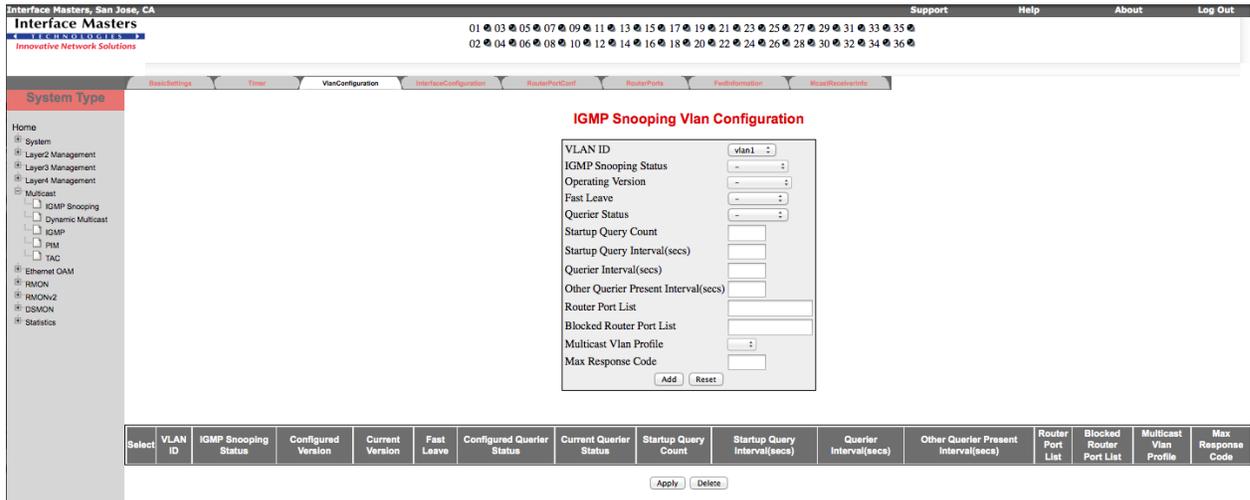


Figure 6-4: IGS Snooping Vlan Configuration - Multicast Group

2. Configure the attributes described in Table 6-4.

Table 6-4: IGMP Snooping Vlan Configuration

Field	Description
VLAN ID	Specifies the VLAN ID for which the IGMP Snooping configuration is to be performed.
IGMP Snooping Status	Specifies the Global status of IGS on the specified VLAN. Options are: <ul style="list-style-type: none"> • Enabled – IGS is enabled. A switch will watch for IGMP messages from the host connected on those interfaces and build the software. This ensures that only the ports that require a given multicast stream actually receive it. • Disabled - IGS is disabled By default, IGS is enabled on VLAN s.
Operating Version	Specifies the Operating Version of IGS for the specified VLAN. Options are: <ul style="list-style-type: none"> • Version 1 • Version 2 • Version 3 Default operating mode on a VLAN is IGMP Version 3.
Fast Leave	Specifies the Fast Leave status of IGS. Options are: <ul style="list-style-type: none"> • Enabled - The switch does not send a group specific query and immediately removes the port from the forwarding table. • Disabled - The switch checks if there are any interested receivers for the group

Field	Description
	by sending a group specific query before removing the port from the forwarding table. By default, Fast Leave status is disabled.
Querier Status	Indicates whether the switch is configured as a querier in a VLAN. Options are: <ul style="list-style-type: none"> • Enabled • Disabled By default, VLAN querier is disabled.
Querier Interval (secs)	Specifies the time period during which the general queries are sent by IGMP snooping, when the switch is configured as querier on a VLAN. This value range between 6 and 600 seconds. Default value is 125 seconds. <input type="checkbox"/> A router must be configured as a querier for a VLAN only when there are no queriers or routers in the network.
Router Port List	Specifies the Router port list for VLAN. By default, Router Port list is set to None.
Blocked Router Port List	Specifies the list of ports which are configured statically as blocked router ports. By default, Blocked Router Port list is set to None.
Multicast Vlan Profile	Specifies the multicast profile identification configured for a particular VLAN and can be used for multicast VLAN classification.
Max Response Code	Specifies the maximum response code advertised in queries which are sent over this vlan. This value ranges between 0 and 255 tenths of a second. Default value is 0.
Configured Version	Displays the configured IGMP version on the given VLAN.
Current Version	Displays the working IGMP Version on the given VLAN.
Configured Querier Status	Displays the configured querier status in the VLAN.
Current Querier Status	Displays the current querier status in the VLAN.

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

6.1.4 Interface Configuration

The **IGMP Snooping Interface Configuration** page allows you to configure IGMP Snooping on specific interface.

To configure IGS Interface

1. Select **Multicast > IGMP Snooping > InterfaceConfiguration** to open the **IGMP Snooping Interface Configuration** page.

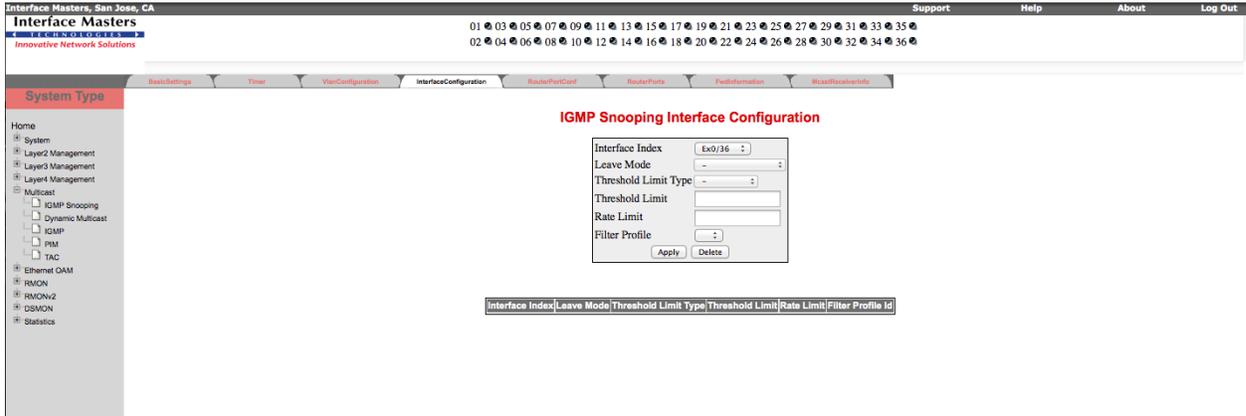


Figure 6-5: IGS Snooping Interface Configuration - Multicast Group

2. Configure the attributes described in Table 6-5.

Table 6-5: IGMP Snooping Interface Configuration

Field	Description
Interface Index	Specifies the interface index of the port.
Leave Mode	<p>Specifies the mechanism to be used for processing leave messages in the down stream interface. Options are:</p> <ul style="list-style-type: none"> • Explicit Tracking – Leave messages are processed using the explicit tracking mechanism. • Fast Leave – Leave messages are processed using the fast leave mechanism. • Normal Leave – A group or group specific query is sent on the interface when a leave message is received. <p>By default, Leave Mode is Normal Leave</p> <p><input type="checkbox"/> This field can be configured only when the Snoop Leave Level is set to Port Based.</p>
Threshold Limit Type	<p>Indicates the type of limit to be applied on the interface. Options are:</p> <ul style="list-style-type: none"> • None – No limiting is done. • Groups – Limit is set for groups • Channels – Limit is set for channel (group, source) registrations <p>By default, Threshold limit type is set to none.</p> <p><input type="checkbox"/> The channel limit is applied only for IGMPv3 include and allow reports whereas the group limit is applied for all IGMP reports.</p>
Threshold Limit	<p>Configures the maximum number of unique entries (channel or group) which can be learned simultaneously on the interface.</p> <p><input type="checkbox"/> This field can be configured only when the Threshold Limit Type is set.</p> <p>By default the threshold limit is zero.</p>
Rate Limit	Configures the rate limit for a down stream interface in the units of the number of IGMP packets per second.

Field	Description
	By default the rate limit is set to 4294967295
Filter Profile Id	Specifies the multicast profile index configured for the downstream interface. By default, Filter Profile Id is set to zero.

3. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
4. Select the required entry and click **Delete** for the entry to be deleted.

6.1.5 RouterPortConf

The **IGMP Snooping Vlan Router Port Configuration** page allows you to configure the details of the router port.

To configure VLAN Router Port

1. Select **Multicast > IGMP Snooping > RouterPortConf** to open the **IGMP Snooping VLAN Router Port Configuration** page.

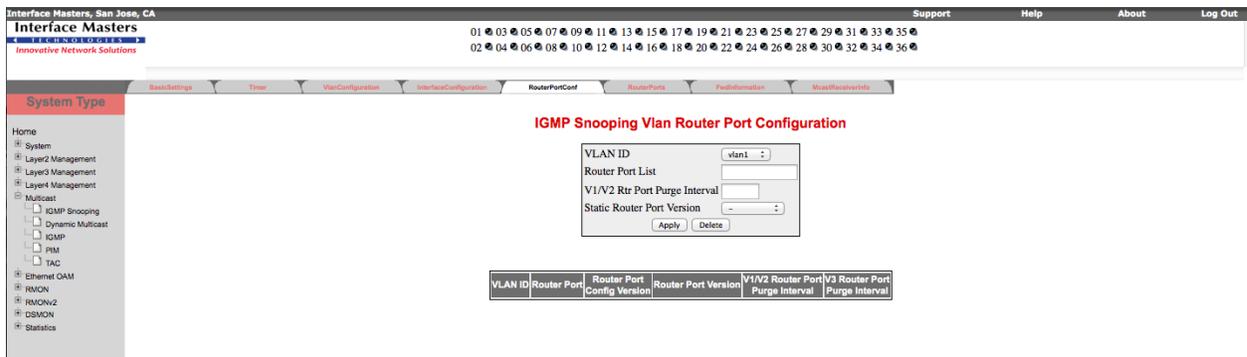


Figure 6-6: IGS Vlan Router Port Configuration - Multicast Group

2. Configure the attributes described in Table 6-6.

Table 6-6: IGMP Snooping Vlan Router Port Configuration

Field	Description
VLAN ID	Specifies the VLAN ID.
Router Port List	Specifies the list of ports which are configured statically as router ports.
V1/V2 Rtr Port Purge Interval	Specifies the time interval after which proxy assumes that there are no v1/v2 routers present on the upstream port. By default, V1/V2 Rtr Port Purge Interval is set to 125
Static Router Port Version	Specifies the operating version of the IGMP proxy on the upstream router port. Options are : <ul style="list-style-type: none"> • Version1 – Indicates that the operating version of IGMP proxy is version 1 • Version2 - Indicates that the operating version of IGMP proxy is version 2 • Version3 - Indicates that the operating version of IGMP proxy is version 3

Field	Description
	By default, Static Router Port Version is Version 3
Router Port	Displays the interface index of the port which is defined as an upstream router port.
Router Port Config Version	Displays the configured version of the IGMP Proxy on the upstream router port. By default, Router Port Config Version is set to Version 3
Router Port Version	Displays the operating version of the IGMP proxy on the upstream router port. By default, Router Port Version is set to Version 3
V3 Router Port Purge Interval	Displays the time interval after which proxy assumes that there are no IGMP v3 routers present on the upstream port. By default, V3 Router Port Purge Interval is set to 125.

3. Select the required entry. Modify the parameters and click Apply for the configuration to take effect.
4. Select the required entry and click Delete for the entry to be deleted.

6.1.6 RouterPorts

The **IGMP Snooping VLAN Router Ports** page displays the configured IGS VLAN Router Port mapping.

To display router ports

1. Select **Multicast > IGMP Snooping > RouterPorts** to open the **IGMP Snooping VLAN Router Ports** page.

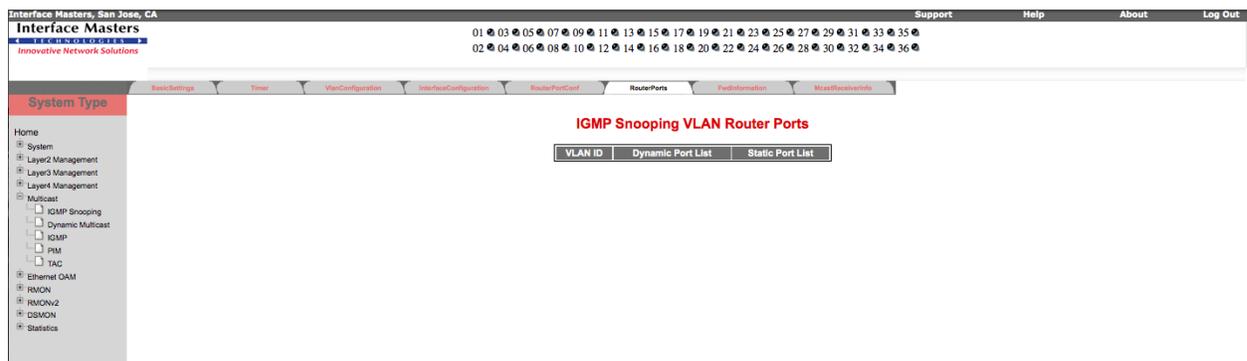


Figure 6-7: IGMP Snooping VLAN Router Ports - Multicast Group

2. The **VLAN Router Ports** attributes are described in Table 6-7.

Table 6-7: IGMP Snooping Router Ports

Field	Description
VLAN ID	Specifies the VLAN ID.
Dynamic Port List	Specifies the list of ports on which routers are present. <input type="checkbox"/> These router ports are learnt through control messages received from routers and can also be configured statically.

Static Port List	Specifies the list of ports which are configured statically as router ports.
------------------	--

6.1.7 FwdInformation

The **IP Based** or the **MAC Based Multicast Forwarding Table** page displays the IGS group information.

To display Group Information

1. Select **Multicast > IGMP Snooping > FwdInformation** to open the **MAC Based Multicast Forwarding table** page (Figure 6-8) or the **IP Based Multicast Forwarding table (Error! Reference source not found.)** page.

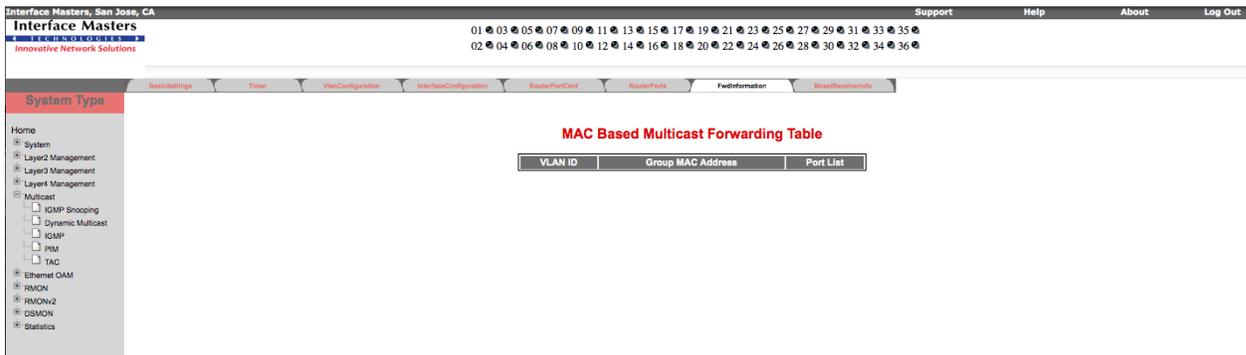


Figure 6-8: MAC Based Multicast Forwarding Table - Multicast Group

Table 6-8: Displaying Group Information – MAC Based Multicast Forwarding Table

Field	Description
VLAN ID	Specifies the VLAN ID pertaining to the MAC based multicast forwarding entry.
Group MAC Address	Specifies the Group MAC Multicast address that is learnt.
Port List	Specifies the learnt ports list onto which the multicast data packets for the group will be forwarded.

6.1.8 McastReceiverInfo

The **IGMP Snooping Multicast Receiver Table** page displays an entry for each multicast report sent by each host for a multicast group and requesting data from a specific source.

To display multicast report

1. Select **Multicast > IGMP Snooping>McastReceiverInfo** to open the **Multicast Receiver Table** page.

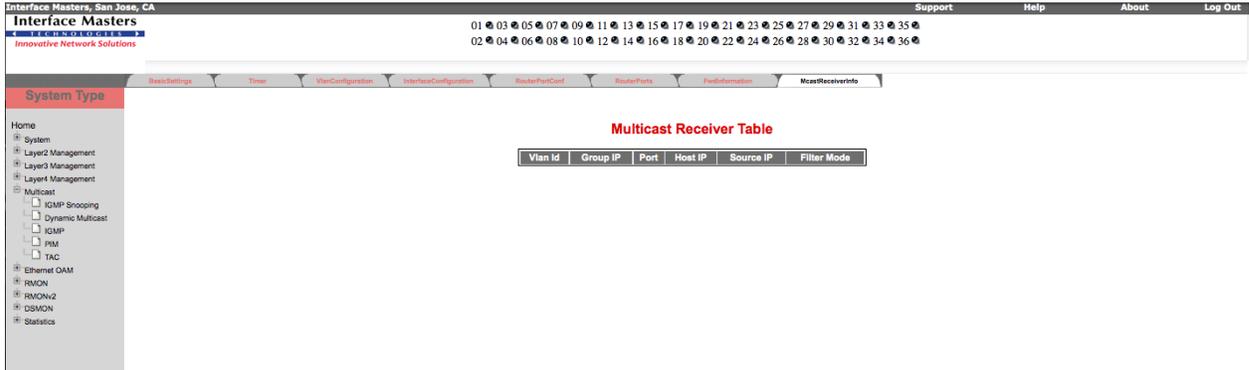


Figure 6-9: Multicast Receiver Table - Multicast Group

2. The **Multicast Receiver Table** attributes are described in Table 6-9.

Table 6-9: IGMP Snooping Multicast Receiver Table

Field	Description
Vlan ID	Displays the VLAN ID pertaining to the multicast receiver table.
Group IP	Displays the multicast group address for which the receiver has sent a request to join the group.
Port	Displays the interface on which the multicast group address is learnt.
Host IP	Displays the IP address of the multicast receiver that has been sent to the multicast group to join the group
Source IP	Displays the unicast source address of the data source that sends multicast data to the group.
Filter Mode	Displays the mode that has been registered by the multicast receiver for the unicast source address specified. Options are <ul style="list-style-type: none"> • Include • Exclude

6.2 Dynamic Multicast

The **Dynamic Multicast** link permits to enable/disable Dynamic Multicast at the switch level and also at the per-port level. This essentially gives more control over the switch to the users. Once you choose to enable the protocol on the switch, you can decide on the ports on which the protocol needs to run.

It is also possible to enable/disable Restricted Group Registration on a per-port level. This will enable you to restrict the multicast groups learnt through GMRP learning.

The **Dynamic Multicast** link on the left pane allows you to configure the Dynamic Multicast information through the following links:

- DynamicMulticast
- Port Settings

By default, the **Dynamic Multicast Global Configuration** page is loaded.

6.2.1 DynamicMulticast

The **Dynamic Multicast Global Configuration** page allows you to configure the Dynamic Multicast status.

To configure Dynamic Multicast Global Settings

1. Select **Multicast > Dynamic Multicast** to open the **Dynamic Multicast Global Configuration** page.

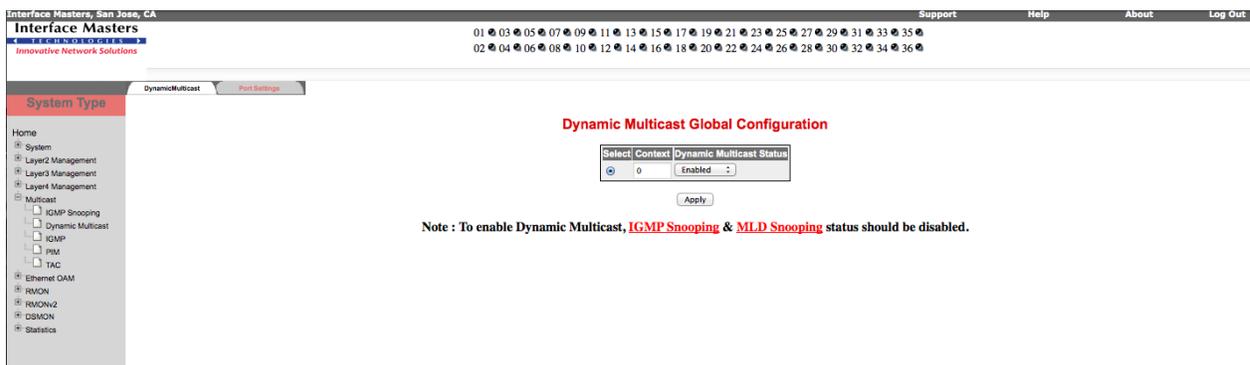


Figure 6-10: Dynamic Multicast Global Configuration

2. Configure the attributes described in Table 6-10.

Table 6-10: Configuring Dynamic Multicast Global

Field	Description
Context	Specifies the Context ID for which the Dynamic Multicast Status is to be enabled/disabled.
Dynamic Multicast Status	Indicates the status of Dynamic Multicast (GMRP) protocol in the system. Options are: <ul style="list-style-type: none"> • Enabled - Allows data transmission to multiple recipients using the same stream. • Disabled - Does not allow multicast routing. <input type="checkbox"/> At the system level, dynamic multicast and IGMP snooping are mutually exclusive. It means that at a point of time either Dynamic Multicast or IGMP Snooping can only be enabled.

3. Click **Apply** for the configuration to take effect.

6.2.2 Port Settings

The **Dynamic Multicast Port Configuration** page allows you to configure the Dynamic Multicast port settings.

To configure Dynamic Multicast Port Settings

1. Select **Multicast > Dynamic Multicast > Port Settings** to open the **Dynamic Multicast Port Configuration** page.

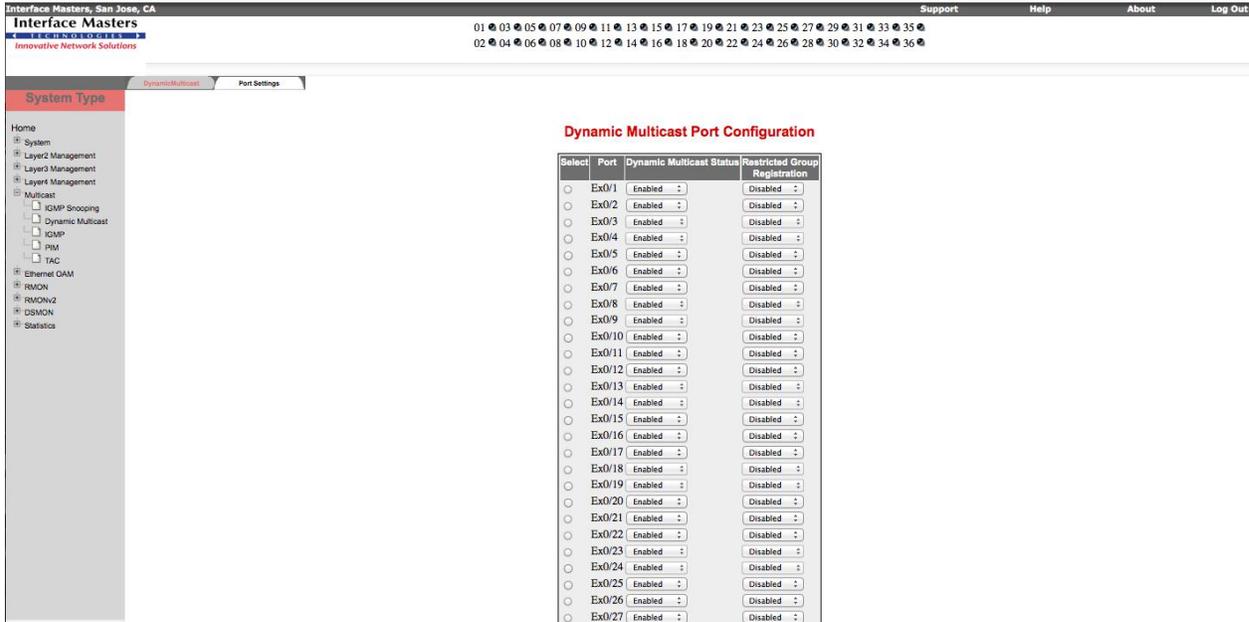


Figure 6-11: Dynamic Multicast Port Configuration

2. Configure the attributes described in Table 6-11.

To configure Dynamic Multicast Port Configuration, IGS must be disabled.

Table 6-11: Configuring Dynamic Multicast Port

Field	Description
Port	Specifies the Port for which the GMRP and the Restricted Group Registration is to be configured.
Dynamic Multicast Status	<p>Indicates the status of Dynamic Multicast (GMRP) protocol in the system. Options are:</p> <ul style="list-style-type: none"> • Enabled - Allows data transmission to multiple recipients using the same stream. • Disabled - Does not allow multicast routing. <p><input type="checkbox"/> At the system level, dynamic multicast and IGMP snooping are mutually exclusive. It means that at a point of time either Dynamic Multicast or IGMP Snooping can only be enabled.</p>
Restricted Group Registration	<p>Specifies the Restricted Group Registration status. Options are:</p> <ul style="list-style-type: none"> Enabled - Enables Restricted Group Registration. Disabled - Disables Restricted Group Registration. <p><input type="checkbox"/> Restricted Group Registration enables you to restrict the multicast groups learnt through GMRP learning.</p>

3. Click **Apply** for the configuration to take effect.

6.3 TAC

TAC (Transmission and Admission Control) is a utility module that can be used by multicast protocols for filtering multicast packets and multicast VLAN classification.

The **TAC** link on the left pane allows you to configure the **TAC** information through the following links:

- Profile
- Profile filters

By default, the **TAC Profile Configuration** page is loaded.

6.3.1 Profile

The **TAC Profile Configuration** page allows you to configure the multicast profile which is used to filter incoming IGMP/MLD reports from customers.

To configure TAC Profile

1. Select **Multicast > TAC** to open the **TAC Profile Configuration** page.

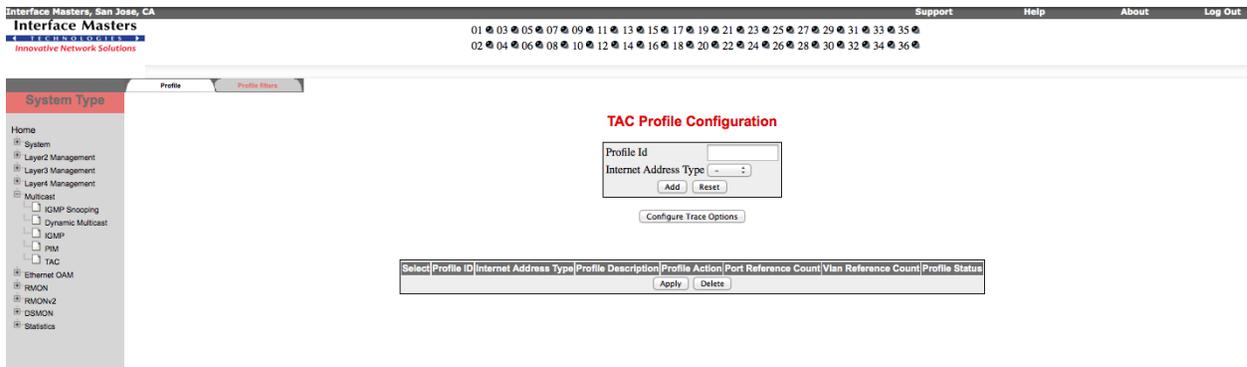


Figure 6-12: TAC Profile Configuration – Multicast Group

2. Configure the attributes described in Table 6-12.

Table 6-12: Configuring TAC Profile

Field	Description
Profile Id	Specifies the identifier for multicast profile entry.
Internet Address Type	Specifies whether the configured rule is for IPv4 or IPv6 address.
Profile Description	Specifies the description for the profile entry.
Profile Action	Specifies whether to allow or deny the channels associated with this profile. Options are: <ul style="list-style-type: none"> • Permit – Allows the channels associated with this profile. • Deny – Denies the channels associated with this profile. By default, Profile Action is set to Deny

Field	Description
Port Reference Count	Displays the number of configured profile to port mappings.
Vlan Reference Count	Displays the number of configured profile to Vlan mappings.
Profile Status	Specifies the status of a row in the multicast profile table. Options are <ul style="list-style-type: none"> Active – Indicates that the status of the specific row is active in the multicast profile table. InActive – Indicates that the status of the specific row is inactive in the multicast profile table.

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

6.3.2 Profile filters

The **TAC Profile Filter Configuration** page specifies the packets for which the configuration needs to be enforced.

To specify packets

1. Select **Multicast > TAC > Profile filters** to open the **TAC Profile Filter Configuration** page.

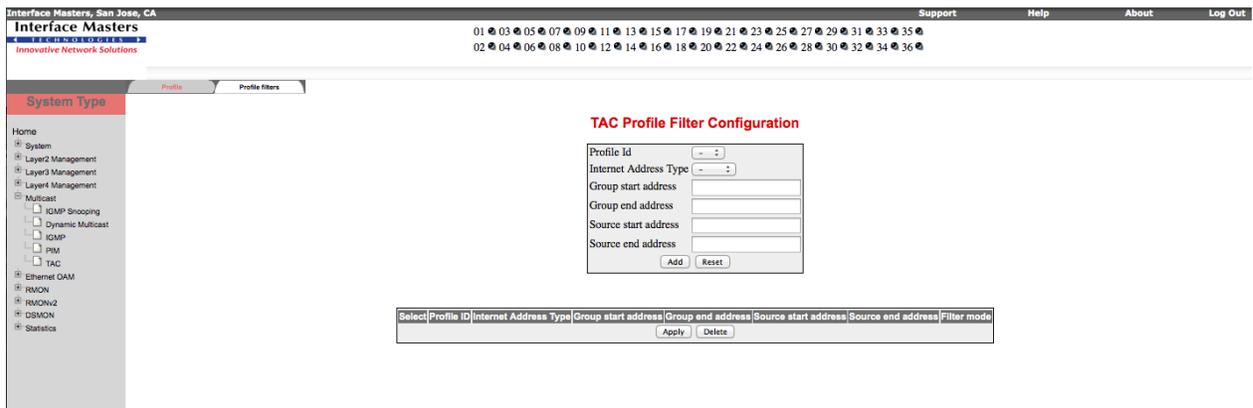


Figure 6-13: TAC Profile Filter Configuration – Multicast Group

2. Configure the attributes described in Table 6-13.

Table 6-13: TAC Profile Filters

Field	Description
Profile Id	Specifies the identifier for multicast profile entry.
Internet Address Type	Specifies whether the configured rule is for IPv4 or IPv6 address.

Field	Description
Group start address	<p>Specifies the starting address of the multicast group address range.</p> <p><input type="checkbox"/> To configure a specific address, both the start and end group address must be the same.</p>
Group end address	<p>Specifies the ending address of the multicast group address range.</p> <p><input type="checkbox"/> To configure a specific address, both the start and end group address must be the same.</p>
Source start address	<p>Specifies the starting address of the multicast source address range</p> <p><input type="checkbox"/> To configure a specific address, both the start and end source address must be the same.</p>
Source end address	<p>Specifies the ending address of the multicast source address range.</p> <p><input type="checkbox"/> To configure a specific address, both the start and end source address must be the same.</p>
Filter mode	<p>Specifies the type of packets to be filtered. Options are:</p> <ul style="list-style-type: none"> • Include – Applies the filter for include IGMP/ MLD reports • Exclude – Applies the filter for exclude IGMP / MLD reports. • Any – Applies the filter for all the packets <p>By default, Filter mode is set to Any</p>

3. Click **Add** to save the entry in the configuration table. Click **Reset** to clear the configured values.
4. Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.
5. Select the required entry and click **Delete** for the entry to be deleted.

Chapter

7

Ethernet OAM

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).

The **Ethernet OAM** link on the left pane allows you to configure the **EOAM** parameters through the following links:

- Basic Settings
- Port Settings
- LinkEvent Settings
- Loopback Settings

By default, the **Ethernet OAM Basic Settings** page is loaded.

7.1 Basic Settings

The **Ethernet OAM Basic Settings** page allows you to configure basic settings of the EOAM.

To configure EOAM basic settings

1. Select **Ethernet OAM** to open **Ethernet OAM Basic Settings** page.

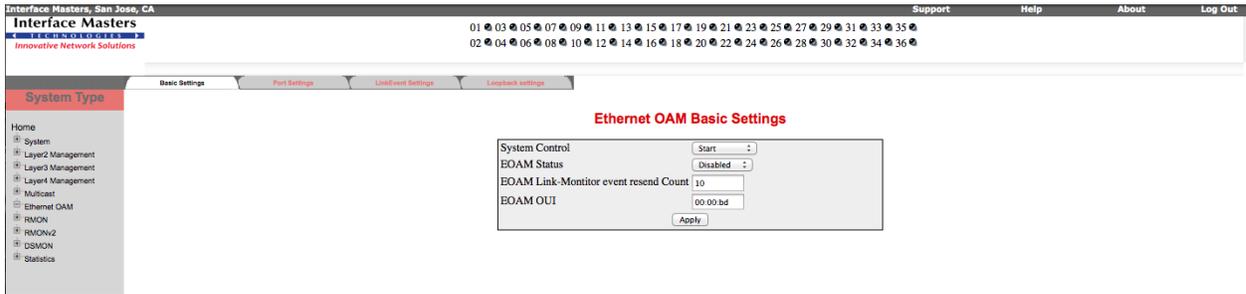


Figure 7-1: Ethernet OAM Basic Settings – EOAM Group

2. Configure the parameters described in Table 7-1.

Table 7-1: Ethernet OAM Basic Settings

Field Name	Description
System Control	Specifies the administrative system control status of EOAM module. Options are: <ul style="list-style-type: none"> • Start – Allocates resources required by EOAM module and starts EOAM on all ports. • Shutdown – Releases allocated resources and shutdowns the EOAM on all ports. By default, this is Start .
EOAM Status	Specifies the administrative module status of EOAM module. Options are: <ul style="list-style-type: none"> • Enabled – Enables the EOAM in the device. • Disabled – Disables the EOAM in the device. By default, this is Disabled .
EOAM Link-Monitor event resend Count	Specifies the number of times an error event OAMPDU will be sent repeatedly. This value ranges between 1 and 10. Default value is 10.
EOAM OUI	Specifies the Organizational Unique Identifier of the local EOAM client. Default value is the first three bytes of the system MAC address.

3. Click **Apply** for the configuration to take effect.

7.2 Port Settings

The **Ethernet OAM Port Settings** page allows you to configure the port related parameters.

To configure port related parameters

1. Select **Ethernet OAM > Port Settings** to open **Ethernet OAM Port Settings** page.

Select	Port	Status	Mode	LB Permit/Deny	Operational Status	Remote LB	Link Event	Uni Directional	Variable Retrieval
<input type="radio"/>	Ex0/1	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/2	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/3	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/4	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/5	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/6	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/7	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/8	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/9	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/10	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/11	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/12	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/13	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/14	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/15	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/16	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/17	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/18	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/19	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/20	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/21	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/22	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable
<input type="radio"/>	Ex0/23	Disabled	Active	Deny	Disabled	Enable	Enable	Disable	Enable

Figure 7-2: Ethernet OAM Port Settings – EOAM Group

2. Configure the parameters described in Table 7-2.

Table 7-2: Ethernet OAM Port Settings

Field Name	Description
Port	Specifies the interface index.
Status	Specifies the default administrative OAM mode for the interface. Options are: <ul style="list-style-type: none"> Enabled – Enables the operation of EOAM over the interface. Disabled – Disables the operation of EOAM over the interface. By default, this is Disabled .
Mode	Specifies the EOAM mode for the interface. Options are: <ul style="list-style-type: none"> Active – Sets the remote OAM entity in a loopback state. Passive – Does not set the OAM entity in the loopback state. By default, this is Active .
LB Permit/Deny	Specifies whether received OAM loopback commands are processed or ignored. Options are: <ul style="list-style-type: none"> Permit – Processes the OAM loopback commands. Deny – Ignores the received loopback commands. By default, this is Deny .

Field Name	Description
Operational Status	<p>Indicates the operational status of EOAM. Options are:</p> <ul style="list-style-type: none"> • Disabled – OAM is disabled on the interface. • LinkFault – Link is transmitting OAMPDUs with a link fault indication. • PassiveWait – Reflects the state in which the OAM entity is waiting to see if the peer device is OA capable. • ActiveSendLocal – Reflects the OAM entity actively trying to discover whether the peer has OAM capability, but has not yet made that determination. • SendLocalAndRemote – Reflects that the local OA entity has discovered the peer, but has not yet accepted or rejected the configuration of the peer. • SendLocalAndRemoteOk – Local device allows the OAM peering. • OamPeeringLocallyRejected – Local OAM entity rejects the peer OAM entity. • OamPeeringRemotelyRejected – Remote OAM entity rejects the peering. • Operational – Local OAM entity learns that both it and the remote OAM entity have accepted the peering. • InitiatingLoopBack – Local OAM entity is in loopback process with its peer • R-LoopBack – Remote OAM entity is in loopback mode • TerminatingLoopBack – Local OAM entity is in process of terminating the loopback state • L-LoopBack – Local OAM entity is in loopback mode • Unknown – Parser and multiplexer of OAM entity is in unexpected state • HalfDuplex – EOAM is enabled but the interface is in half-duplex operation.
Remote LB	<p>Indicates whether the EOAM Remote Loopback functionality is enabled / disabled. Options are:</p> <ul style="list-style-type: none"> • Enable – EOAM Remote Loopback functionality is enabled • Disable - EOAM Remote Loopback functionality is disabled
Link Event	<p>Indicates whether the EOAM link event(s) monitoring functionality is enabled / disabled. Options are:</p> <ul style="list-style-type: none"> • Enable – EOAM link event(s) monitoring functionality is enabled • Disable – EOAM link event(s) monitoring functionality is disabled
Uni Directional	<p>Indicates whether the Uni-Directional support is enabled / disabled on that interface. Options are:</p> <ul style="list-style-type: none"> • Enable – Uni-Directional support is enabled • Disable – Uni-Directional support is disabled
Variable Retrieval	<p>Indicates whether the EOAM Variable Retrieval support is enabled / disabled. Options are:</p> <ul style="list-style-type: none"> • Enable – EOAM Variable Retrieval support is enabled • Disable – EOAM Variable Retrieval support is disabled

3. Click **Apply** for the configuration to take effect.

Field Name		Description
	Threshold	Specifies the number of symbol errors that must occur within a given window for generating an Event notification OAMPDU with an Errored Symbol Period Event TLV. This value ranges between 1 and 18446744073708999999. Default value is 1 symbol error.
Frame	Enabled/Disabled	Specifies whether the OAM entity should send an Event Notification OAMPDU when an Errored Frame Event occurs. Options are: <ul style="list-style-type: none"> • Enabled – Sends an Event Notification OAMPDU. • Disabled – Does not send an Event Notification OAMPDU. By default, this is Enabled .
	Window (100 msec)	Specifies the amount of time (in 100ms increments) over which the threshold is defined. This value ranges between 10 and 600. Default value is 10 (1 Second).
	Threshold	Specifies the number of frame errors that must occur for generating an Event notification OAMPDU with an Errored Frame Event TLV. This value ranges between 1 and 4294967295. Default value is 1 frame error.
Frame-Period	Enabled/Disabled	Specifies whether the OAM entity should send an Event Notification OAMPDU when an Errored Frame Period Event occurs. Options are: <ul style="list-style-type: none"> • Enabled – Sends an Event Notification OAMPDU. • Disabled – Does not send an Event Notification OAMPDU. By default, this is Enabled .
	Window	Specifies the number of frames over which the threshold is defined. This value ranges between 1 and 4294967295. Default value is the number of minimum size Ethernet frames that can be received over the physical layer in one second. <input type="checkbox"/> Frame period window size should be greater than the threshold value.
	Threshold	Specifies the number of frame errors that must occur for generating an Event notification OAMPDU with an Errored Frame Period Event TLV. This value ranges between 0 and 4294967294. Default value is 1 frame error.
Frame-Seconds	Enabled/Disabled	Specifies whether the OAM entity should send an Event Notification OAMPDU when an Errored Frame Seconds Event occurs. Options are: <ul style="list-style-type: none"> • Enabled – Sends an Event Notification OAMPDU. • Disabled – Does not send an Event Notification OAMPDU. By default, this is Enabled .
	Window (100 msec)	Specifies the amount of time (in 100ms increments) over which the threshold is defined. This value ranges between 100 and 9000. Default value is 100 (10 Second). <input type="checkbox"/> Frame second window size should be greater than the threshold value.

Field Name	Description
Threshold	Specifies the number of errored frame seconds that must occur for generating an Event notification OAMPDU with an Errored Frame Seconds Summary Event TLV. This value ranges between 1 and 900. Default value is 1 errored frame second.
Critical Event	<p>Specifies whether the local OAM entity must attempt to indicate a critical event through the OAMPDU flags to its peer OAM entity when a critical event occurs. Options are:</p> <ul style="list-style-type: none"> • Enabled – Indicates the critical event to the peer OAM entity. • Disabled – Does not indicate the critical event. <p>By default, this is Enabled.</p> <p><input type="checkbox"/> This field does not have any effect on the system that does not support critical event capability.</p>
Dying Gasp	<p>Specifies whether the local OAM entity must attempt to indicate a dying gasp through the OAMPDU flags field to its peer OAM entity when a dying gasp event occurs. Options are:</p> <ul style="list-style-type: none"> • Enabled – Indicates the dying gasp. • Disabled – Does not indicate the dying gasp. <p>By default, this is Enabled.</p> <p><input type="checkbox"/> This field does not have any effect on the system that does not support dying gasp capability.</p>

3. Click **Apply** for the configuration to take effect.

7.4 Loopback Settings

The **Ethernet OAM Loopback Settings** page allows you to configure the loopback state of the local link and view the status of the loopback function.

To configure loopback state and view loopback status

1. Select **Ethernet OAM > Loopback Settings** to open **Ethernet OAM Loopback Settings** page.

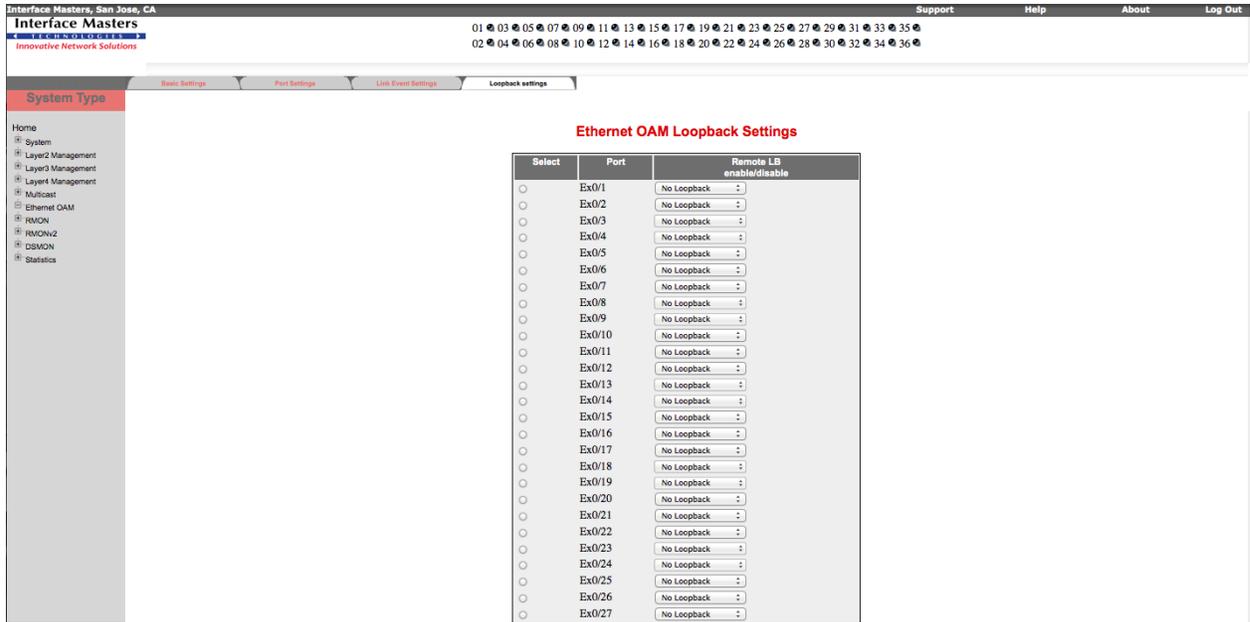


Figure 7-4: Ethernet OAM Loopback Settings – EOAM Group

2. Configure the parameters described in Table 7-4.

Table 7-4: Ethernet OAM Loopback Settings

Field Name	Description
Port	Specifies the interface index.
Remote LB enable/disable	<p>Specifies the loopback status of the OAM entity. Options are:</p> <ul style="list-style-type: none"> • No Loopback – Local OAM client operates in normal mode with no loopback in progress. • Initiating – OAM client is waiting for a response for the loopback OAMPDU sent after initiating a loopback. • Remote - LB – Local OAM client knows that the remote OAM entity is in loopback mode. • Terminating - LB – Local OAM client is in the process of terminating the remote loopback. • Local - LB – Remote OAM client has put the local OAM entity in loopback mode. • Unknown – The OAM loopback is in a transition state. <p><input type="checkbox"/> The user can select only the options Initiating and Terminating - LB, while other options denotes the loopback status.</p> <p><input type="checkbox"/> The option Initiating can be selected, only if the loopback status is in No Loopback.</p> <p><input type="checkbox"/> The option Terminating - LB can be selected, only if the loopback status is in Remote - LB.</p>

3. Click **Apply** for the configuration to take effect.

Chapter

8

RMON

RMON 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. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

The **RMON** link on the left pane allows you to configure **RMON** parameters through the following links:

- Basic Settings
- Alarms
- Ethernet Statistics
- Events
- History

By default, the **RMON Basic Settings** page is loaded.

8.1 Basic Settings

The **RMON Basic Settings** page allows you to configure the RMON status.



It is possible to configure other RMON settings only when RMON is enabled in the device.

To configure the Basic Setting for the device

1. Click **RMON** to open the **RMON Basic Settings** page.

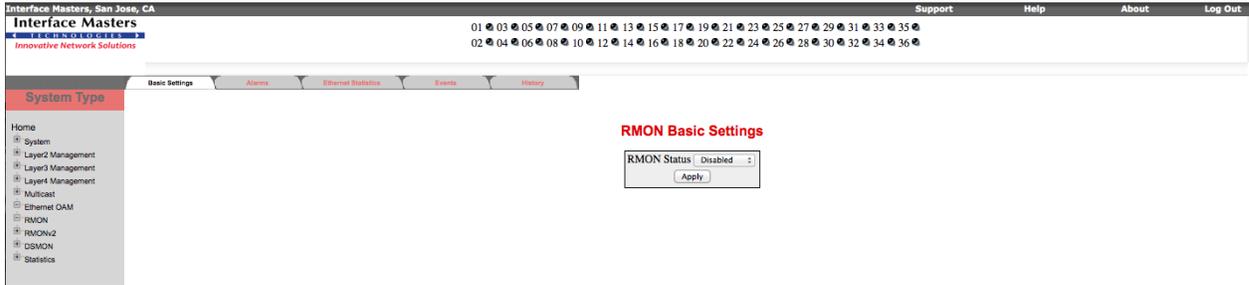


Figure 8-1: RMON Basic Settings - RMON Group

2. Configure the attributes described in Table 8-1.

Table 8-1: RMON Basic Settings

Field Name	Description
RMON Status	Specifies the status of RMON on the switch. Options are: <ul style="list-style-type: none"> • Enabled - Enables RMON in the switch. • Disabled - Disables RMON in the switch.

3. Click **Apply** for the configuration to take effect.

8.2 Alarms

The **RMON Alarm Configuration** page allows you to configure RMON alarm settings.



RMON status must be enabled for RMON Alarm configuration.

To configure Alarms for the device

1. Click **RMON > Alarms** to open the **RMON Alarm Configuration** page.

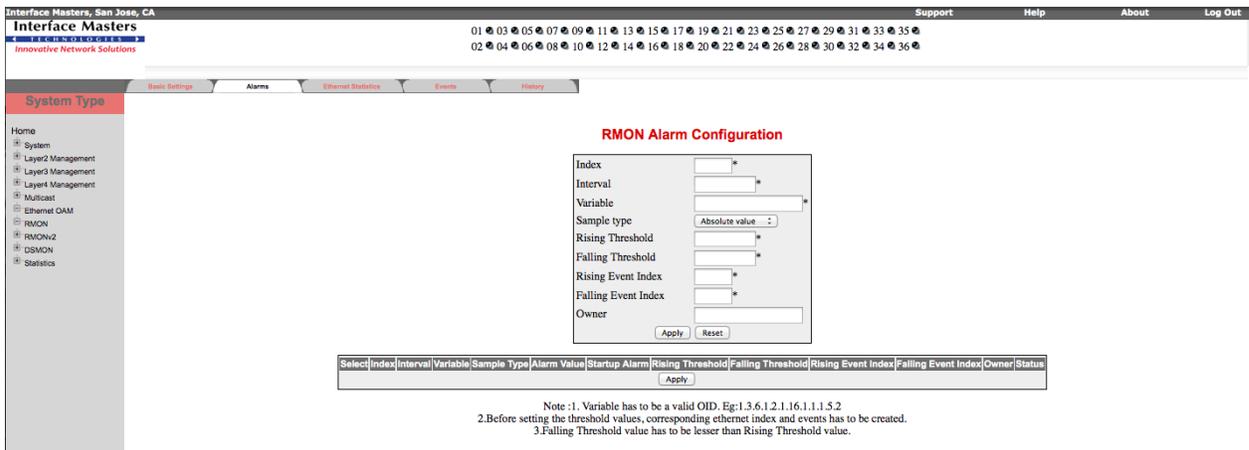


Figure 8-2: RMON Alarm Configuration - RMON Group

2. Configure the attributes described in Table 8-2.

Table 8-2: RMON Alarm Configuration

Field Name	Description
Index	<p>Specifies the RMON alarm table index.</p> <p>The index value uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for an object in the device.</p> <p>This value ranges between 1 and 65535.</p>
Interval	<p>Specifies the time interval in seconds for which the alarm monitors the variable. It is during this interval the data is sampled and compared with the rising and falling thresholds.</p> <p>This value ranges between 1 and 65535.</p>
Variable	Specifies the MIB object variable on which the alarm is set.
Sample Type	<p>Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. Options are:</p> <ul style="list-style-type: none"> • Absolute value - The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. • Delta value - The value of the selected variable at the last sample will be subtracted from the current value, and the difference is compared with the thresholds.
Rising Threshold	<p>Specifies the Rising Threshold value.</p> <p>If the startup alarm is set as Rising alarm and if the configured threshold value is reached, then an alarm is raised.</p> <p>When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated.</p> <p>This value ranges between 0 and 2147483647.</p>
Falling Threshold	<p>Specifies the Falling Threshold value.</p> <p>If the startup alarm is set as Falling alarm and this threshold is reached, an alarm is raised.</p> <p>When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated.</p> <p>This value ranges between 0 and 2147483647.</p>
Rising Event Index	<p>Indicates the index of the event to be raised when the Rising threshold is reached.</p> <p>The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object.</p> <p>This value ranges between 1 and 65535.</p>
Falling Event Index	<p>Indicates the index of the event to be raised when the Falling threshold is reached.</p> <p>The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object.</p> <p>This value ranges between 1 and 65535.</p>

Field Name	Description
Owner	Indicates the entity that configured this entry.
Status	Displays the required status of alarm. Options are: <ul style="list-style-type: none"> Valid Under Creation Invalid

- Click **Apply** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required entry, modify the parameters and click **Apply** for the configuration to take effect.

8.3 Ethernet Statistics

The **Ethernet Statistics Configuration** page contains statistics measured by the probe for each monitored interface on the device.



RMON must be enabled for the configuration of the RMON Ethernet statistics.

To configure Statistics for the device

- Click **RMON> Ethernet Statistics** to open the **Ethernet Statistics Configuration** page.

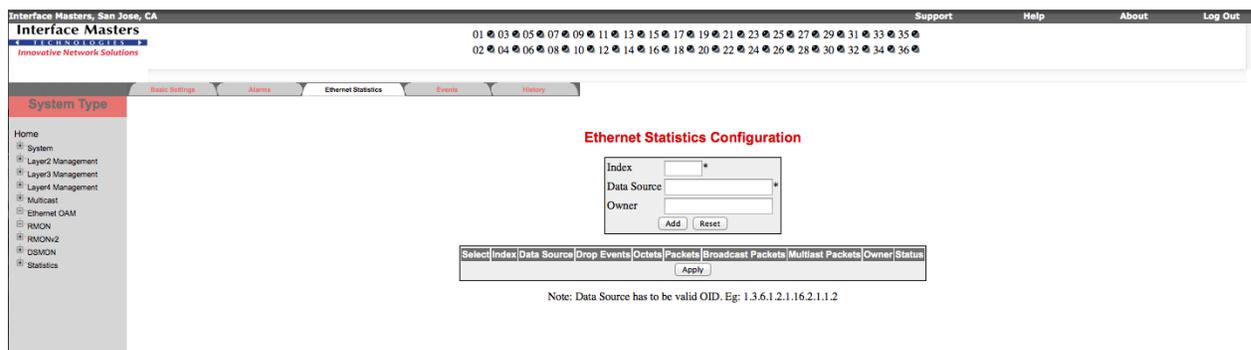


Figure 8-3: Ethernet Statistics Configuration - RMON Group

- Configure the attributes described in Table 8-3.

Table 8-3: RMON Ethernet Statistics

Field Name	Description
Index	Specifies the Ethernet Statistics index that uniquely identifies an entry in the Ethernet Statistics table.
Data Source	Specifies the SNMP object ID of the variable on which the statistics is being collected.
Owner	Indicates the entity that configured this entry.

Field Name	Description
Drop Events	Specifies the number of events in which the packets were dropped due to lack of resources. This number does not specify the number of packets dropped but the number of times the packets were dropped.
Octets	Specifies the total number of octets received from the network. This can be used as a reasonable estimate of 10-Megabit Ethernet utilization.
Packets	Specifies the total number of packets received from the network. This includes bad packets, broadcast packets and multicast packets received.
Broadcast Packets	Specifies the total number of broadcast packets received from the network.
Multicast Packets	Specifies the total number of multicast packets received from the network.
Status	Displays the required status of statistics. Options are: <ul style="list-style-type: none"> Valid – Under Creation – Invalid –

- Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
- Select the required index from the configuration table, modify the required parameters and click **Apply** to apply the configuration.

8.4 Events

The **Event Configuration** page allows you to configure RMON event settings.

To configure the Events for the device

- Click **RMON > Events** to open the **Event Configuration** page.

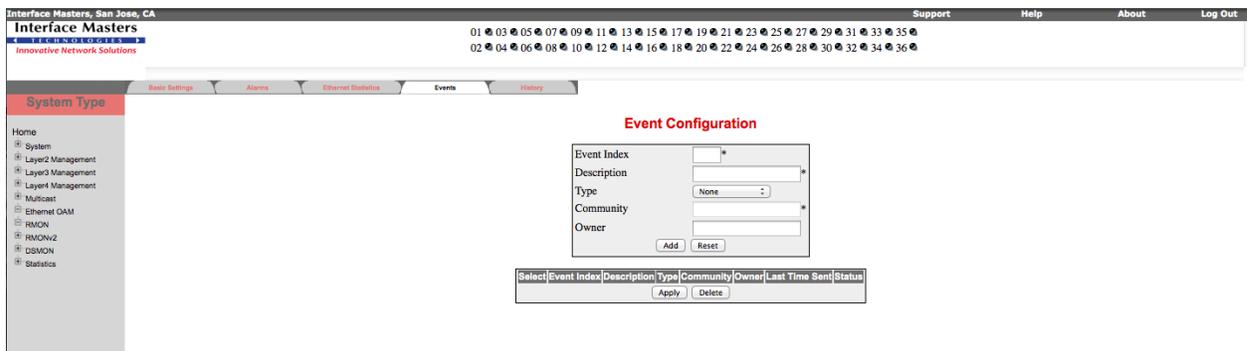


Figure 8-4: Event Configuration - RMON Group

- Configure the attributes described in Table 8-4.

Table 8-4: RMON Event Configuration

Field Name	Description
Index	Specifies 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 between 1 and 65535.
Description	Specifies a brief description of the event. The size of the display string varies between 0 and 127 characters.
Type	Specifies the type of event to be configured. Options are: <ul style="list-style-type: none"> • Log - Creates an entry in the log table for each event. • SNMP Trap - Sends an SNMP trap to one or more management stations. • Log and Trap – Creates an entry in the log table and sends an SNMP trap. • None – No type is set. <input type="checkbox"/> The Community and the Owner fields are disabled, when the event Type is None or Log.
Community	Specifies the SNMP community string used for this trap. <input type="checkbox"/> This is relevant when an SNMP trap is requested for an event.
Owner	Represents the entity that configured this entry.
Last Time Sent	Denotes the time this event entry last generated an event. If this entry has not generated any events, the value will be zero.
Status	Specifies the required status of event. Options are: <ul style="list-style-type: none"> • Valid – Retains the the event as operational. • Invalid - Deletes the event and the associated log entries. • Under Creation - Retains the event as a non-operational entity.

3. Click **Add** to save the entry. If you wish to discard the information you have entered, click **Reset**.
4. Select the required event Index from the configuration table, modify the required parameters and click **Apply** for the configuration to take effect.

8.5 History

The **History Control Configuration** page allows you to configure RMON history settings.

To configure the History for the device

1. Click **RMON > History** to open the **History Control Configuration** page.

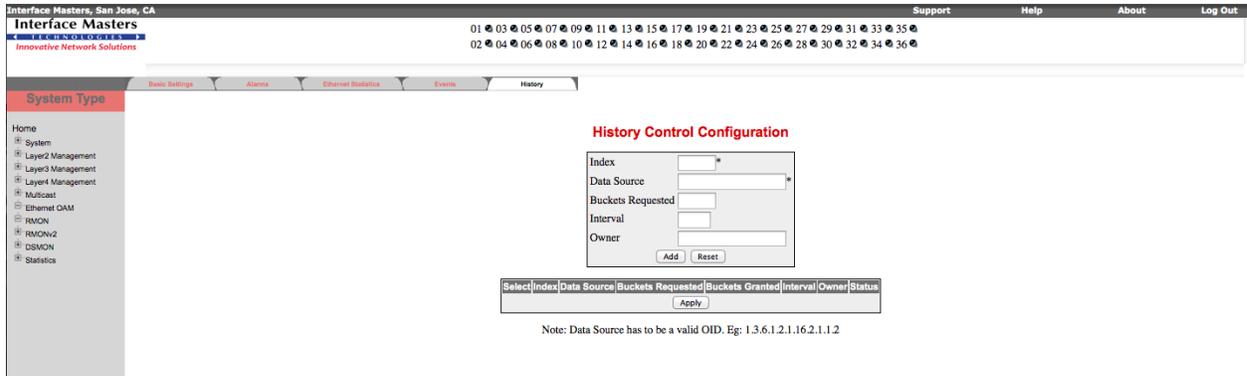


Figure 8-5: History Control Configuration - RMON Group

2. Configure the attributes described in Table 8-5.

Table 8-5: RMON History Control Configuration

Field Name	Description
Index	Uniquely identifies an entry in the History Control Table. Each such entry defines a set of samples at a particular interval for an interface on the device.
Data Source	Specifies the SNMP object id of the variable on which the history is being collected.
Buckets Requested	Indicates the number of buckets to be configured for collecting the RMON statistics, that is, the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry. This value ranges between 1 and 65535. Default value is 50.
Interval	Specifies the time interval in seconds between two successive pollings to collect the statistics. This value ranges between 1 and 3600 seconds. Default value is 1800 seconds.
Owner	Represents the entity that configured this entry.
Buckets Granted	Denotes the number of buckets granted for collecting the RMON statistics. This value ranges between 1 and 65535. This is a read-only field.
Status	Specifies the required status of event. Options are: <ul style="list-style-type: none"> Valid - Retains the event as operational. Invalid - Deletes the event and the associated log entries. Under Creation - Retains the event as a non-operational entity.

- Click **Add** to save the entry. If you wish to discard, the information you have entered, click **Reset**.
- Select the required entry. Modify the parameters and click **Apply** for the configuration to take effect.

Chapter 9

RMONv2

RMONv2 is an extension of the RMON that deals with the information at the physical and data link network levels to support monitoring and protocol analysis of LANs. RMONv2 adds support for network and application layer monitoring.

The **RMONv2 Basic Settings** page allows you to configure RMONv2 related parameters.

To configure RMONv2 related parameters

1. Select **System > RMONv2** to open **RMONv2 Basic Settings** page.

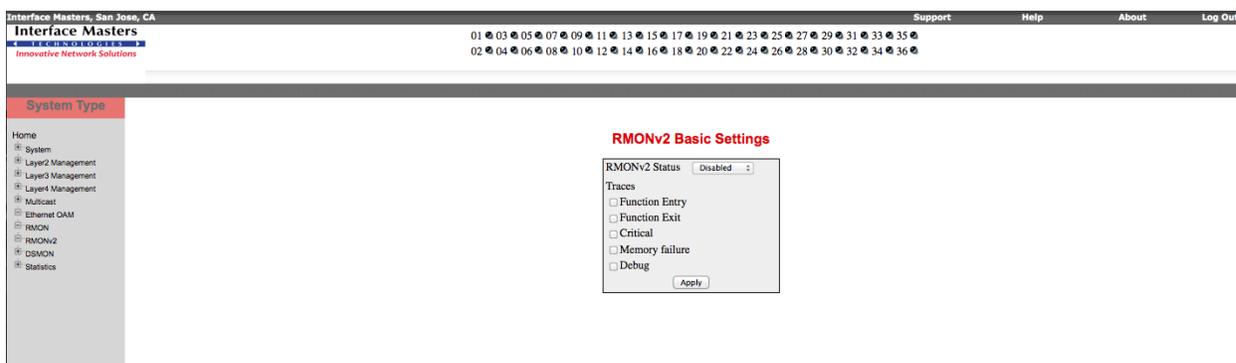


Figure 9-1: RMONv2 Basic Settings – RMONv2 Group

2. Configure the parameters described in the Table 9-1.

Table 9-1: RMONv2 Basic Settings

Field Name	Description
------------	-------------

Field Name	Description
RMONv2 Status	Specifies the admin status for RMON version 2. The options are: <ul style="list-style-type: none">• Enabled – Enables RMONv2 in the switch.• Disabled – Disables RMONv2 in the switch. By default, RMONv2 is disabled.
Traces	Specifies the traces that are defined for RMONv2. The options are: <ul style="list-style-type: none">• Function Entry - Displays all function entry trace messages.• Function Exit - Displays all function exit trace messages.• Critical - Displays all critical traces.• Memory failure - Displays all traces related to memory failure.• Debug - Displays all debug traces. <input type="checkbox"/> More than one trace can be selected.

3. Click **Apply** for the configuration to take effect.

Chapter 10

DSMON

DSMON (Differentiated Services Monitoring) is used to monitor the network traffic usage of DSCP (Differentiated Services Code Point) values. DSMON allows network management application to determine performance details such as network throughput for traffic associated with different DSCPs.

The **DSMON Basic Settings** page allows you to configure DSMON related parameters.

To configure DSMON related parameters

1. Select **System > DSMON** to open **DSMON Basic Settings** page.

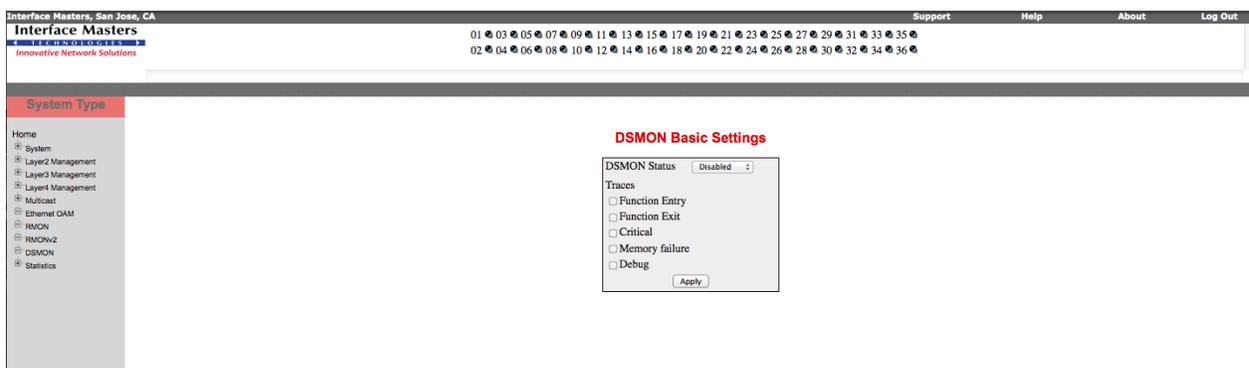


Figure 10-1: DSMON Basic Settings – DSMON Group

2. Configure the parameters described in the Table 10-1.

Table 10-1: DSMON Basic Settings

Field Name	Description
------------	-------------

Field Name	Description
DSMON Status	Specifies the admin status for DSMON. The options are: <ul style="list-style-type: none">• Enabled – Enables DSMON in the switch.• Disabled – Disables DSMON in the switch. By default, DSMON is disabled.
Traces	Specifies the traces that are defined for DSMON. The options are: <ul style="list-style-type: none">• Function Entry - Displays all function entry trace messages.• Function Exit - Displays all function exit trace messages.• Critical - Displays all critical traces.• Memory failure - Displays all traces related to memory failure.• Debug - Displays all debug traces. <input type="checkbox"/> More than one trace can be selected.

3. Click **Apply** for the configuration to take effect.

Chapter 11

Statistics

This chapter describes the statistics of the various protocols.

The **Statistics** link on the left pane opens the **Statistics** page. This page allows you to view the statistics of the various protocols of **ISS** and other information.

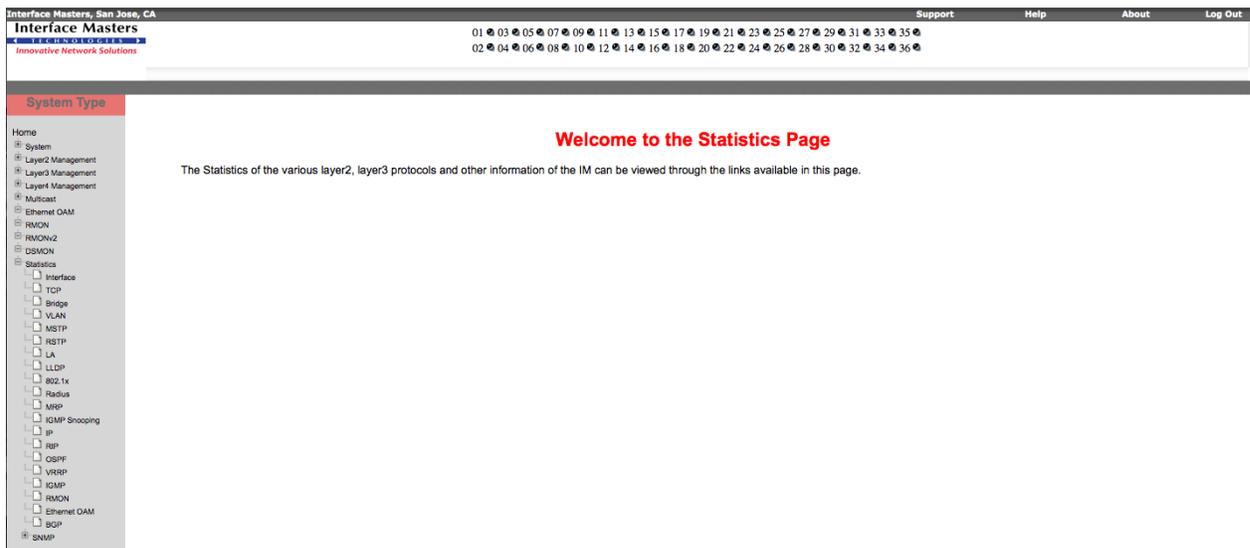


Figure 11-1: Statistics - Statistics Group

The various Statistics pages available are:

Bridge Information

This page shows the information associated with Bridge. The information includes the Spanning Tree Protocol that is supported, Priority, Topology changes, the Designated root and the various time values associated with the bridge.

Interface

The *Interface* link under Statistics in the left pane opens the following pages:

1. Interface Statistics

Displays the management information applicable to all the interfaces available in the Switch.

2. Ethernet Statistics

Displays the statistics for a collection of Ethernet-like interfaces attached to the ISS.

LA

The *LA* link under the Statistics in the left pane opens the following pages:

1. LA Port Statistics

Displays the Link Aggregation Protocol statistics for each port on the device.

2. LA Neighbor Statistics Information

Displays the Neighbor statistics for each port on the device.

MSTP

The *MSTP* link under Statistics in the left pane opens the following pages:

1. MSTP Information

Displays the information corresponding to the Multiple Spanning Tree protocol.

2. MSTP CIST Port Statistics

Displays a list of information maintained by every port for the Common Spanning Tree.

3. MSTP MSTI Port Statistics

Displays a list of information maintained by every port for each and every spanning tree instance.

802.1x

The *802.1x* link under the Statistics in the left pane opens the following pages:

1. 802.1x Session Statistics

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.

2. 802.1x Supplicant Session Statistics

Displays the Supplicant Session statistics.

3. 802.1x MAC Session Statistics

Displays the MAC Session statistics.

RMON Ethernet Statistics

This page displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.

RSTP

The *RSTP* link under Statistics in the left pane opens the following pages:

1. RSTP Information

Displays the information on the bridges that supports the Spanning Tree protocol.

2. RSTP Port Statistics

Displays the various RSTP statistics involved with each of the port available in the system like the role, state, transition state machine, various packet statistics etc.

VLAN

The *VLAN* link under Statistics in the left pane opens the following pages:

1. VLAN Current Database

Displays the information for a VLAN that is configured in the device or that is dynamically created as a result of GVRP requests received

2. VLAN Port Statistics

Displays the traffic statistics for all the available VLANs in the device.

3. VLAN Multicast Table

Displays the VLAN Dynamic group Registrations statistics.

4. VLAN Counter Statistics

Displays the VLAN Counter statistics.

5. VLAN Capabilities

Displays the VLAN capabilities.

6. VLAN FDB Entries

Displays information about a specific unicast MAC address for which the device has some forwarding and/or filtering information.

IGMP Snooping

The *IGS* link under Statistics in the left pane opens the following pages:

1. IGMP Snooping Clear Statistics

Displays the IGMP snooping clear statistics.

2. IGMP Snooping V1/V2 Statistics

Displays the IGMP snooping statistics pertaining to IGMP snooping v1 and v2.

3. IGMP Snooping V3 Statistics

Displays the IGMP snooping statistics pertaining to IGMP snooping v3.

MLD Snooping

The *MLDS* link under Statistics in the left pane opens the following pages:

1. MLDS Statistics

Displays the MLD snooping statistics pertaining to MLDv1.

2. MLDSV2 Statistics

Displays the MLD snooping statistics pertaining to MLDv2.

EOAM Interface Statistics

This page displays the EOAM Interface Statistics information.

SNMP

This page displays the SNMP statistics.

RADIUS

This page displays the RADIUS Server statistics.

The following are a few sample screen shots depicting the Statistics pages:

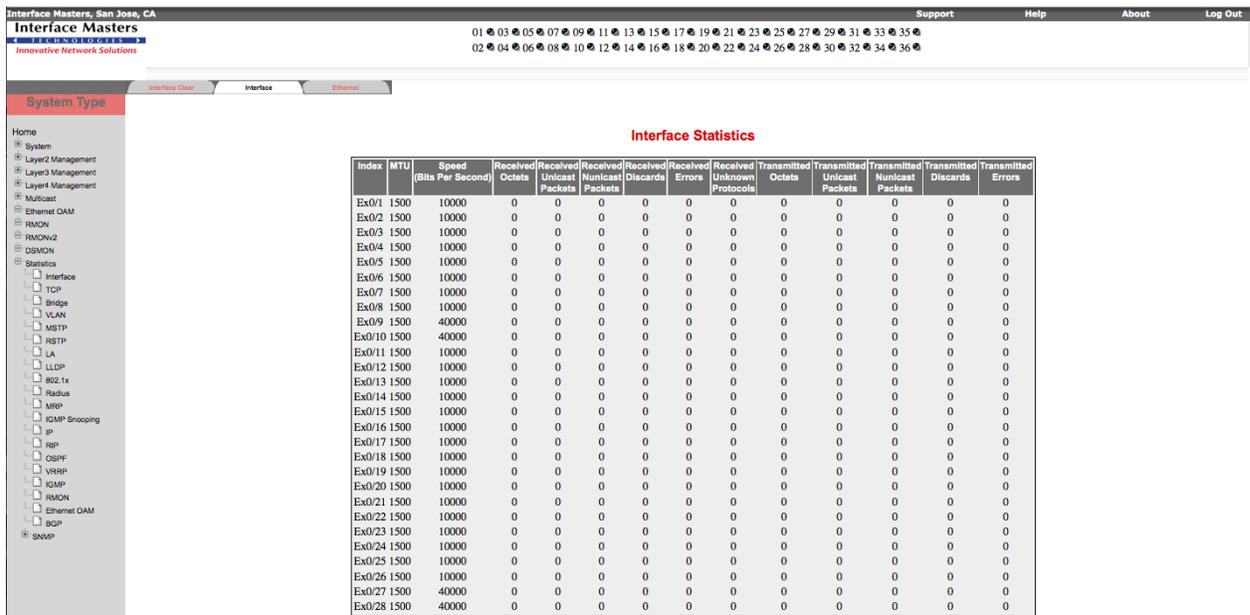


Figure 11-2: Interface Statistics - Statistics Group

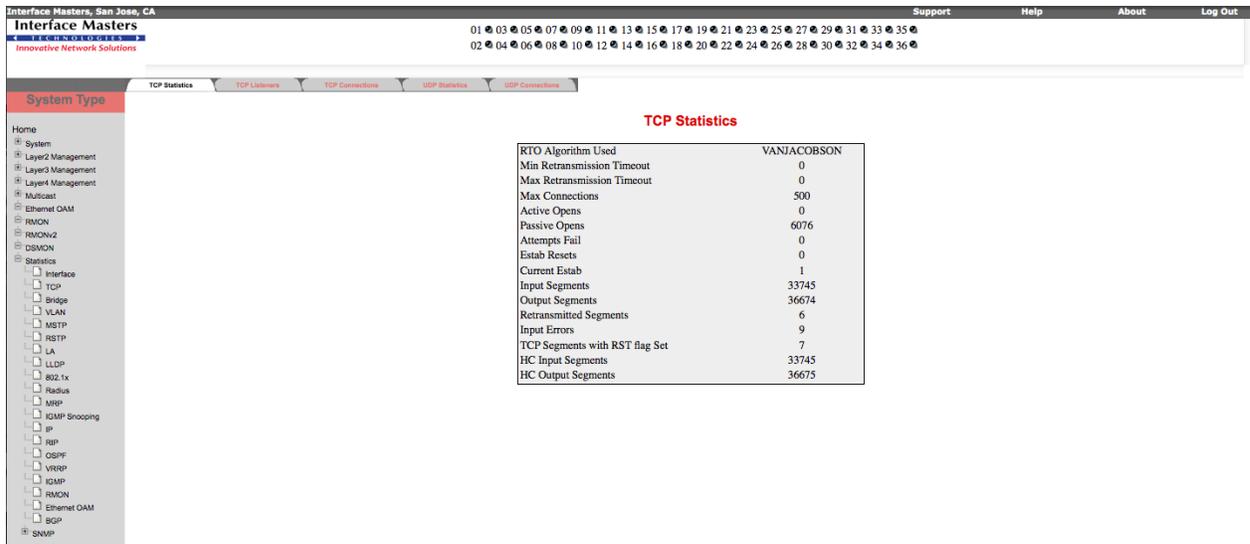


Figure 11-3: TCP Statistics - Statistics Group

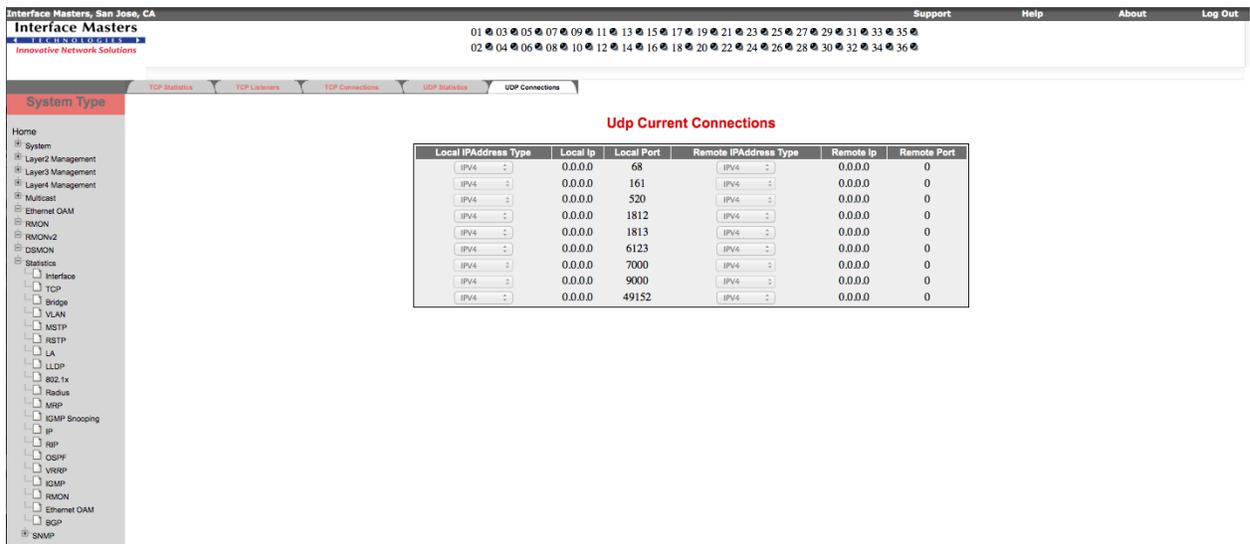


Figure 11-4: UDP Current Connection – Statistics Group

Interface Masters, San Jose, CA
 Interface Masters
 Innovative Network Solutions

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
 02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

System Type

Home

- System
- Layer2 Management
- Layer3 Management
- Layer4 Management
- Multicast
- Ethernet OAM
- RMON
- RMON2
- DSMON
- Statistics
 - Interface
 - TCP
 - Bridge
 - VLAN
 - MSTP
 - RSTP
 - LA
 - LLDP
 - 802.1x
 - Radius
 - MRP
 - IGMP Snooping
 - IP
 - RIP
 - OSPF
 - VRP
 - IGMP
 - RMON
 - Ethernet OAM
 - SGP
 - SNMP

UDP Statistics

InDatagrams	15300
No of Ports	15267
InErrors	15267
OutDatagrams	2
HC InDatagrams	15300
HC OutDatagrams	2

Figure 11-5: UDP Statistics - Statistics Group

Interface Masters, San Jose, CA
 Interface Masters
 Innovative Network Solutions

01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35
 02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36

System Type

Home

- System
- Layer2 Management
- Layer3 Management
- Layer4 Management
- Multicast
- Ethernet OAM
- RMON
- RMON2
- DSMON
- Statistics
 - Interface
 - TCP
 - Bridge
 - VLAN
 - MSTP
 - RSTP
 - LA
 - LLDP
 - 802.1x
 - Radius
 - MRP
 - IGMP Snooping
 - IP
 - RIP
 - OSPF
 - VRP
 - IGMP
 - RMON
 - Ethernet OAM
 - SGP
 - SNMP

IGMP Snooping Clear Statistics

Clear Vlan Counters All Vlan ID

Vlan ID

Apply

Figure 11-6: IGMP Snooping Clear Statistics – Statistics Group