



1/10 and 10-Gigabit Layer 2/3 Ethernet Switches



SSE-G24-TG4
1/10-Gigabit Ethernet Switch



SSE-G48-TG4
1/10-Gigabit Ethernet Switch



SSE-X24S/R
10/40-Gigabit Ethernet Switch



SSE-X3348S/R
10/40-Gigabit Ethernet Switch



SSE-X3348T/R
10/40-Gigabit Ethernet Switch

User's Manual

Revision 1.1d

The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPERMICRO BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPERMICRO SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate"

WARNING: HANDLING OF LEAD SOLDER MATERIALS USED IN THIS PRODUCT MAY EXPOSE YOU TO LEAD, A CHEMICAL KNOWN TO THE STATE OF CALIFORNIA TO CAUSE BIRTH DEFECTS AND OTHER REPRODUCTIVE HARM.

1/10 and 10-Gigabit Layer 2/3 Ethernet Switches User's Manual
Release Date: April 7, 2017

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2015 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Table of Contents

Chapter 1 Introduction	1-1
1-1 Introduction.....	1-1
1-2 Overview.....	1-1
1-3 Product Checklist of Typical Components.....	1-2
1-4 Features.....	1-3
1-5 Physical Characteristics.....	1-3
1-6 Contacting Supermicro.....	1-4
Chapter 2 Standardized Warning Statements	2-1
2-1 About Standardized Warning Statements.....	2-1
Warning Definition.....	2-1
Installation Instructions.....	2-3
Circuit Breaker.....	2-4
Power Disconnection Warning.....	2-5
Equipment Installation.....	2-6
Restricted Area.....	2-7
Battery Handling.....	2-9
Redundant Power Supplies.....	2-10
Backplane Voltage.....	2-11
Comply with Local and National Electrical Codes.....	2-12
Product Disposal.....	2-13
Hot Swap Fan Warning.....	2-14
Power Cable and AC Adapter.....	2-15
Chapter 3 Installation and Setup	3-1
3-1 Installation.....	3-1
3-2 Configuring the Switch Module.....	3-1
Web-based Management Utility.....	3-1
Command Line.....	3-2
Firmware.....	3-3
Firmware Upgrading Procedures.....	3-3
Firmware Failure Recovery Steps.....	3-6
Chapter 4 Ports and Indicators	4-1
4-1 SSE-G24-TG4 Ports and Indicators.....	4-1
4-2 SSE-G48-TG4 Ports and Indicators.....	4-2

4-3 SSE-X24S/R Ports and Indicators.....	4-3
4-4 SSE-X3348S/R Ports and Indicators	4-4
4-5 SSE-X3348T/R Ports and Indicators	4-5
4-6 Ports	4-6
RJ45 Compatible Port.....	4-6
Combo Ports	4-6
10-Gb/s Port Module Bays.....	4-6
Serial Ports	4-7
Power Port	4-7
4-7 Indicators	4-7
Chapter 5 Web Based Management Utility	5-1
Nomenclature.....	5-1
5-1 Overview	5-1
5-2 Login.....	5-2
5-3 Home Page	5-3
Top Page Links	5-7
Top LED Display	5-7
Left Side Tree.....	5-7
Middle Configuration Link Table	5-8
5-4 System Management Page	5-9
System Settings	5-10
System Settings	5-10
System Version	5-12
Management IP.....	5-13
File Management	5-14
Save Configuration.....	5-14
File Copy	5-15
File Management	5-15
Firmware Upgrade	5-15
Management Security	5-16
Management Security	5-16
User Accounts	5-17
Radius	5-18
TACACS+.....	5-19
TACACS+ Servers	5-20
IP Auth Manager	5-21
SSH.....	5-22
SSL	5-23

Syslog	5-24
ACL	5-25
MAC ACL	5-26
IP Standard ACL.....	5-27
IP Extended ACL.....	5-28
WEB Settings.....	5-30
SNMP.....	5-31
Community.....	5-33
Group	5-34
Group Access.....	5-35
View	5-36
Target Address	5-37
Target Parameter	5-38
User.....	5-39
Trap Manager.....	5-40
SNMP AgentX	5-41
RMON	5-42
Basic Settings	5-42
Events	5-43
Alarm.....	5-44
Ethernet Statistics	5-45
History.....	5-47
QoS.....	5-48
Basic Settings	5-48
Classmap	5-49
Policymap.....	5-50
VLAN COS.....	5-51
COS Queue Mapping.....	5-51
Queue Configuration	5-52
Time Management	5-53
NTP Settings	5-53
Clock Settings	5-55
Stack	5-55
Stack Settings	5-58
Stack Details	5-59
Stack Link Status	5-60
Stack Counters.....	5-61
CX4 Cable Length.....	5-62
5-5 Layer 2 Management.....	5-63
Layer 2 Basic Settings	5-64

Port Manager	5-65
Basic Settings	5-66
Port Monitoring.....	5-67
Port Control.....	5-68
Storm Control/Rate Limiting.....	5-69
Protected Ports	5-70
VLAN.....	5-71
Basic Settings	5-71
Port Settings.....	5-72
Static VLANs	5-73
Protocol Group	5-74
Port Protocol	5-75
MAC VLAN.....	5-76
Wildcard	5-77
Dynamic VLAN.....	5-78
Dynamic VLAN.....	5-78
Port Settings.....	5-79
GARP Timers	5-80
Spanning Tree.....	5-81
RSTP	5-81
Global Settings.....	5-82
Basic Settings	5-83
Port Settings.....	5-84
Port Status	5-85
MSTP	5-86
Basic Settings	5-87
Timers	5-88
Port Configuration	5-89
VLAN Mapping.....	5-90
Port Settings.....	5-91
CIST Port Status	5-92
Link Aggregation (LA)	5-93
Basic Settings	5-94
Interface Settings	5-95
Port Settings.....	5-96
LLDP	5-97
Global Settings	5-97
Interface Settings	5-99
802.1x	5-101
Basic Settings	5-101

Port Settings.....	5-102
Timers	5-103
Local AS	5-105
Filters	5-106
Unicast Filters	5-106
Multicast Filters	5-107
Link Tracking.....	5-108
Loop Protect.....	5-109
5-6 Layer 3 Management.....	5-110
IP.....	5-111
VLAN Interface.....	5-111
IPv4 AddrConf.....	5-112
Static ARP.....	5-113
IP Route	5-114
LoopBack Settings	5-115
IP V6	5-116
IPv6 Route	5-116
IPv6 Interface.....	5-117
ND Cache.....	5-118
Address Settings.....	5-119
Address Profile.....	5-120
Prefix Settings.....	5-121
DHCP Server	5-122
Basic Settings	5-122
Pool Settings	5-123
MAC Binding	5-124
Port Binding.....	5-125
DHCP Relay.....	5-126
Basic Settings	5-126
Interface Conf.....	5-127
RIP	5-127
Basic Settings	5-128
Interface	5-129
Neighbors.....	5-130
Security	5-131
Summarization	5-132
RIPng.....	5-132
RIP6 Interface	5-133
Filters	5-134
OSPF	5-134

Basic Settings	5-135
Area.....	5-136
Interface	5-137
Virtual Interface	5-139
Neighbor.....	5-140
RRD Route.....	5-141
Aggregation.....	5-142
AsExtAggregation	5-143
OSPF V3.....	5-144
Basic Settings	5-145
Interface	5-146
Area.....	5-148
Ext Aggregation.....	5-149
BGP	5-150
Basics.....	5-151
Neighbors.....	5-152
Multi-Exit Disc	5-153
Local Pref	5-154
Filters	5-155
Route Aggr	5-156
Advanced	5-157
Community.....	5-159
RRD	5-160
Basic Settings	5-160
BGP.....	5-161
RIP	5-162
OSPF	5-163
RRD6	5-164
Basic Settings	5-164
Filters	5-165
OSPFv3.....	5-166
RIP6.....	5-167
VRRP	5-168
Basic Settings	5-168
VRRP Settings.....	5-169
5-7 Multicast.....	5-170
IGMP Snooping.....	5-170
Basic Settings	5-171
Timer	5-172
Interface Configuration.....	5-173

Router Ports	5-174
Group Information	5-175
Dynamic Multicast	5-176
Dynamic Multicast	5-176
Port Settings	5-177
IGMP	5-178
Basic Settings	5-178
Interface Configuration	5-179
Group Information	5-180
Source Information	5-181
PIM	5-182
Basic Settings	5-182
Component	5-183
Interfaces	5-184
Candidate RPs	5-185
Threshold	5-186
Static RP	5-187
DVMRP	5-188
Basic Settings	5-188
Interfaces	5-189
5-8 Statistics	5-190
Interface	5-191
Interface	5-191
Ethernet	5-193
Port Channel	5-194
Radius	5-196
TACACS+ Statistics	5-198
Syslog	5-200
Syslog Buffer	5-200
Syslog File	5-201
RMON Ethernet Statistics	5-202
SNMP Statistics	5-204
Agent	5-204
AgentX	5-205
VLAN	5-207
Current DB	5-207
Multicast Table	5-208
Capabilities	5-209
MAC Address Table	5-210
RSTP Statistics	5-210

Information	5-211
Port Statistics	5-212
MSTP Statistics.....	5-213
MSTP Information	5-213
CIST Port Statistics	5-214
MSTI Port Statistics.....	5-216
Link Aggregation (LA)	5-217
Port LACP Stats	5-217
Neighbor Stats	5-218
LLDP	5-219
Statistics.....	5-219
Errors	5-220
Neighbors.....	5-221
Traffic	5-222
Interface Traffic	5-223
802.1X.....	5-223
Session Stats	5-224
Supp-Session Stats.....	5-225
Mac-Session Stats	5-226
IP.....	5-227
ARP Cache	5-227
ICMP Statistics.....	5-228
IPv6.....	5-229
IPv6 Interface	5-229
ICMPv6	5-231
RIP	5-233
RIP6.....	5-233
Interface Statistics.....	5-234
Route Information.....	5-235
OSPF	5-235
Route Information.....	5-236
Link State Database.....	5-237
OSPFv3	5-238
OSPFv3 Route Information	5-238
OSPFv3 Link State Database	5-239
VRRP	5-240
IGMP Snooping.....	5-242
IGS Clear Stats	5-242
IGS Statistics.....	5-243
IGS V3 Statistics	5-244

IGMP	5-245
PIM.....	5-246
Interface Stats	5-247
Neighbor Stats	5-248
BSR Info.....	5-249
RP Set Info.....	5-250
Mroute Info.....	5-251
DVMRP	5-252
Routes.....	5-252
Multicast Routes.....	5-253
Prune Forward	5-254

Appendix A Rack Installation	A-1
A-1 Overview	A-1
A-2 Unpacking the System	A-1
A-3 Preparing for Setup	A-1
Choosing a Setup Location	A-1
A-4 Warnings and Precautions!	A-2
Rack Precautions.....	A-2
General Precautions	A-2
Lithium Battery Precaution.....	A-2
Rack Mounting Considerations	A-3
Ambient Operating Temperature	A-3
Reduced Airflow	A-3
Mechanical Loading	A-3
Circuit Overloading.....	A-3
Reliable Ground	A-3
A-5 Rack Mounting Instructions.....	A-3
Identifying the Sections of the Rack Rails	A-3
Separating the Sections of the Rails.....	A-4
Installing the Inner Rails.....	A-4
Installing the Outer Rails.....	A-5
Installing the Switch into a Rack	A-8
Installing the Switch into a Telco Rack	A-9

Notes

Preface

About this Manual

This manual is written for professional system integrators, Information Technology professionals, service personnel and technicians. It provides information for the installation and use of Supermicro's Layer 2/3 1/10 and 10-Gigabit Ethernet switches. Installation and maintenance should be performed by experienced professionals only.

Manual Organization

Chapter 1: Introduction

The first chapter provides a checklist of the main components included with Layer 2/3 1/10 and 10-Gigabit Ethernet switches and describes their main features.

Chapter 2: System Safety

You should familiarize yourself with this chapter for a general overview of safety precautions that should be followed when installing and servicing Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

Chapter 3: Setup and Installation

Refer here for details on installing Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

Chapter 4: Ports and Indicators

This chapter covers the various ports and LED indicators found on Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

Chapter 5: Web-based Interface

This chapter covers the web-based interface control screens for Layer 2/3 1/10 and 10-Gigabit Ethernet switches and their use.

Appendix A: Rack Installation

This appendix describes the steps to take to attach rack-mounting rails to the SSE-X24S/R, the SSE-X3348S/R and the SSE-X3348T/R switches for installation in a rack.

Notes

Chapter 1

Introduction

1-1 Introduction

This document is designed to provide **Supermicro Switch** users with the information required to configure the basic functionalities on the switch through the Web graphical user interface (GUI).

Supermicro Switch products can be configured through Web browsers like Internet Explorer or Mozilla Firefox. To manage a switch through a web browser, type in the management IP address in the web browser address bar. This will allow you to start accessing the switch. For example, if the management IP address of the switch is 192.168.100.102, the switch can be accessed through the Web browser by typing **http://192.168.100.102** in the address bar of the web browser.

NOTE: Most of the contents of this manual apply to all of these seven switch products:

- SSE-G24-TG4
- SSE-G48-TG4
- SSE-X24S/R
- SSE-X3348S/R
- SSE-X3348T/R
- SBM-GEM-X2C
- SBM-GEM-X2C+
- SBM-XEM-X10SM

In a few sections the contents differ for these products. In those specific places, the applicable product is clearly identified. So if any particular product is not mentioned, you can assume that the contents are valid for these six products.

1-2 Overview

Both the SSE-G24-TG4 and the SSE-G48-TG4 1/10-Gigabit Ethernet Layer 2/3 switches include two bays for up to four 10-Gb/s uplink ports (one or two dual-port CX4 modules and/or one or two dual-port XFP modules and/or one or two dual port SFP+ modules), and either 24 (SSE-G24-TG4) or 48 (SSE-G48-TG4) duplex 1-Gb/s (RJ45) ports for LAN interfaces (of which four are combo ports that can alternately be connected to SFP cables with an appropriate transceiver). These Ethernet switches also have an external serial connector for connecting to an external console.

The SSE-X24S and SSE-X24SR are fully self-contained; no additional modules are required. The SSE-X3348S and SSE-X3348SR are also fully self contained, as are the SSE-X3348T and SSE-X3348T/R. All of the 10G switches contain two redundant hot-swappable power supplies installed at the factory. The SSE-X24S, SSE-X3348S and SSE-X3348T have a “normal” airflow direction for cooling – from the front of the unit to the back. The SSE-X24SR, SSE-X3348SR and SSE-X3348T/R have a “reverse” airflow direction for cooling – from the back of the unit to the front. The models are otherwise identical. The SSE-X24SR, SSE-X3348SR or SSE-X3348T/R may be more appropriate for large data center installations with the switch installed in the rear of a rack facing the “hot aisle”.

1-3 Product Checklist of Typical Components

The following components are included with SSE-G24-TG4 or SSE-G48-TG4 Layer 2/3 1/10-Gigabit Ethernet switches:

- Serial cable
- Power cables
- Mounting Ears for rack assembly (see note)
- Two 10-Gb/s port module bays for either CX-4, XFP, or SFP+ ports (modules sold separately)
- CD-ROM with manuals

The following components are included with the SSE-X24S/R switches:

- Power Cables (2)
- Mounting ears for rack assembly (see note)
- CD-ROM with manuals

The following components are included with the SSE-X3348S/R and SSE-X3348T/R switches:

- Power cables
- Console Cable
- Mounting ears for rack assembly (see note)
- Quick Installation Guide

NOTE: The mounting ears can secure an SSE-X24S/R or SSE-X3348S/R switch to a rack, but will not reliably support the full weight of the switch for an extended period of time. Please use Supermicro mounting rails (CSE-PT52L) for full support of the switch in a rack installation (see Appendix A for details).

1-4 Features

The Layer 2/3 1/10 and 10-Gigabit Ethernet switches offer the following features:

- 1:1 Non-blocking Connectivity
- Jumbo Frames support (up to 9k bytes)
- Layer 2/3 switch
- Link Aggregation support
- Comprehensive routing and switching protocol support (QoS, Priority, Flow Control, OSPF-v2, RIP v2, ACLs and IGMPv2/v3)
- Browser based management/CLI interface
- Telnet accessible – RFC854/855
- Supports STP, RSTP, MSTP, IGMP snooping and 802.1x

1-5 Physical Characteristics

The Layer 2/3 1/10 and 10-Gigabit Ethernet switches have the following physical characteristics:

- 1U form factor
- Dimensions: 440 x 387 x 44 mm (17.32 x 15.24 x 1.73 inch) (W x D x H) or 440 x 473 x 44 mm (17.3 x 18.62 x 1.73 inch) for the SSE-X3348S/R
- Weight: 5.6 kg (12.4 lbs) SSE-G24-TG4, 6.2 kg (13.7 lbs) SSE-G48-TG4, 7.58 kg (16.7 lbs) SSE-X24S/R, 8.2 kg (18.1 lbs) SSE-X3348S/R, or 9.2 kg (20.3 lbs) SSE-X3348T/R

1-6 Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)

Web Site: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 23511
Taiwan (R.O.C)

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Web Site: www.supermicro.com.tw

Technical Support:

Email: support@supermicro.com.tw

Tel: +886-(2)-8226-3990

Chapter 2

Standardized Warning Statements

2-1 About Standardized Warning Statements

The following statements are industry standard warnings, provided to warn the user of situations which have the potential for bodily injury. Should you have questions or experience difficulty, contact Supermicro's Technical Support department for assistance. Only certified technicians should attempt to install or configure components.

Read this appendix in its entirety before installing or configuring components in the Supermicro chassis.

These warnings may also be found on our web site at http://www.supermicro.com/about/policies/safety_information.cfm.

Warning Definition



Warning!

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

警告の定義

この警告サインは危険を意味します。

人身事故につながる可能性がありますので、いずれの機器でも動作させる前に、電気回路に含まれる危険性に注意して、標準的な事故防止策に精通して下さい。

此警告符号代表危險。

您正處於可能受到嚴重傷害的工作環境中。在您使用設備開始工作之前，必須充分意識到觸電的危險，並熟練掌握防止事故發生的標準工作程序。請根據每項警告結尾的聲明號碼找到此設備的安全性警告說明的翻譯文本。

此警告符號代表危險。

您正處於可能身體可能會受損傷的工作環境中。在您使用任何設備之前，請注意觸電的危險，並且要熟悉預防事故發生的標準工作程序。請依照每一注意事項後的號碼找到相關的翻譯說明內容。

Warnung

WICHTIGE SICHERHEITSHINWEISE

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES.

IMPORTANTES INFORMATIONS DE SÉCURITÉ

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS.

תקנת הצהרות אזהרה

הצהרות הבאות הן אזהרות על פי תקני התעשייה, על מנת להזהיר את המשתמש מפני חבלה פיזית אפשרית. במידה ויש שאלות או היתקלות בבעיה כלשהי, יש ליצור קשר עם מחלקת תמיכה טכנית של סופרמיקרו. טכנאים מוסמכים בלבד רשאים להתקין או להגדיר את הרכיבים.

יש לקרוא את הנספח במלואו לפני התקנת או הגדרת הרכיבים במארזי סופרמיקרו.

تحذير! هذا الرمز يعني خطر انك في حالة يمكن أن تتسبب في اصابة جسدية .
قبل أن تعمل على أي معدات، كن على علم بالمخاطر الناجمة عن الدوائر
الكهربائية

وكن على دراية بالممارسات الوقائية لمنع وقوع أي حوادث
استخدم رقم البيان المنصوص في نهاية كل تحذير للعثور ترجمتها

안전을 위한 주의사항

경고!

이 경고 기호는 위험이 있음을 알려 줍니다. 작업자의 신체에 부상을 야기 할 수 있는 상태에 있게 됩니다. 모든 장비에 대한 작업을 수행하기 전에 전기회로와 관련된 위험 요소들을 확인하시고 사전에 사고를 방지할 수 있도록 표준 작업절차를 준수해 주시기 바랍니다.

해당 번역문을 찾기 위해 각 경고의 마지막 부분에 제공된 경고문 번호를 참조하십시오

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwings symbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij een elektrische installatie betrokken risico's en dient u op de hoogte te zijn van de standaard procedures om ongelukken te voorkomen. Gebruik de nummers aan het eind van elke waarschuwing om deze te herleiden naar de desbetreffende locatie.

BEWAAR DEZE INSTRUCTIES

Installation Instructions



Warning!

Read the installation instructions before connecting the system to the power source.

設置手順書

システムを電源に接続する前に、設置手順書をお読み下さい。

警告

将此系统连接电源前，请先阅读安装说明。

警告

將系統與電源連接前，請先閱讀安裝說明。

Warnung

Vor dem Anschließen des Systems an die Stromquelle die Installationsanweisungen lesen.

¡Advertencia!

Lea las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Attention

Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

יש לקרוא את הוראות התקנה לפני חיבור המערכת למקור מתח.

اقر إرشادات التركيب قبل توصيل النظام إلى مصدر للطاقة

시스템을 전원에 연결하기 전에 설치 안내를 읽어주십시오.

Waarschuwing

Raadpleeg de installatie-instructies voordat u het systeem op de voedingsbron aansluit.

Circuit Breaker



Warning!

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 20 A.

サーキット・ブレーカー

この製品は、短絡（過電流）保護装置がある建物での設置を前提としています。

保護装置の定格が 250 V、20 A を超えないことを確認下さい。

警告

此产品的短路（过载电流）保护由建筑物的供电系统提供，确保短路保护设备的额定电流不大于 250V, 20A。

警告

此產品的短路（過載電流）保護由建築物的供電系統提供，確保短路保護設備的額定電流不大於 250V, 20A。

Warnung

Dieses Produkt ist darauf angewiesen, dass im Gebäude ein Kurzschluss- bzw. Überstromschutz installiert ist. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung nicht mehr als: 250 V, 20 A beträgt.

¡Advertencia!

Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del edificio. Asegúrese de que el dispositivo de protección no sea superior a: 250 V, 20 A.

Attention

Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifiez que le courant nominal du dispositif de protection n'est pas supérieur à :250 V, 20 A.

מוצר זה מסתמך על הגנה המותקנת במבנים למניעת קצר חשמלי. יש לוודא כי המכשיר המגן מפני הקצר החשמלי הוא לא יותר מ-250 V, 20 A

هذا المنتج يعتمد على معدات الحماية من الدوائر القصيرة التي تم تثبيتها في
المبنى
تأكد من أن تقييم الجهاز الوقائي ليس أكثر من: 20A, 250V

경고 !

이 제품은 전원의 단락 (과전류) 방지에 대해서 전적으로 건물의 관련 설비에 의존합니다. 보호장치의 정격이 반드시 250V(볼트), 20A(암페어)를 초과하지 않도록 해야 합니다.

Waarschuwing

Dit product is afhankelijk van de kortsluitbeveiliging (overspanning) van uw elektrische installatie. Controleer of het beveiligde apparaat niet groter gedimensioneerd is dan 220V, 20A.

Power Disconnection Warning



Warning!

The system must be disconnected from all sources of power and the power cord removed from the power supply module(s) before accessing the chassis interior to install or remove system components.

電源切斷の警告

システムコンポーネントの取り付けまたは取り外しのために、シャーシ内部にアクセスするには、

システムの電源はすべてのソースから切斷され、電源コードは電源モジュールから取り外す必要があります。

警告

在你打开机箱并安装或移除内部器件前，必须将系统完全断电，并移除电源线。

警告

在您打開機殼安裝或移除內部元件前，必須將系統完全斷電，並移除電源線。

Warnung

Das System muss von allen Quellen der Energie und vom Netzanschlusskabel getrennt sein, das von den Spg.Versorgungsteilmodulen entfernt wird, bevor es auf den Chassisinnenraum zurückgreift, um Systemsbestandteile anzubringen oder zu entfernen.

¡Advertencia!

El sistema debe ser disconnected de todas las fuentes de energía y del cable eléctrico quitado de los módulos de fuente de alimentación antes de tener acceso el interior del chasis para instalar o para quitar componentes de sistema.

Attention

Le système doit être débranché de toutes les sources de puissance ainsi que de son cordon d'alimentation secteur avant d'accéder à l'intérieur du châssis pour installer ou enlever des composants de système.

אזהרה מפני ניתוק חשמלי

!אזהרה!

יש לנתק את המערכת מכל מקורות החשמל ויש להסיר את כבל החשמלי מהספק לפני גישה לחלק הפנימי של המארז לצורך התקנת או הסרת רכיבים.

يجب فصل النظام من جميع مصادر الطاقة وإزالة سلك الكهرباء من وحدة امداد الطاقة قبل

الوصول إلى المناطق الداخلية للهيكल لتثبيت أو إزالة مكونات الجهاز

경고!

시스템에 부품들을 장착하거나 제거하기 위해서는 채시 내부에 접근하기 전에 반드시 전원 공급장치로부터 연결되어있는 모든 전원과 전기코드를 분리해주어야 합니다.

Waarschuwing

Voordat u toegang neemt tot het binnenwerk van de behuizing voor het installeren of verwijderen van systeem onderdelen, dient u alle spanningsbronnen en alle stroomkabels aangesloten op de voeding(en) van de behuizing te verwijderen.

Equipment Installation



Warning!

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

機器の設置

トレーニングを受け認定された人だけがこの装置の設置、交換、またはサービスを許可されています。

警告

只有经过培训且具有资格的人员才能进行此设备的安装、更换和维修。

警告

只有經過受訓且具資格人員才可安裝、更換與維修此設備。

Warnung

Das Installieren, Ersetzen oder Bedienen dieser Ausrüstung sollte nur geschultem, qualifiziertem Personal gestattet werden.

¡Advertencia!

Solamente el personal calificado debe instalar, reemplazar o utilizar este equipo.

Attention

Il est vivement recommandé de confier l'installation, le remplacement et la maintenance de ces équipements à des personnels qualifiés et expérimentés.

אזהרה!

צוות מוסמך בלבד רשאי להתקין, להחליף את הציוד או לתת שירות עבור הציוד.

يجب أن يسمح فقط للموظفين المؤهلين والمدربين لتكيب واستبدال أو خدمة هذا الجهاز
경고!

훈련을 받고 공인된 기술자만이 이 장비의 설치, 교체 또는 서비스를 수행할 수 있습니다.

Waarschuwing

Deze apparatuur mag alleen worden geïnstalleerd, vervangen of hersteld door geschoold en gekwalificeerd personeel.

Restricted Area



Warning!

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. (This warning does not apply to workstations).

アクセス制限区域

このユニットは、アクセス制限区域に設置されることを想定しています。

アクセス制限区域は、特別なツール、鍵と錠前、その他のセキュリティの手段を用いてのみ出入りが可能です。

警告

此部件应安装在限制进出的场所，限制进出的场所指只能通过使用特殊工具、锁和钥匙或其它安全手段进出的场所。

警告

此裝置僅限安裝於進出管制區域，進出管制區域係指僅能以特殊工具、鎖頭及鑰匙或其他安全方式才能進入的區域。

Warnung

Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Der Zutritt zu derartigen Bereichen ist nur mit einem Spezialwerkzeug, Schloss und Schlüssel oder einer sonstigen Sicherheitsvorkehrung möglich.

¡Advertencia!

Esta unidad ha sido diseñada para instalación en áreas de acceso restringido. Sólo puede obtenerse acceso a una de estas áreas mediante la utilización de una herramienta especial, cerradura con llave u otro medio de seguridad.

Attention

Cet appareil doit être installée dans des zones d'accès réservés. L'accès à une zone d'accès réservé n'est possible qu'en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité.

אזור עם גישה מוגבלת

אזהרה!

יש להתקין את היחידה באזורים שיש בהם הגבלת גישה. הגישה ניתנת בעזרת כלי אבטחה בלבד (מפתח, מנעול וכד').

تم تخصيص هذه الوحدة لتركيبها في مناطق محظورة .
يمكن الوصول إلى منطقة محظورة فقط من خلال استخدام أداة خاصة،
قفل ومفتاح أو أي وسيلة أخرى للأمان

경고 !

이 장치는 접근이 제한된 구역에 설치하도록 되어있습니다. 특수도구, 잠금 장치 및 키, 또는 기타 보안 수단을 통해서만 접근 제한 구역에 들어갈 수 있습니다.

Waarschuwing

Dit apparaat is bedoeld voor installatie in gebieden met een beperkte toegang. Toegang tot dergelijke gebieden kunnen alleen verkregen worden door gebruik te maken van speciaal gereedschap, slot en sleutel of andere veiligheidsmaatregelen.

Battery Handling



Warning!

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

電池の取り扱い

電池交換が正しく行われなかった場合、破裂の危険性があります。交換する電池はメーカーが推奨する型、または同等のものを使用下さい。使用済電池は製造元の指示に従って処分して下さい。

警告

電池更換不當會有爆炸危險。請只使用同類電池或製造商推薦的功能相當的電池更換原有電池。請按製造商的說明處理廢舊電池。

警告

電池更換不當會有爆炸危險。請使用製造商建議之相同或功能相當的電池更換原有電池。請按照製造商的說明指示處理廢棄舊電池。

Warnung

Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Attention

Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

¡Advertencia!

Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

אזהרה!

קיימת סכנת פיצוץ של הסוללה במידה והוחלפה בדרך לא תקינה. יש להחליף את הסוללה בסוג התואם מחברת יצרן מומלצת.

סילוק הסוללות המשומשות יש לבצע לפי הוראות היצרן.

هناك خطر من انفجار في حالة استبدال البطارية بطريقة غير صحيحة فعليك استبدال البطارية

فقط بنفس النوع أو ما يعادلها كما أوصت به الشركة المصنعة تخلص من البطاريات المستعملة وفقا لتعليمات الشركة الصانعة

경고!

배터리가 올바르게 교체되지 않으면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

Waarschuwing

Er is ontploffingsgevaar indien de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type die door de fabrikant aanbevolen wordt. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften afgevoerd te worden.

Redundant Power Supplies



Warning!

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.

冗長電源裝置

このユニットは複数の電源装置が接続されている場合があります。

ユニットの電源を切るためには、すべての接続を取り外さなければなりません。

警告

此部件连接的电源可能不止一个，必须将所有电源断开才能停止给该部件供电。

警告

此裝置連接的電源可能不只一個，必須切斷所有電源才能停止對該裝置的供電。

Warnung

Dieses Gerät kann mehr als eine Stromzufuhr haben. Um sicherzustellen, dass der Einheit kein Strom zugeführt wird, müssen alle Verbindungen entfernt werden.

¡Advertencia!

Puede que esta unidad tenga más de una conexión para fuentes de alimentación. Para cortar por completo el suministro de energía, deben desconectarse todas las conexiones.

Attention

Cette unité peut avoir plus d'une connexion d'alimentation. Pour supprimer toute tension et tout courant électrique de l'unité, toutes les connexions d'alimentation doivent être débranchées.

אם קיים יותר מספק אחד

אזהרה!

ליחידה יש יותר מחיבור אחד של ספק. יש להסיר את כל החיבורים על מנת לרוקן את היחידה.

قد يكون لهذا الجهاز عدة اتصالات بوحدات امداد الطاقة.
يجب إزالة كافة الاتصالات لعزل الوحدة عن الكهرباء

경고 !

이 장치에는 한 개 이상의 전원 공급 단자가 연결되어 있을 수 있습니다. 이 장치에 전원을 차단하기 위해서는 모든 연결 단자를 제거해야만 합니다.

Waarschuwing

Deze eenheid kan meer dan één stroomtoevoeraansluiting bevatten. Alle aansluitingen dienen verwijderd te worden om het apparaat stroomloos te maken

Backplane Voltage



Warning!

Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.

バックプレーンの電圧

システムの稼働中は危険な電圧または電力が、バックプレーン上にかかっています。

修理する際にはご注意ください。

警告

当系统正在进行时，背板上有很危险的电压或能量，进行维修时务必小心。

警告

當系統正在進行時，背板上有危險的電壓或能量，進行維修時務必小心。

Warnung

Wenn das System in Betrieb ist, treten auf der Rückwandplatine gefährliche Spannungen oder Energien auf. Vorsicht bei der Wartung.

¡Advertencia!

Quando el sistema está en funcionamiento, el voltaje del plano trasero es peligroso. Tenga cuidado cuando lo revise.

Attention

Lorsque le système est en fonctionnement, des tensions électriques circulent sur le fond de panier. Prendre des précautions lors de la maintenance.

מתח בפנל האחורי

אזהרה !

קיימת סכנת מתח בפנל האחורי בזמן תפעול המערכת. יש להיזהר במהלך העבודה.

هناك خطر من التيار الكهربائي أو الطاقة الموجودة على اللوحة
عندما يكون النظام يعمل كن حذرا عند خدمة هذا الجهاز

경고 !

시스템이 동작 중일 때 후면판 (Backplane) 에는 위험한 전압이나 에너지가 발생 합니다. 서비스 작업 시 주의하십시오 .

Waarschuwing

Een gevaarlijke spanning of energie is aanwezig op de backplane wanneer het systeem in gebruik is. Voorzichtigheid is geboden tijdens het onderhoud.

Comply with Local and National Electrical Codes



Warning!

Installation of the equipment must comply with local and national electrical codes.

地方および国の電気規格に準拠

機器の取り付けはその地方および国の電気規格に準拠する必要があります。

警告

设备安装必须符合本地与本国电气法规。

警告

設備安裝必須符合本地與本國電氣法規。

Warnung

Die Installation der Geräte muss den Sicherheitsstandards entsprechen.

¡Advertencia!

La instalacion del equipo debe cumplir con las normas de electricidad locales y nacionales.

Attention

L'équipement doit être installé conformément aux normes électriques nationales et locales.

תיאום חוקי החשמל הארצי

אזהרה !

התקנת הציוד חייבת להיות תואמת לחוקי החשמל המקומיים והארציים.

تركيب المعدات الكهربائية يجب أن يمتثل للقوانين المحلية والوطنية المتعلقة
بالكهرباء

경고!

현 지역 및 국가의 전기 규정에 따라 장비를 설치해야 합니다.

Waarschuwing

Bij installatie van de apparatuur moet worden voldaan aan de lokale en nationale elektriciteitsvoorschriften.

Product Disposal



Warning!

Ultimate disposal of this product should be handled according to all national laws and regulations.

製品の廃棄

この製品を廃棄処分する場合、国の関係する全ての法律・条例に従い処理する必要があります。

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

¡Advertencia!

Al deshacerse por completo de este producto debe seguir todas las leyes y reglamentos nacionales.

Attention

La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.

סילוק המוצר

אזהרה!

סילוק סופי של מוצר זה חייב להיות בהתאם להנחיות וחוקי המדינה.

عند التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القوانين واللوائح الوطنية

경고!

이 제품은 해당 국가의 관련 법규 및 규정에 따라 폐기되어야 합니다.

Waarschuwing

De uiteindelijke verwijdering van dit product dient te geschieden in overeenstemming met alle nationale wetten en reglementen.

Hot Swap Fan Warning



Warning!

The fans might still be turning when you remove the fan assembly from the chassis. Keep fingers, screwdrivers, and other objects away from the openings in the fan assembly's housing.

ファン・ホットスワップの警告

シャーシから冷却ファン装置を取り外した際、ファンがまだ回転している可能性があります。ファンの開口部に、指、ドライバー、およびその他のものを近づけないで下さい。

警告

当您从机架移除风扇装置，风扇可能仍在转动。小心不要将手指、螺丝起子和其他物品太靠近风扇。

警告

當您從機架移除風扇裝置，風扇可能仍在轉動。小心不要將手指、螺絲起子和其他物品太靠近風扇。

Warnung

Die Lüfter drehen sich u. U. noch, wenn die Lüfterbaugruppe aus dem Chassis genommen wird. Halten Sie Finger, Schraubendreher und andere Gegenstände von den Öffnungen des Lüftergehäuses entfernt.

¡Advertencia!

Los ventiladores podran dar vuelta cuando usted quite ell montaje del ventilador del chasis. Mandtenga los dedos, los destornilladores y todos los objetos lejos de las aberturas del ventilador

Attention

Il est possible que les ventilateurs soient toujours en rotation lorsque vous retirerez le bloc ventilateur du châssis. Prenez garde à ce que doigts, tournevis et autres objets soient éloignés du logement du bloc ventilateur.

! אזהרה

כאשר מסירים את חלקי המאוורר מהמארו, יתכן והמאווררים עדיין עובדים. יש להרחיק למרחק בטוח את האצבעות וכלי עבודה שונים מהפתחים בתוך המאוורר

من الممكن أن المراوح لا تزال تدور عند إزالة كتلة المروحة من الهيكل يجب إبقاء الأصابع ومفكات البراغي وغيرها من الأشياء بعيدا عن الفتحات في كتلة المروحة.

경고 !

새시로부터 팬 조립품을 제거할 때 팬은 여전히 회전하고 있을 수 있습니다. 팬 조립품 외관의 열려있는 부분들로부터 손가락 및 스크류드라이버, 다른 물체들이 가까이 하지 않도록 배치해 주십시오.

Waarschuwing

Het is mogelijk dat de ventilator nog draait tijdens het verwijderen van het ventilatorsamenstel uit het chassis. Houd uw vingers, schroevendraaiers en eventuele andere voorwerpen uit de buurt van de openingen in de ventilatorbehuizing.

Power Cable and AC Adapter



Warning!

When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL or CSA -certified cables (that have UL/CSA shown on the code) for any other electrical devices than products designated by Supermicro only.

電源コードと AC アダプター

製品を設置する場合、提供または指定された接続ケーブル、電源コードと AC アダプターを使用下さい。他のケーブルやアダプタを使用すると故障や火災の原因になることがあります。電気用品安全法は、UL または CSA 認定のケーブル (UL/CSE マークがコードに表記) を Supermicro が指定する製品以外に使用することを禁止しています。

警告

安装此产品时,请使用本身提供的或指定的连接线,电源线和电源适配器.使用其它线材或适配器可能会引起故障或火灾。除了 Supermicro 所指定的产品,电气用品和材料安全法律规定禁止使用未经 UL 或 CSA 认证的线材。(线材上会显示 UL/CSA 符号)。

警告

安裝此產品時,請使用本身提供的或指定的連接線,電源線和電源適配器.使用其它線材或適配器可能會引起故障或火災。除了 Supermicro 所指定的產品,電氣用品和材料安全法律規定禁止使用未經 UL 或 CSA 認證的線材。(線材上會顯示 UL/CSA 符號)。

Warnung

Bei der Installation des Produkts, die zur Verfügung gestellten oder benannt Anschlusskabel, Stromkabel und Netzteile. Verwendung anderer Kabel und Adapter kann zu einer Fehlfunktion oder ein Brand entstehen. Elektrische Geräte und Material Safety Law verbietet die Verwendung von UL-oder CSA-zertifizierte Kabel, UL oder CSA auf der Code für alle anderen elektrischen Geräte als Produkte von Supermicro nur bezeichnet gezeigt haben.

¡Advertencia!

Al instalar el producto, utilice los cables de conexión previstos o designados, los cables y adaptadores de CA. La utilización de otros cables y adaptadores podría ocasionar un mal funcionamiento o un incendio. Aparatos Eléctricos y la Ley de Seguridad del Material prohíbe el uso de UL o CSA cables certificados que tienen UL o CSA se muestra en el código de otros dispositivos eléctricos que los productos designados por Supermicro solamente.

Attention

Lors de l'installation du produit, utilisez les bables de connection fournis ou désigné. L'utilisation d'autres cables et adaptateurs peut provoquer un dysfonctionnement ou un incendie. Appareils électroménagers et de loi sur la sécurité Matériel interdit l'utilisation de UL ou CSA câbles certifiés qui ont UL ou CSA indiqué sur le code pour tous les autres appareils électriques que les produits désignés par Supermicro seulement.

חשמליים ומתאמי AC

אזהרה!

כאשר מתקינים את המוצר, יש להשתמש בכבלים, ספקים ומתאמים AC אשר נועדו וסופקו לשם כך. שימוש בכל כבל או מתאם אחר יכול לגרום לתקלה או קצר חשמלי. על פי חוקי שימוש במכשירי חשמל וחוקי בטיחות, קיים איסור להשתמש בכבלים המוסמכים ב- UL או ב- CSA (כשאר מופיע עליהם קוד של UL/CSA) עבור כל מוצר חשמלי אחר שלא צוין על ידי סופרקמיקרו בלבד.

عند تركيب الجهاز يجب استخدام كابلات التوصيل، والكابلات الكهربائية ومحولات التيار المتردد التي . أن استخدام أي كابلات ومحولات أخرى يتسبب في حدوث عطل أو حريق. تم توفيرها لك مع المنتج الأجهزة الكهربائية ومواد قانون السلامة يحظر استخدام الكابلات UL أو CSA معتمدة من قبل لأي أجهزة كهربائية أخرى غير المنتجات المعينة من قبل Supermicro (التي تحمل علامة UL/CSA)

경고 !

제품을 설치할 때에는 제공되거나 지정된 연결케이블과 전원케이블, AC 어댑터를 사용해야 합니다. 그 밖의 다른 케이블들이나 어댑터들은 고장 또는 화재의 원인이 될 수 있습니다. 전기용품안전법 (Electrical Appliance and Material Safety Law) 은 슈퍼마이크로에서 지정한 제품들 외에는 그 밖의 다른 전기 장치들을 위한 UL 또는 CSA 에서 인증한 케이블 (전선 위에 UL/CSA 가 표시) 들의 사용을 금지합니다.

Waarschuwing

Bij het installeren van het product, gebruik de meegeleverde of aangewezen kabels, stroomkabels en adapters. Het gebruik van andere kabels en adapters kan leiden tot een storing of een brand. Elektrisch apparaat en veiligheidsinformatiebladen wet verbiedt het gebruik van UL of CSA gecertificeerde kabels die UL of CSA die op de code voor andere elektrische apparaten dan de producten die door Supermicro alleen.

Notes

Chapter 3

Installation and Setup

This chapter covers the setup of Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

3-1 Installation

To install Layer 2/3 Gigabit Ethernet switches use the procedure below.

Installing the Switch

1. Carefully unpack the switch from its shipping container and verify that all parts are present.
2. Install the 10-Gb/s add-on module(s) in the rear (SSE-G24-TG4 and SSE-G48-TG4 only).
3. Install the mounting ears onto the side of the switch using a screwdriver.
4. Mount the switch into your rack assembly (see Appendix A for optional rail mounting of the SSE-X24S/R, SSE-X3348S/R or SSE-X3348T/R).

3-2 Configuring the Switch Module

A Layer 2/3 1/10 and 10-Gigabit Ethernet Switch module can be configured using two methods. You may configure it:

- Through the web-based management utility
- Directly through a command line (using a telnet interface or a serial console)

The management utility accesses the switch module through any web browser. To access the switch directly, use the command line.

Any port may be configured as *up* (active) or *down* (inactive). All ports are active by default.

Web-based Management Utility

You can use the web-based management utility on a web browser to configure the switch module. You can access the configuration menu by a network connection.

Command Line

Configuring the switch can be done using a command line via telnet or by using the serial console interface.

Accessing CLI through Telnet

To access the command line via telnet, follow the below steps.

1. Connect a PC to a network that is accessible to the switch.

For example, connect a PC to any of the front panel ports of the switch and make sure the PC has an IP address on the same subnet as the switch management IP.

2. In the PC, start a telnet client session with the switch management IP (default IP is **192.168.100.102**).

This brings up the switch's command line interface for user login.

3. Enter the default username (**ADMIN**) and password (**ADMIN**) to login to the switch.
4. To view the switch configurations use **show commands** and to configure the switch type **config term** to get access to the configuration commands. For help type **?** or **help**.

Accessing CLI through a Serial Console

To access the command line via a serial console, follow the steps below.

1. Connect a PC serial port to the switch console port.
2. In the PC, open any serial port access applications, such as Hyperterminal or Term Term.
3. Choose the serial port connected with the switch and configure with the following parameters:

Baudrate = 9600

Data bits = 8

Parity = None

Stop bit = 1

4. This brings up the switch's command line interface for user login.
5. Enter username and password to login to the switch.
6. To view the switch configurations use **show commands** and to configure the switch type **config term** to get access to the configuration commands. For help type **?** or **help**.

For further information on the use of the command line interface, see the separate *CLI User's Guide* manual on your enclosed CD-ROM.

Firmware

The firmware for Layer 2/3 1/10 and 10-Gigabit Ethernet switches resides on a chip on the PCB.

The switch has internal flash memory in two areas to hold two firmware images. The flash area used for the normal firmware image is referred to as the *normal* area. The other flash area, referred to as the *fallback* area, is used to store the firmware image for fallback purpose in case of a failure to boot from the normal area.

Firmware Upgrading Procedures

The procedures for firmware upgrading and using a fallback firmware image are listed below.

Upgrading Firmware on the Switch using TFTP or the Network

To upgrade the switch's firmware, use the procedure below.

1. Designate a server or the network as an FTP server.
2. Copy the latest firmware to the TFTP root directory on the TFTP server machine.
3. Make sure the upgraded TFTP server and switch both have network reachability.
4. Login to the Switch CLI, either through Telnet or a serial console port.
5. Type the command below to upgrade the firmware in the normal area:

```
firmware upgrade tftp://<ip-address>/<filename>
flash:normal
```

Here *<ip-address>* is the IP address of the TFTP server and *<filename>* is the name of the firmware image file.

6. On successful download, the CLI displays the following string:

```
Firmware download completed successfully.
```
7. After a successful download, reboot the switch to use this latest firmware.
8. If the download fails, check the IP address, file name, network connections and configurations to reach the TFTP server.
9. If the switch does not come up after the firmware upgrade due to any incorrect firmware images, boot the switch using a fallback firmware image. Refer to the procedure "[Booting using a Fallback Firmware Image](#)" below to boot the switch using a fallback firmware image.
10. Once the switch is booted with a fallback firmware, repeat the above steps to upgrade with the correct firmware image.
11. On successful upgrade to the latest firmware, it is advised that you upgrade the fallback firmware image also. Follow the steps listed in the procedure "[Upgrading Fallback Firmware using TFTP](#)" below to upgrade the fallback firmware image.

Booting using a Fallback Firmware Image

Use the procedure below to boot using a fallback firmware image.

1. Reboot the switch by power cycling the switch power.
2. During reboot, press any key when it displays the below text (as shown in [Figure 3-1](#)).

Hit any key to stop autoboot: 5

Figure 3-1. Displayed Text for Rebooting

```
Decompressing...OK

Image Running Clock = 1
Image Running Clock = 21
system memory informations :
pool size : 25MB
free size : 21MB

PRODUCT TYPE : 24 GE Ports + 4 GE Combo Ports L2 Managed PoE Switch
Hit any key to stop autoboot: 5

ERROR: PCI configuration read(0x0=0xffffffff) -READ ERROR
ERROR: PCI configuration read(0x0=0xffffffff) -READ ERROR
PCI unit 0: Dev0xb313, Rev 0x01, Chip BCM56313_A0, Driver BCM56314_A0
SOC unit 0 attached to PCI device BCM56313_A0
Test chip 0.....OK

<<< USER MENU >>>

> SYSTEM INFO:
Hardware Version      : B1-01
-----
IP Address           : 192.168.2.32
Subnet Mask          : 255.255.255.0
Default Gateway      : 192.168.2.100
TFTP Server          : 192.168.2.100
Firmware File Name   : SBM-GEM-X2C-v5.2.10.bin

> MENU OPTIONS:
Press [H] to Set Hardware Info
Press [G] to Get Hardware Info
Press [F] to Download Firmware
Press [J] to Jump to Firmware

SMC>
```

3. Once the boot sequence is interrupted, it will display menu options as shown in [Figure 3-1](#).

Use the "H" option to set hardware information by typing the character **H**. This will display the hardware information that can be changed as shown in [Figure 3-2](#).

Figure 3-2. Setting Hardware Information

```
SMC>H

> HARDWARE INFO:
Local IP (ip) = 192.168.2.32
Subnet Mask (mask) = 255.255.255.0
Default Gateway (gateway) = 192.168.2.100
TFTP Server (tftpaddr) = 192.168.2.100
Firmware Name (randiskname) = SBM-GEM-32C-v5.2.10.bin
Randisk Flag (rflag) = 0

SMC.POSC> rflag=1

> HARDWARE INFO:
Local IP (ip) = 192.168.2.32
Subnet Mask (mask) = 255.255.255.0
Default Gateway (gateway) = 192.168.2.100
TFTP Server (tftpaddr) = 192.168.2.100
Firmware Name (randiskname) = SBM-GEM-32C-v5.2.10.bin
Randisk Flag (rflag) = 1

SMC.POSC> exit

Save before Exit ? [Y/N] y

Saving Hardware Info ... OK

> HARDWARE INFO:
Local IP (ip) = 192.168.2.32
Subnet Mask (mask) = 255.255.255.0
Default Gateway (gateway) = 192.168.2.100
TFTP Server (tftpaddr) = 192.168.2.100
Firmware Name (randiskname) = SBM-GEM-32C-v5.2.10.bin
Randisk Flag (rflag) = 1
```

4. To choose the boot from a fallback image, type the command: `rflag=1`
5. Type `Save` to save the hardware information.
6. Type `Exit` to exit the hardware information menu.
7. Type **J** to boot the image. In this case it will boot from a fall back image.
8. In case you wish to later move back to a normal image, repeat the above the steps with one difference for [step 4](#), where you should use the command `rflag=0` instead of `rflag=1` to boot with a normal firmware image.

Upgrading Fallback Firmware using TFTP

To upgrade the fallback firmware using TFTP, use the procedure below:

1. Copy the latest firmware to the TFTP root directory on the TFTP server machine.
2. Make sure the upgraded TFTP server and switch both have network reach ability.

3. Login to the Switch CLI either through Telnet or a serial console port.
4. Type the below command to upgrade the firmware in the normal area:

```
firmware upgrade tftp://<ip-address>/<filename> flash:fallback
```

Here *<ip-address>* is the IP address of the TFTP server and *<filename>* is the name of the firmware image file.
5. On a successful download, the CLI displays the following string:

```
Firmware download completed successfully.
```
6. After a successful download, reboot the switch using the fallback image to verify the fallback image. Refer to the steps listed above in the procedure ["Booting using a Fallback Firmware Image"](#) to boot the switch in the fallback image.
7. Once both the normal and fallback image both have latest firmware, continue to use the normal image as directed in [step 8](#) of the procedure ["Booting using a Fallback Firmware Image"](#).

Firmware Failure Recovery Steps

In case you have any issues in booting the switch with either a normal or fallback image, use the procedure below to recover the switch functionality with a correctly working firmware image.

Recovering Switch Functionality with a Firmware Image

1. Copy the latest firmware to the TFTP root directory on a TFTP server machine.
2. Make sure the upgraded TFTP server and switch both have network reachability.
3. Reboot the switch by power cycling the switch power.
4. During reboot, press any key when it displays the below text (as shown in [Figure 3-1](#)).

```
Hit any key to stop autoboot: 5
```
5. Once the boot sequence is interrupted, it will display menu options as shown in [Figure 3-1](#). Use the "H" option to set hardware information by typing the character **H**. This will display the hardware information that can be changed as shown in [Figure 3-2](#).
6. Configure the IP address for this switch (only for booting purposes) using the command: `ip=<IP address>`
For example **ip=192.168.2.3**
7. Configure the subnet mask for this switch IP address using the following command:
`mask=<subnet mask>`
For example **mask=255.255.255.0**
8. Configure the TFTP server IP address using the following command:
`tftpaddr=<TFTP server IP>`

For example **tftpaddr=192.168.2.100**

9. Configure the gateway address to reach the TFTP server using the following command if the TFTP server is in a different network:

```
gateway=<gateway IP>
```

For example **gateway=192.168.2.100**

10. Configure the firmware image file name using the following command:

```
ramdiskname=<filename>
```

For example **ramdiskname= SBM-GEM-X2C-v5.2.10.bin**

11. Type *Save* to save the hardware information.
12. Type *Exit* to exit the hardware information menu.
13. Type **F** to download the firmware image. In this case it will download to the normal image area.
14. On a successful download, the switch displays the below string.

```
Updating the ramdisk image ...  
This may take awhile  
OK
```

15. After a successful download, boot the switch to use this latest firmware by typing **J**.
16. If the download fails, check the IP address, file name, network connections and configurations to reach the TFTP server.

Notes

Chapter 4

Ports and Indicators

This chapter covers the ports and LED indicators found on Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

4-1 SSE-G24-TG4 Ports and Indicators

Figure 4-1. SSE-G24-TG4 Ports and Indicators

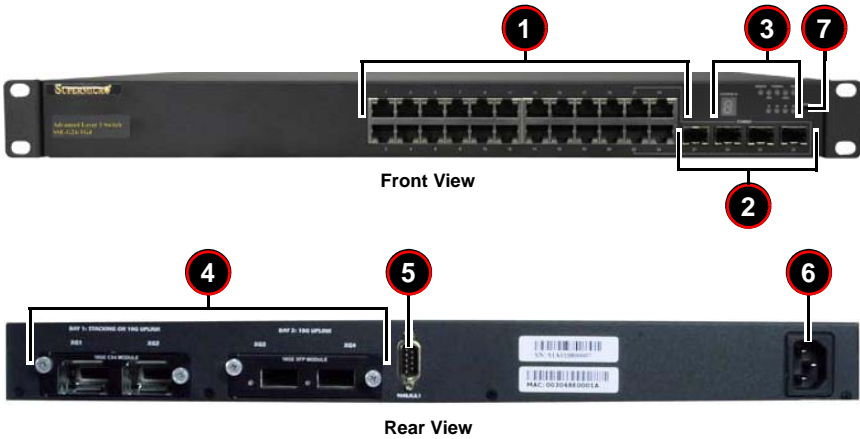


Table 4-1. SSE-G24-TG4 Switch Module Ports and Indicators

Item	Description
1	RJ45 10/100/1000 Ethernet ports (24)
2	SFP Combo Ports (4)
3	LEDs and Stacking Indicator ID
4	10-Gb/s Port Module Bays (2 bays for up to 4 ports for CX-4, XFP or SFP+)
5	Serial Port
6	Power Port
7	Reset

4-2 SSE-G48-TG4 Ports and Indicators

Figure 4-2. SSE-G48-TG4 Ports and Indicators

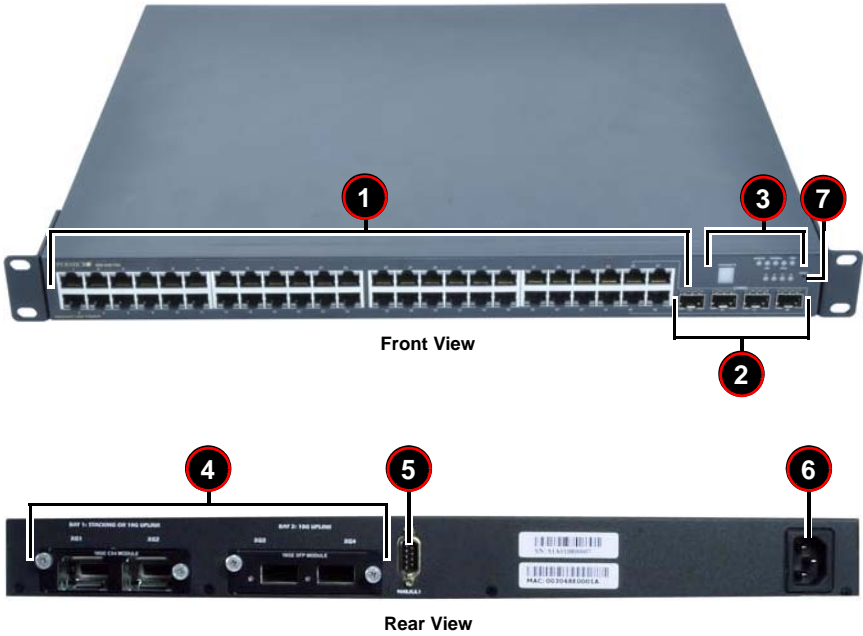


Table 4-2. SSE-G24-TG4 Switch Module Ports and Indicators

Item	Description
1	RJ45 10/100/1000 Ethernet ports (48)
2	SFP Combo Ports (4)
3	LEDs and Stacking Indicator ID
4	10-Gb/s Port Module Bays (2 bays for up to 4 ports for CX-4 or XFP)
5	Serial Port
6	Power Port
7	Reset

4-3 SSE-X24S/R Ports and Indicators

Figure 4-3. SSE-X24S/R Ports and Indicators

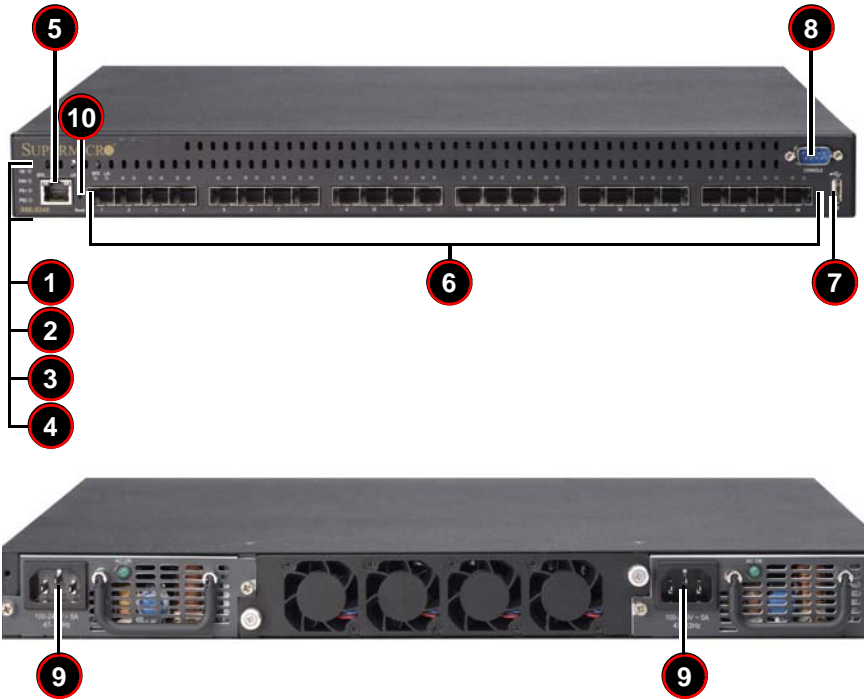


Table 4-3. SSE-X24S/R Switch Module Ports and Indicators

Item	Description
1	System Status Indicator
2	Fan Status Indicator
3	Status Indicator – Power Supply 1
4	Status Indicator – Power Supply 2
5	1-Gbps port (Line or console)
6	10-Gbps Ethernet Ports – SFP+ connectors
7	USB Port
8	Serial Console Port
9	Power Ports
10	Reset

4-4 SSE-X3348S/R Ports and Indicators

Figure 4-4. SSE-X3348S/R Ports and Indicators

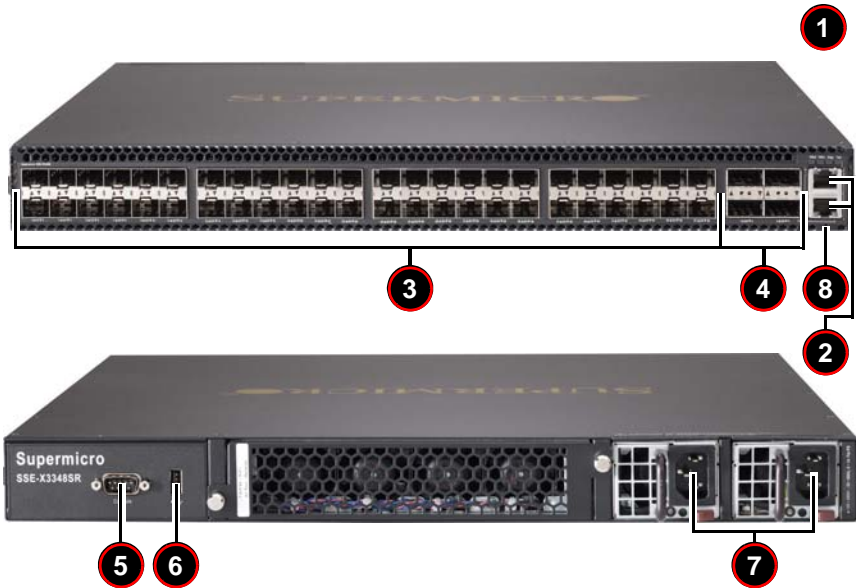


Table 4-4. SSE-X3348S/R Switch Module Ports and Indicators

Item	Description
1	Status indicators for: System, Fan, Power Supply 1 and Power Supply 2
2	1-Gbps ports (Line or console)
3	10-Gbps Ethernet Ports - SFP+ connectors
4	40-Gbps Ethernet ports – QSFP connectors
5	Serial Console Port
6	USB Port
7	Power Port
8	Reset

4-5 SSE-X3348T/R Ports and Indicators

Figure 4-5. SSE-X3348T/R Ports and Indicators

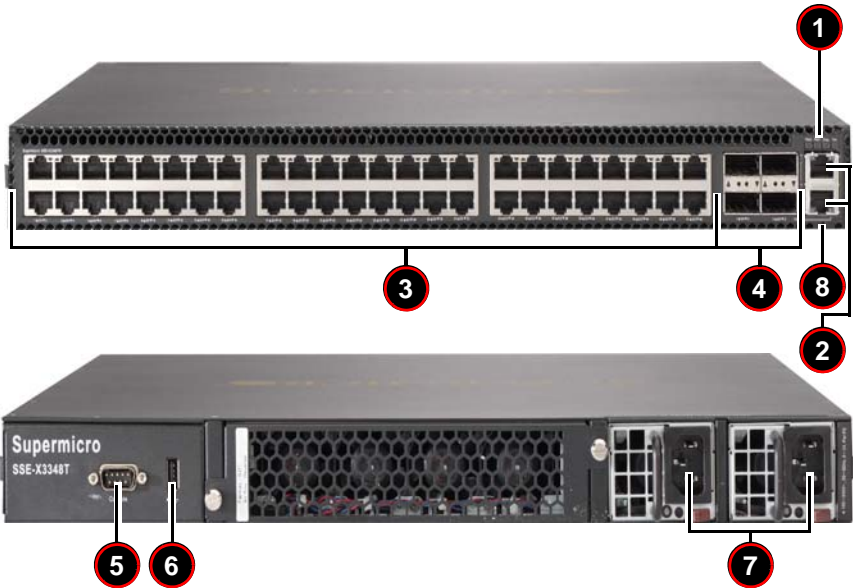


Table 4-5. SSE-X3348T/R Switch Module Ports and Indicators

Item	Description
1	Status indicators for: System, Fan, Power Supply 1 and Power Supply 2
2	1-Gbps ports (Line or console)
3	10-Gbps Ethernet Ports - RJ45 connectors
4	40-Gbps Ethernet ports – QSFP connectors
5	Serial Console Port
6	USB Port
7	Power Port
8	Reset

4-6 Ports

Both Layer 2/3 1/10-Gigabit Ethernet switches contain several front mounted ports in common.

RJ45 Compatible Port

These 24 (SSE-G24-TG4) or 48 (SSE-G48-TG4) 1-Gb/s duplex ports each accept an RJ45 compatible cable.

Combo Ports

Each of the four SFP 1-Gb/s combo ports can hold a module for a downlinking fiber connector. This can be used instead of the RJ45 connector for only these four ports.

Note that using an SFP port precludes the use of the RJ45 port with the same port number.

10-Gb/s Port Module Bays

Figure 4-6. 10-Gb/s Port Module Bays



AOM-SSE-X2C



AOM-SSE-X2F



AOM-SSE-X2S

The Layer 2/3 1/10-Gigabit Ethernet switches contain two bays in the rear that each house a 2-port 10-Gigabit interface module containing either CX-4, XFP or SFP+ ports, depending upon your chosen configuration (see [Figure 4-6](#)). Bay 1 can be used for Stacking or 10-Gb/s uplink. Bay 2 can also be used for stacking, but it normally is used to house a module for links to one or two external 10-Gb/s switches.

Current modules available are:

- **AOM-SSE-X2C** module with two CX4 copper interface ports for connections up to 12 meters in distance.

NOTE: You must use a Supermicro CX4 cable if you are using one or more of these ports for stacking. You may use the Supermicro CBL-0474L for 1M connections or the CBL-0389L-01 for 3M connections.

- **AOM-SSE-X2F** module with two XFP interface ports for accepting XFP transceivers allowing fiber connections up to 300 meters in distance.
- **AOM-SSE-X2S** module with two SFP+ interface ports for accepting SFP+ copper cables or SFP+ transceivers allowing fiber connections up to 300 meters in distance.

Serial Ports

One serial port is available for communications to an external control console.

Power Port

This port is for connecting the power cable for powering the Layer 2/3 1/10-Gigabit Ethernet switches.

4-7 Indicators

This section covers LED indicators for the Layer 2/3 1/10-Gigabit Ethernet switches. These LEDs are listed and described in [Table 4-6](#).

Table 4-6. SSE-G24-TG4 and SSE-G48-TG4 LED Indicators

LED Name	Description
Master	Indicates this is the master switch in a stacked configuration.
Fan	Indicates fan status.
Thermal	Indicates Thermal status.
Diagnostic	Indicates diagnostic activity.
Power	Indicates power for the system.
Combo LEDs ^a	Indicates activity for the Combo fiber port that corresponds to the number indicated.

a. 21-24 for SSE-G24-TG4 and 45-48 for the SSE-G48-TG4

Notes

Chapter 5

Web Based Management Utility

This chapter is provided to help you quickly get started in using the web-based management utility for all 1/10-Gigabit and 10-Gigabit Layer 2/3 Ethernet switches.

The utility starts with a default IP address, which is also the management IP address. This IP address is essentially provided for remote management of this switch. For managing the switch through web browsers, type in the default IP address in your browser's web address in order to start accessing the switch.

For example, if the management IP address of the switch is **192.168.100.102**, the switch can be accessed through the Web browser by typing <http://192.168.100.102> in the address space of the web browser.

After entering in the IP address, the switch's LOGIN page ([Figure 5-1](#)) should appear.

Nomenclature

The following nomenclature applies to screens found in this chapter:

- **Port */*** – This indicates the stacking ID number, port number
- **Port Number GB */*** – This is for an internal port
- **Port Number Ext */*** – This is for an external port.

5-1 Overview

The Supermicro switch utility for Layer 2/3 1/10 and 10-Gigabit Ethernet switches provides a web-based interface for managing Layer 2 and Layer 3 switching at wire speed for constructing a switched/routed network. This interface provides both a bridging functionality and advanced features such as link aggregation, Dynamic VLAN/Dynamic Multicast, IGMP Snooping and Network Access Control. This web-based interface also comes with several Layer3 features as well (such as wire speed routing, Differentiated Services, multicast routing and so on).

The Supermicro Switch firmware is implemented using open sources from OpenSSL, OpenSSH and other open source communities and is configured using web browsers such as Internet Explorer.

The utility starts with a default IP address, which is also the management IP address. This IP address is essentially provided for remote management of this switch. For managing the switch through web browsers, type in the default IP address in your browser's web address in order 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 typing <http://192.168.1.1> in the address space of the web browser.

The default management IP address for Supermicro Switch products is **192.168.100.102**. This default IP address can be changed in the SYSTEM SETTINGS page in the System Management section.

For the SSE-G48-TG4 and SSE-G24-TG4 switches you can connect to any of the front panel 1G ports or back panel 10G ports to manage the switch with the default management IP. These switches will create VLAN 1 by default with this IP address, including all 1G and 10G ports.

For the SSE-X24S/R, SSE-X3348S/R or SSE-X3348T/R switches you can connect to the 1G Ethernet RJ45 port, one of the 10G Ethernet ports, or one of the 40G Ethernet ports (if so equipped); or the serial console port (on the front of the unit) to manage the switch.

These switches will create VLAN 1 by default with this IP address - including all Ethernet ports.

Note: Blade Switches can be managed with the default IP through the CMM Ethernet connections. The internal management Ethernet ports of Blade Switches are connected with the CMM Ethernet ports internally. If managing the Blade Switch through front panel ports or any other switching ports is preferred, then the user can assign the desired management IP address to VLAN 1. Alternatively users can create any VLAN and manage the switch through switching ports. [Here the term switching ports refers to all internal and external 1G and 10G ports of the switch.]

5-2 Login

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

Figure 5-1. Login Page



The initial login page (Figure 5-1) is used to login to the Supermicro Switch web-based management utility for 10 Gb/s switches. To login, enter your **User Name** and **Password** in the fields provided and press the LOGIN button.

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

After logging in, you will be taken to the HOME page of the utility. See [Section 5-3](#) for further details.

5-3 Home Page

The HOME page ([Figure 5-2](#)) contains links and menus for going to all other control pages in the Supermicro Switch web-based interface utility. A list of controls for this page is shown in [Table 5-1](#). The basic page structure of the HOME page is duplicated for all subsequent sub-pages of the Supermicro Switch web-based interface utility.

NOTE: The SSE-G24-TG4, SSE-G48-TG4, SSE-X24S/R, SSE-X3348S/R and SSE-X3348T/R switches from Supermicro share a common management interface (including the associated feature set) with Supermicro's SBM-GEM-X2C and SBM-GEM-X3S+ Layer 2/3 1/10G Ethernet switches for the Supermicro Blade System.

In this manual you will see many screen shots of pages showing the name of the SBM-GEM-X2C in the upper left hand corner. With the exception of this name, these screens will all have the same structure and appearance in your SSE-G24-TG4, SSE-G48-TG4, SSE-X24S/R, SSE-X3348S/R and SSE-X3348T/R switch.

Figure 5-2. Home Page

The screenshot shows the Supermicro Switch Home Page. The browser address bar displays the URL: `172.31.8.23/~/ipoc/f/homepage.html?Gambitab:d3db353:ibeenejpoek:ibeenejpoek`. The page title is "SUPERMICRO". The navigation menu on the left includes: Home, System Mgmt, Layer2 Mgmt, Layer3 Mgmt, Multicast, and Statistics. The main content area is titled "Supermicro Switch" and contains a grid of management and statistics links. The grid is organized as follows:

System Mgmt	Layer2 Mgmt	Layer3 Mgmt	Multicast
System Settings Management IE File Management Firmware Upgrade Management Security	Layer2 Basic Settings EoM Manager VLAN Dynamic VLAN	IP IP Set EoMCT Server EoMCT Policy	IGMP Snooping IGMP Querier IGMP EoM IGMP
Routing ACL Web Settings SNMP RMON	Dynamic VLAN RSTP MSTP LA	BPDU EoM EoM EoM EoM	IGMP Snooping IGMP Querier IGMP EoM IGMP
System Statistics	Layer2 Statistics	Layer3 Statistics	Multicast Statistics
Interface Radius TACACS+ Server RMON SNMP AGENT SNMP AGENTX	VLAN RSTP MSTP LA BPDU	IP IP Set EoM EoM EoM EoM EoM	IGMP Snooping IGMP Querier IGMP EoM IGMP

At the bottom of the page, there is a copyright notice: "Copyright © Super Micro Computer, Inc. This page is best viewed with 1024x768 resolution."

Table 5-1. Home Page Controls and Components

Number	Name	Description
1	Top Page Links	The Top Page Links are present both on the Home page and all other pages accessed and contain links to support pages or additional controls for all pages viewed with the Web Management Utility. See "Top Page Links" below for further details.
2	Top LED Display	This section of the screen provides an overview port status for the switch. See "Top Page Links" for further details.
3	Left Side Tree	The Left Side Tree contains an expandable list of links for you to use to get to other management pages. All configuration pages contain this navigation tree.
4	Middle Configuration Links Table	Each configuration page contains its own links and controls

The HOME page is displayed on successful validation of the user name and password. The information in this page presents a brief overview of the switch web-based management utility. See [Figure 5-3](#), [Figure 5-4](#) and [Figure 5-5](#) for different views of the Home page for each of Supermicro's 10-Gb/s switches.

Figure 5-3. SSE-G24-TG4 Home Page

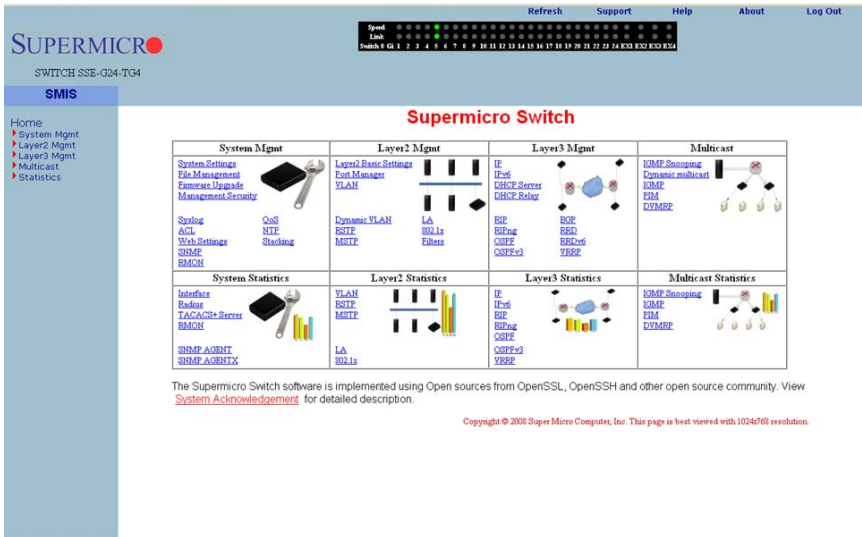


Figure 5-6. SSE-X3348S/R Home Page

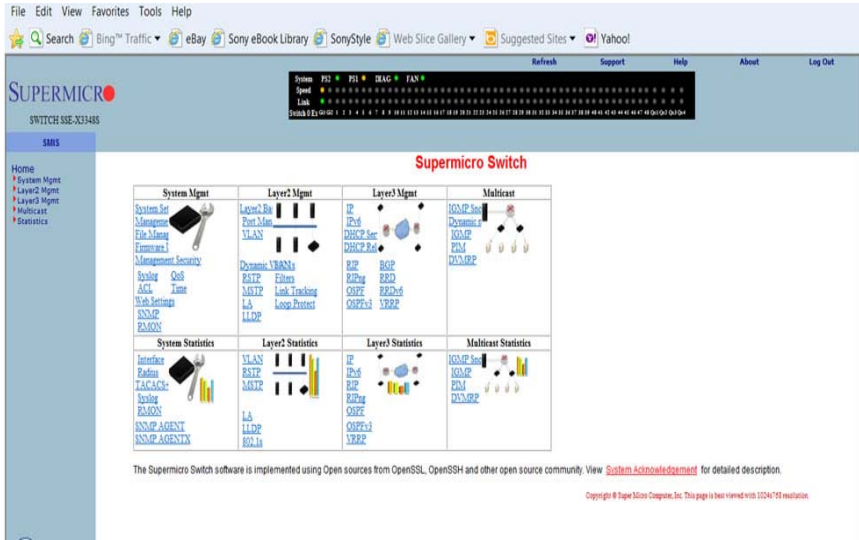
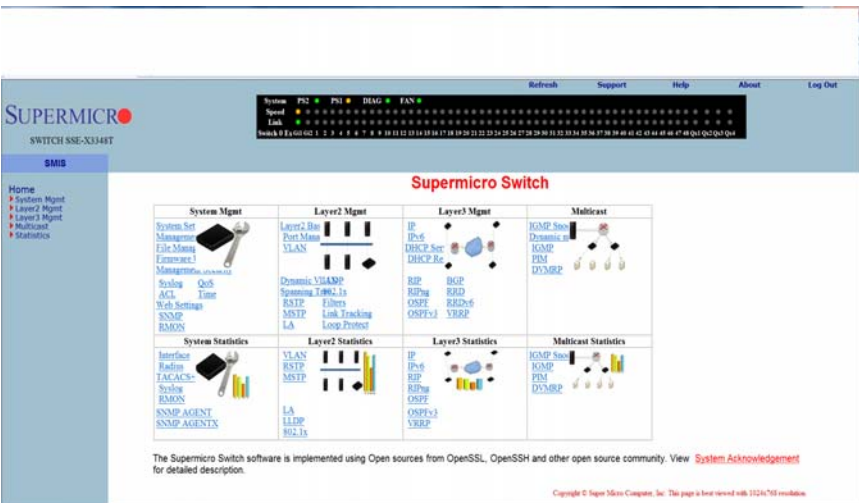


Figure 6. SSE-X3348T/R Home Page



Top Page Links

On the top of all pages of the web-based management utility you can find the following PAGE HEADER links:

- **Refresh** – Click this link to refresh the contents of the page. Unlike the browser refresh button, this link refreshes only the contents of the middle of the page which has the active data.
- **Support** – Click this link to get technical support for Supermicro Products.
- **Help** – Click on this link to open a context specific help page that covers all the items on the page being viewed.
- **About** – Click this link to get additional information about the web-based management utility, the switch and also the versions supported.
- **Log Out** – Click this link to log out of the web session and go back to the Login page.

Top LED Display

This part of the screen displays the **Port Status**, **Speed** and **Link Status** for every port of the switch.

Since the number of ports is different in various switches, this display shows a different number of ports for each when the Web Management Utility is run:

- For the SSE-G24-TG4 switch, it displays twenty-four 1-Gigabit Ethernet (Gi) ports and four 10-Gigabit Ethernet (Ex-Extreme Ethernet) ports.
- For the SSE-G48-TG4 switch, it displays forty-eight Gi ports and four Ex ports.
- For the SSE-X24S/R switches, it displays twenty-four 10-Gigabit ports.
- For the SSE-X3348S/R switches, it displays forty-eight 10-Gigabit ports and four 40-Gigabit ports
- For the SSE-X3348T/R switches, it displays forty-eight 10-Gigabit ports and four 40-Gigabit ports

NOTE: Ex ports configured as stacking ports will not be displayed.

In stacking, the **Switch Identifier** will be displayed on top of this LED display. This allows you to select a stack member switch of interest, and to view the LED display for the corresponding switch.

NOTE: Stacking is not supported on the SSE-X24S/R, SSE-X3348T/R, or SSE-X3348S/R switches.

For **Link**, a green light corresponding to a number indicates that that numbered port is up, whereas a red light corresponding to a number indicates that this port is down.

Left Side Tree

The tree display on the left side of the page provides quick access to the configuration pages. This tree is organized based on the features supported in the switch. The main features are categorized in the following groups.

- System Management - System based configurations
- Layer 2 Management - Layer 2 Protocols including VLAN, RSTP, MSTP, ...
- Layer 3 Management - Layer 3 Protocols including - IP, RIP, OSPF,
- Multicast Management - Multicast Protocols including IGMP, PIM, ...
- Statistics - Statistics and Counters for all the features.

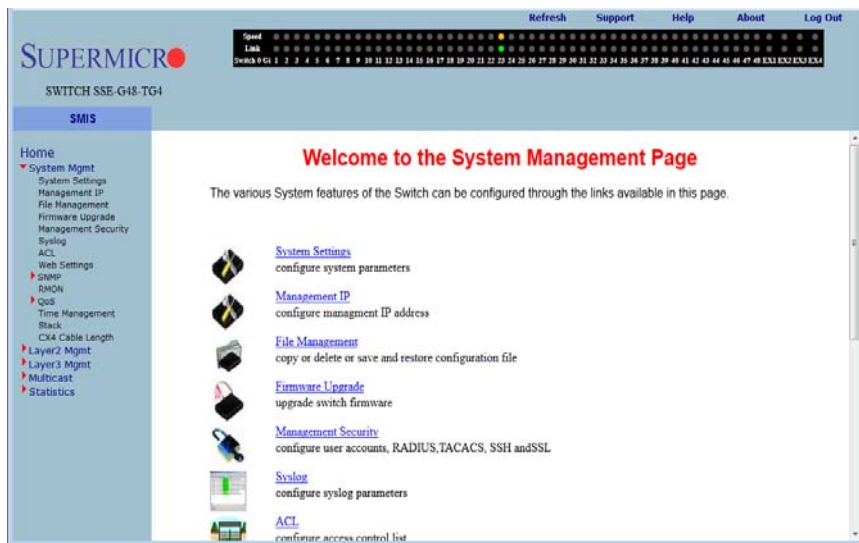
This tree is displayed on the left navigation pane on all configuration pages. This makes it easier for you to choose any configuration page directly without going back to the home page every time. To go to one of a MANAGEMENT page's sub-pages, click on the ► symbol to expand the list.

Middle Configuration Link Table

This section of the page displays a table of links to all major configurations. This table provides links similar to the Left Side Tree links. The configuration links are categorized based on features of the switch.

5-4 System Management Page

Figure 5-1. System Management Page



The SYSTEM MANAGEMENT page (Figure 5-1) contains the following links:

- [System Settings](#)
- [Management IP](#)
- [File Management](#)
- [Firmware Upgrade](#)
- [Management Security](#)
- [Syslog](#)
- [ACL](#)
- [WEB Settings](#)
- [SNMP](#)
- [RMON](#)
- [QoS](#)
- [Time Management](#)
- [Stack](#)
- [CX4 Cable Length](#)

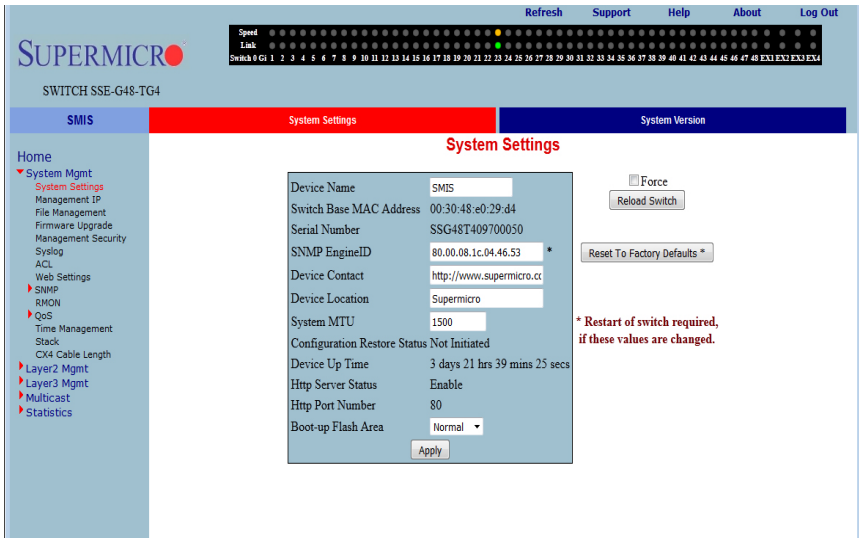
System Settings

The following pages can be accessed through the System Settings link:

- [System Settings](#)
- [System Version](#)

System Settings

Figure 5-2. System Settings Page



Clicking the SYSTEM INFORMATION tab brings up the SYSTEM SETTINGS page (Figure 5-2). This page provides system related information and also helps you configure system specific parameters. Table 5-2 lists the parameters found on this page.

Table 5-2. System Information Page Parameters

Parameter	Description
Device Name	Assigns a name to identify this device – 15 Characters input limit. The factory default is SMIS .
Switch Base MAC Address	This displays the MAC Address of the switch.
Serial Number	This displays the serial number of the switch.
SNMP Engine ID	Sets the SNMP engine ID with 5 to 32 hexadecimal characters separated by dots for the local or remote SNMP engine. A restart of the switch required if these values are changed. The factory default is 80.00.08.1c.04.46.53
Device Contact	Assigns a contact person's name with a 255-character input limit. The factory default is http://www.supermicro.com/support .

Table 5-2. System Information Page Parameters (Continued)

Parameter	Description
Device Location	This specifies the location of this switch using a 255-characters input limit. The factory default is Supermicro .
System MTU	This specifies the maximum transmission unit (MTU) size of IP packets sent on an interface. The valid range is between 1500 and 9210, while the default value is 1500 .
PIM Mode	PIM (Protocol Independent Multicast) is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. SPARSE MODE uses shared trees to forward multicast datagrams to a set of specific directly connected designated router(s). DENSE MODE uses multicast sources to send multicast data packets to all attached routers. The factory default mode is Sparse .
Snoop Forward Mode	This sets the multicast flows of multicast data so they can be forwarded based on IP addresses or MAC addresses. The factory default mode is MAC addresses .
Configuration Restore Status	This shows the status of the configuration restore process, and whether it is successful or a failure. If the configuration is not saved, the Restore Status will show Not Initiated .
Device Up Time	This shows the time from which the device is UP.
HTTP Server Status	This shows the HTTP (Hypertext Transfer Protocol) server status.
HTTP Port Number	This shows the HTTP (Hypertext Transfer Protocol) Port number.
Boot-up Flash Area	For this parameter, the chosen system RAM disk boots from <i>Normal</i> (primary boot up image) or <i>Fallback</i> (secondary boot up image). The factory default is Normal .

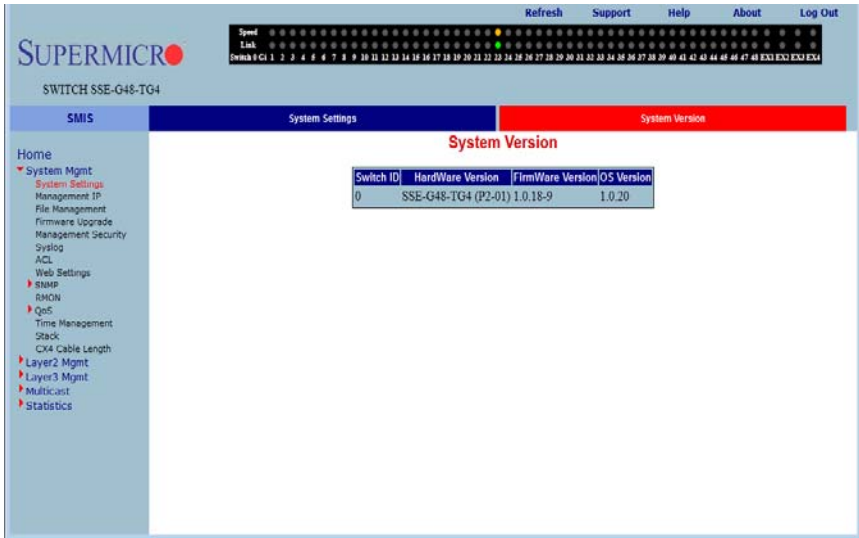
This page also has a control to **Reset To Factory Defaults**. This clears all switch configuration and local user accounts information. This reset requires reboot of the switch.

WARNING: Make sure to have all necessary configurations backed up before doing *Reset To Factory Defaults*.

This page also provides a control to *Reboot* the switch. In stacking, the Switch Identifier is displayed on top of this reboot button. You can select the interested stack member switch to reboot the corresponding switch. You can also select the ALL option to reboot all stack members.

System Version

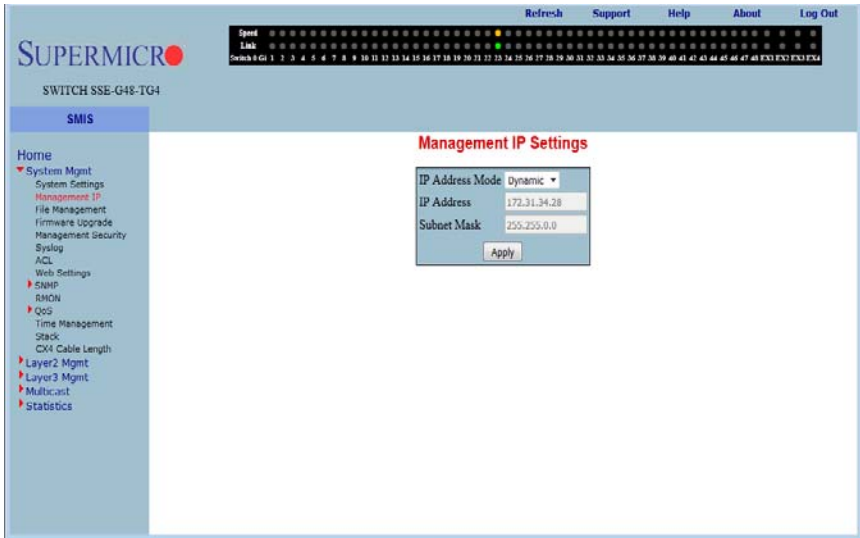
Figure 5-3. System Version Page



Clicking the SYSTEM VERSION tab brings up the SYSTEM VERSION page (Figure 5-3). This page provides a table that displays system version information including the *Switch ID*, *Hardware Version* and *Firmware Version* for each switch.

Management IP

Figure 5-4. Management IP Page



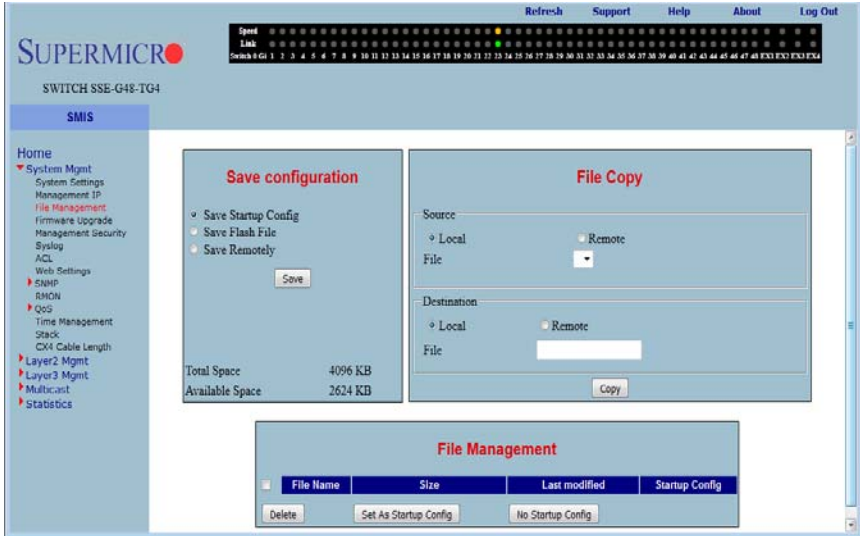
Clicking the MANAGEMENT IP tab brings up the MANAGEMENT IP page (Figure 5-4). This page helps you to manage the IP address for the switch. This page allows configuration of the following settings:

- **IP Address Mode** — This can be either manual or dynamic. If the manual mode is selected, then the management interface takes the configured IP address as the Default IP Address.
- **IP Address** — Configures the management IP address. This is configurable only if the IP Address Mode is manual.
- **Subnet Mask** — Configures the management IP subnet mask. This is configurable only if the IP Address Mode is manual.
- **Default Mgmt Gateway** — Configures the default gateway IP address in blade switches. In TOR switches, gateway IP configuration is not supported; instead the gateway IP address can be specified using the “ip route” configuration.

You can set the switch to DYNAMIC MODE or MANUAL MODE. If you set the switch to DYNAMIC MODE, then it will automatically obtain the IP Address and subset mask from the DHCP Server. If you set the switch to MANUAL MODE, then you can set the IP Address and subnet mask to whatever setting are appropriate to your network. The switch is set to **192.168.100.102** for IP Address and **255.255.255.0** for the Subnet Mask by default.

File Management

Figure 5-5. File Management Page



Clicking the FILE MANAGEMENT link brings up the FILE MANAGEMENT page (Figure 5-5). The FILE MANAGEMENT page helps you to manage the configuration files in the switch. This page provides three main features.

- [Save Configuration](#)
- [File Copy](#)
- [File Management](#)

Save Configuration

You can save a currently running switch configuration in the following three ways:

- **Save Startup Config** - This option saves the currently running configuration in a local flash file with the file name configured as a "startup configuration" file.
- **Save Flash File** - This option saves the currently running configuration in a local flash file with a user specified file name.
- **Save Remotely** - This option saves the currently running configuration into a remote TFTP server. You need to provide the IP address and file name of the TFTP server for this option.

The total configuration memory space and available free space are also displayed for your reference.

File Copy

You can copy a local file to or from a remote TFTP server. This feature is useful to create a backup of configuration files remotely, and also to download configuration files from remote computers to the switch. You need to provide a local file name and also the remote TFTP server's IP address and file name for this feature.

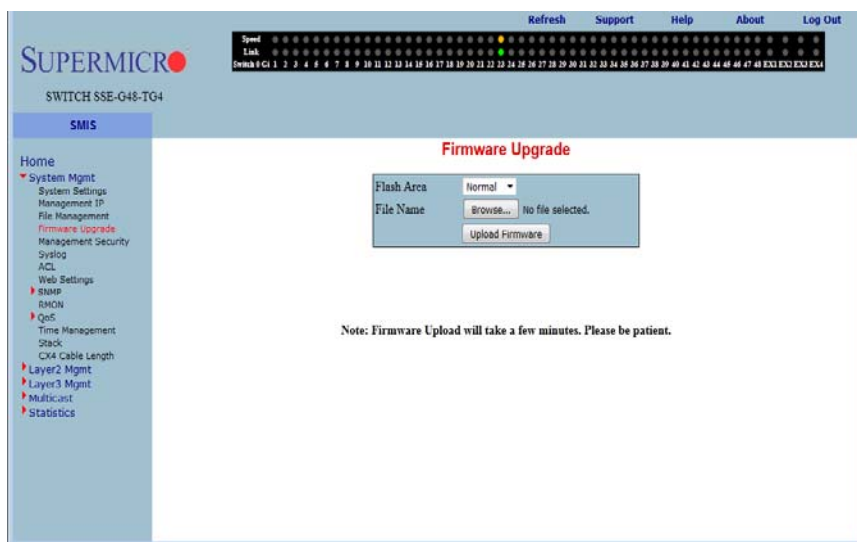
File Management

This section displays information about the configuration files stored in the switch and allows you to do any of the following actions:

- You can select one or more files and delete them.
- You can choose a Startup Configuration file from this file list.
- You can choose the File option and enter a name for a Startup Configuration file. Alternatively you can choose the "File" option and enter the name for the "Startup Config" file.
- You can also choose the NO RESTORE option for not loading any configuration files on the next reboot of the switch.

Firmware Upgrade

Figure 5-6. Firmware Upgrade Page



Clicking the FIRMWARE UPGRADE link brings up the FIRMWARE UPGRADE page (Figure 5-6). This page allows you to upgrade the firmware in NORMAL or FALLBACK MEMORY. In stacking, the firmware is upgraded in all stack members automatically.

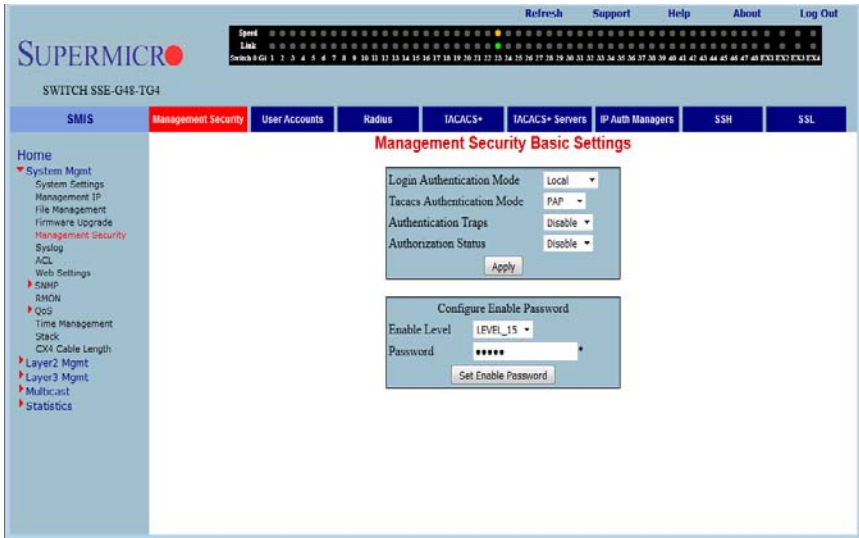
Management Security

The MANAGEMENT SECURITY link provides configuration for the following features:

- [Management Security](#)
- [User Accounts](#)
- [Radius](#)
- [TACACS+](#)
- [TACACS+ Servers](#)
- [IP Auth Manager](#)
- [SSH](#)
- [SSL](#)

Management Security

Figure 5-7. Management Security Basic Settings Page



Clicking the MANAGEMENT SECURITY tab brings up the MANAGEMENT SECURITY BASIC SETTINGS page (Figure 5-7). This page allows you to setup the below listed basic security parameters (Table 5-3).

Table 5-3. Management Security Basic Settings Page Parameters

Parameter	Description
Authentication mode	The authentication modes supported are LOCAL, RADIUS and TACACS. The default option is LOCAL mode where the user name and password is authenticated using a local user data base. In RADIUS mode, the authentication request is sent to the configured RADIUS servers. In TACACS mode, the authentication request is sent to the configured TACACS server.
Authentication traps	This parameter allows you to ENABLE or DISABLE SNMP Traps for SNMP access authentication events.
Authorization Status	When the login authentication mode is TACACS, a user can enable or disable authorization status.

Administrative users can also create *Enable Passwords* in this page. Low privilege users can use these *Enable Passwords* in the WEB SETTINGS page to enable access to privilege configurations.

Administrative users can set an *Enable Password* for all privilege levels. By default, the Enable Password is set only for the highest level (**Level_15**). This default password is the same as the default password set for the ADMIN user login.

User Accounts

Figure 5-8. Management User Account Configuration Page

The screenshot displays the 'Management User Account Configuration' page. At the top, there is a status bar with 'Speed' and 'Link' indicators. Below it, the 'SUPERMICR' logo and 'SWITCH SSE-G48-TG4' are visible. The navigation tabs include 'SMIS', 'Management Security', 'User Accounts' (selected), 'Radius', 'TACACS+', 'TACACS+ Servers', 'IP Auth Managers', 'SSH', and 'SSL'. The left sidebar lists various system management options like 'System Mgmt', 'System Settings', 'Management IP', 'File Management', 'Firmware Upgrade', 'Management Security', 'Syslog', 'ACL', 'Web Settings', 'SNMP', 'RMON', 'QoS', 'Time Management', 'Stack', 'CX4 Cable Length', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The main content area features a 'Current Active Users' table with columns for 'Session', 'User Name', and 'Peer Address', showing one active session for 'ADMIN' at '172.31.32.101'. Below this is a form to add a new user with fields for 'User Name' (ADMIN), 'Password' (masked), 'Privilege' (DEFAULT), and 'Admin user' (checkbox). There are 'Apply' and 'Reset' buttons. At the bottom, a table lists existing users with columns for 'Select', 'User Name', and 'Privilege', showing 'ADMIN (Admin user)' with privilege level 15 and 'stockuser' with privilege level 1. A 'Delete' button is located below the table.

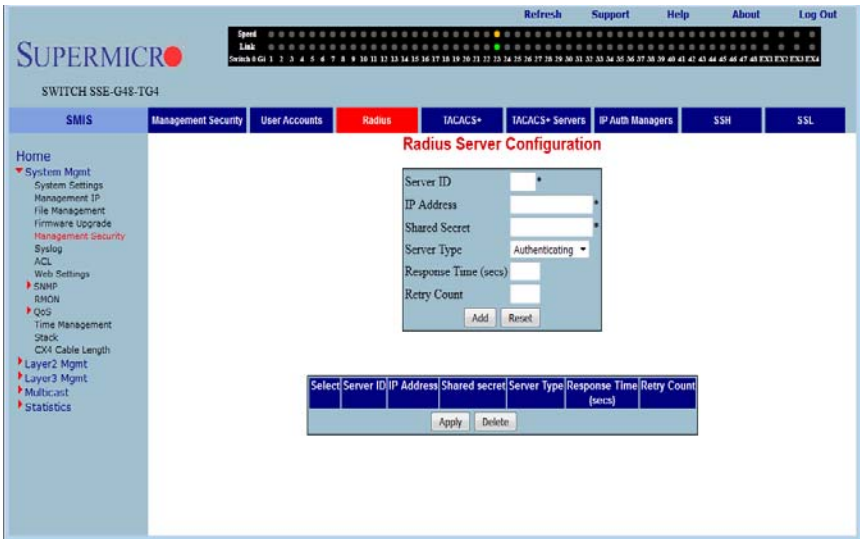
Clicking the LOCAL USERS tab brings up the MANAGEMENT USER ACCOUNT CONFIGURATION page (Figure 5-8). This page allows you to create or delete local user accounts. You need more than privilege *Level_5* to view all pages and need more than privilege *Level_10* for changing the configurations. The highest, *Level_15*, is for Administrator privilege.

Any one of the configured users can be specified as ADMIN user.

The current active users are displayed with session, user name and peer address details.

Radius

Figure 5-9. Radius Server Configuration Page



Clicking the RADIUS tab brings up the RADIUS SERVER CONFIGURATION page (Figure 5-9). This page allows you to configure the RADIUS server parameters as shown in Table 5-4.

Table 5-4. RADIUS Server Configuration Page Parameters

Parameter	Description
Server ID	This parameter specifies the unique identifier of the RADIUS Server Entry using a 2-characters input limit. The allowed value range is from 1 to 10. The factory default is blank.
IP Address	This parameter specifies the IP Address of the RADIUS Server. The factory default is blank.

Table 5-4. RADIUS Server Configuration Page Parameters

Parameter	Description
Shared Secret	This parameter specifies the secret string, which is shared between the RADIUS Server and the RADIUS Client. This field contains a 255-characters input limit, and the factory default is blank.
Server Type	This parameter specifies the RADIUS server type as either: <ul style="list-style-type: none"> • Authenticating (default): to authenticate users or devices before granting them access to a network • Accounting: to account for usage of those services • Both: Authenticating and Accounting
Response Time (secs)	This parameter specifies the maximum time within which the Radius Server has to respond for a request from the Radius Client. The valid range is 0 to 120 seconds. The factory default is blank.
Retry Count	This parameter specifies the maximum number of times a radius request is to be re-transmitted before getting a response from the Radius Server. The valid range is 1 to 254. The factory default is blank.

TACACS+

Figure 5-10. TACACS+ Global Settings Page

The screenshot displays the SUPERMICRO web management interface for a SWITCH SSE-G48-TG4. The top navigation bar includes links for Refresh, Support, Help, About, and Log Out. The main navigation menu has tabs for SMIS, Management Security, User Accounts, Radius, TACACS+, TACACS+ Servers, IP Auth Managers, SSH, and SSL. The TACACS+ tab is active, showing the 'TACACS+ Global Settings' page. On the left, a sidebar menu lists various system management options, with 'Management Security' expanded to show 'TACACS+'. The main content area contains a form with the following fields:

- Active Server IP Address: 0.0.0.0
- Re-Transmit: 2
- Apply button

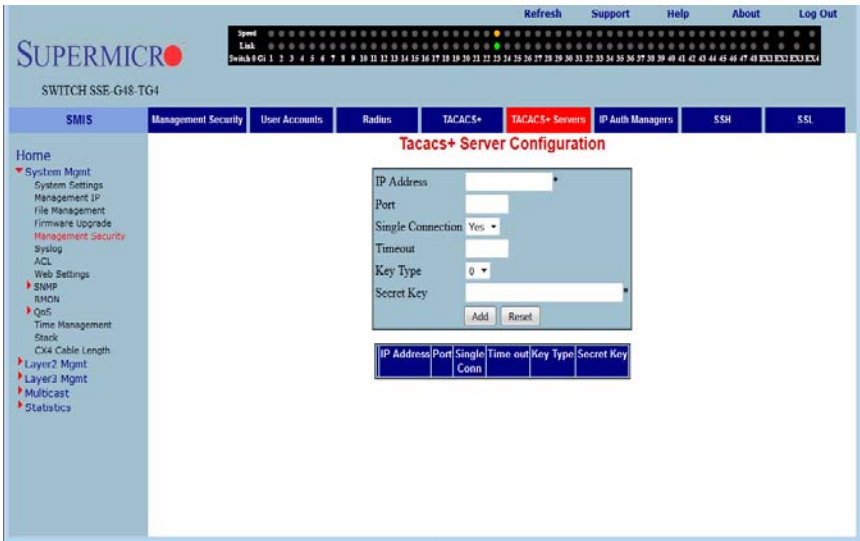
The TACACS+ GLOBAL SETTINGS page (Figure 5-10) allows you to configure TACACS+ retries and choose an active TACACS server. The parameters for this page are shown in Table 5-5.

Table 5-5. TACACS+ Global Settings Page Parameters

Parameter	Description
Active Server IP Address	Specifies the IP address of the active TACACS server. This server should have been already configured in the TACACS+ SERVER CONFIGURATION page (Figure 5-11). The factory default is 0.0.0.0 .
Retries	This parameter determines the number of times the switch searches the active TACACS server from the list of servers maintained. The allowed values are from 1 to 100. The factory default is 2 .

TACACS+ Servers

Figure 5-11. TACACS+ Server Configuration Page



Clicking the TACACS+ SERVERS tab brings up the TACACS+ SERVER CONFIGURATION page (Figure 5-11), which allows you to configure TACACS servers. The parameters for this page are shown in Table 5-6.

Table 5-6. TACACS+ Server Configuration Page Parameters

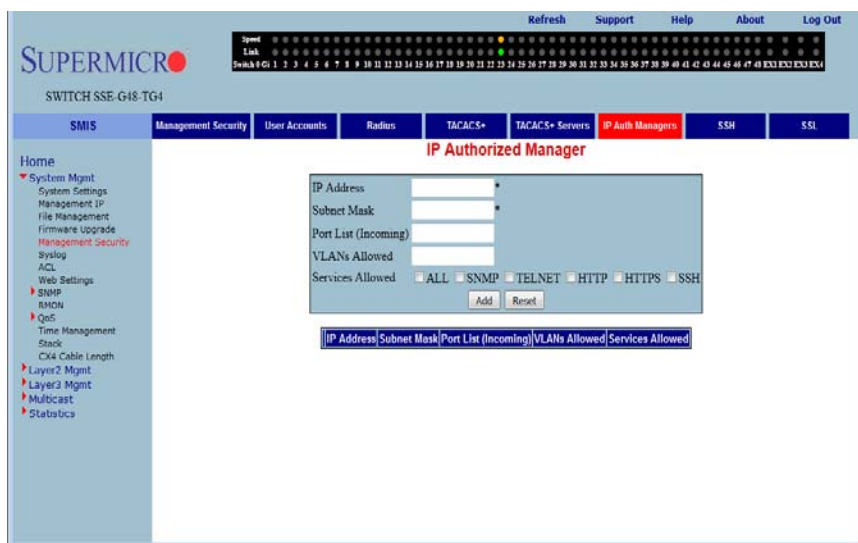
Parameter	Description
IP Address	This specifies the IP address of the TACACS server. The factory default is blank.
Port	This specifies the TCP port for TACACS protocol. The valid range is from 1 to 65000. The factory default is blank.
Single Connection	Specify Yes or No for a single TCP connection. If Yes, it establishes only a single TCP connection with a given TACACS server. The factory default is Yes.

Table 5-6. TACACS+ Server Configuration Page Parameters

Parameter	Description
Timeout	The time for which the switch will wait for a response from the TACACS server before closing the connection is specified with this parameter. It is configurable in seconds, with the valid range is from 4 to 15 and the default as 5-seconds..
Key Type	Specifies the Key Type for the TACACS server. The allowed key type is 0 or 7. The default key type is 0. The key 0 type key is plain text. For key 7 type, the user must provide the encrypted key string.
Secret Key	This specifies the encryption key for the given TACACS server. It has a 32-character input limit, and the factory default is blank.

IP Auth Manager

Figure 5-12. IP Authorized Manager Page



Clicking the IP AUTH MANAGER tab brings up the IP AUTHORIZED MANAGER page (Figure 5-12), which allows you to configure allowed management nodes for managing the switch. The parameters for this page are shown in Table 5-7.

Table 5-7. IP Authorized Manager Page Parameters

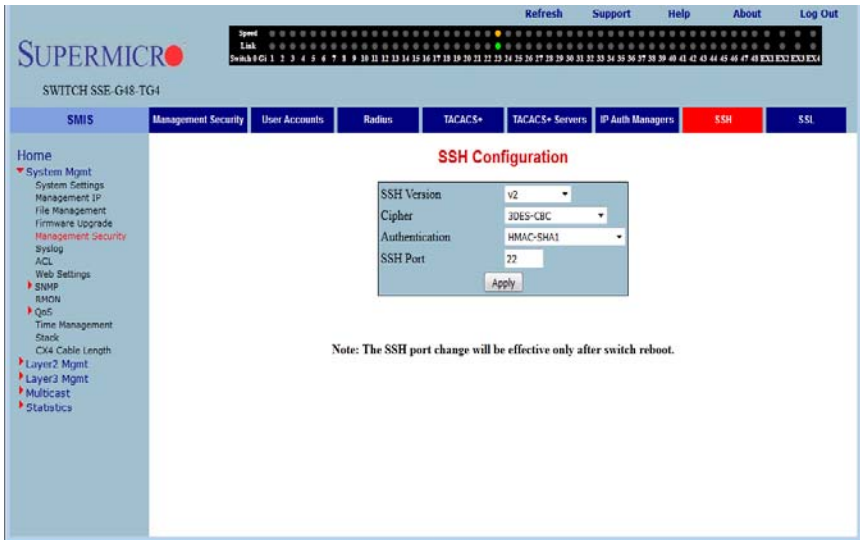
Parameter	Description
IP Address	This specifies the IP address of the manager. The default address of 0.0.0.0 indicates "Any Manager".
Subnet Mask	This specifies the sub-network mask for the specified IP address.

Table 5-7. IP Authorized Manager Page Parameters

Parameter	Description
Port List (Incoming)	This lists the port through which the manager can access this switch. Ports can be comma separated or provided as a range (for example Gi0/1 or Ex0/1). The factory default is blank.
VLANs Allowed	This parameter specifies the VLANs through which the manager can access this switch. VLANs can be comma separated or provided as range (for example 1,2,3 or 1-3 or 1,2-3).
Services Allowed	These control buttons are used to indicate the service type, and can be one or more of the following: TELNET, SSH, HTTP, HTTPS, SNMP or ALL.

SSH

Figure 5-13. SSH Configuration



Clicking the SSH (Secure Shell) tab brings up the SSH CONFIGURATION page (Figure 5-13), which allows you to configure SSH version and keys. The parameters for this page are shown in Table 5-8.

Table 5-8. SSH Configuration Page Parameters

Parameter	Description
SSH Version	The default for this parameter is v2. You can choose to configure this as compatible with v1 instead.

Table 5-8. SSH Configuration Page Parameters

Parameter	Description
Cipher	The default for this parameter is 3DES-CBC . You can instead choose to configure it as <i>3DES-CBC</i> or <i>DES-CBC</i> or both
Authentication	This parameter's default is HMAC-SHA1 . You can instead choose to configure it as <i>HMAC-SHA1</i> or <i>HMAC-MD5</i> or both.

SSL

Figure 5-14. SSL Configuration Page

The screenshot shows the Supermicro web management utility interface. At the top, there is a navigation bar with 'Refresh', 'Support', 'Help', 'About', and 'Log Out' buttons. Below this is the 'SUPERMICRO' logo and the device name 'SWITCH SSE-G48-TG4'. A menu bar contains 'SMIS', 'Management Security', 'User Accounts', 'Radius', 'TACACS+', 'TACACS+ Servers', 'IP Auth Managers', 'SSH', and 'SSL'. The 'SSL' tab is selected, displaying the 'SSL Configuration' page. The page is divided into several sections: 'Cipher Suite' with checkboxes for RSA-NULL-MD5, RSA-NULL-SHA, RSA-DES-SHA, RSA-3DES-SHA, DH-RSA-DES-SHA, DH-RSA-3DES-SHA, RSA-EXP1024, and DES-SHA; 'Crypto Key RSA' with a dropdown menu set to '1024' and an 'Apply' button; 'Server Status' showing 'Server is ENABLED' with a 'DISABLE' button; and 'Certificate Request' with a 'Subject' text box and a 'CREATE' button. On the right side, the 'Server Certificate' section displays a 'Certificate' data field with a long alphanumeric string.

Clicking the SSL (Secure Socket Layers) tab brings up the SSL CONFIGURATION page (Figure 5-14), which allows you to configure SSL parameters and generate SSL certificates for HTTPS. To configure SSL and enable HTTPS, follow the procedure below using this page.

Configuring SSL and Enabling HTTPS

1. Configure CIPHER SUITE and CRYPTO KEY RSA with your chosen parameters.
2. Create a certificate request by entering the subject name and clicking on the CREATE button.
3. When the page reloads, the text box below the CREATE button will display a certificate request. Copy and paste these contents to a text file that says **a.csr**.

4. To generate an SSL certificate, the **openssl** application can be used. The sub-steps below can be executed in any Linux machine to generate SSL certificates. For other *openssl* implementations, refer to the *openssl* documentation to find the equivalent steps for them.

- a. Execute the below command in the Linux shell.

```
openssl req -x509 -newkey rsa:1024 -keyout cakey.pem
-out cacert.pem
```

- b. Execute the below command also in a Linux shell.

```
openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem
-CAkey cakey.pem -CAcreateserial
```

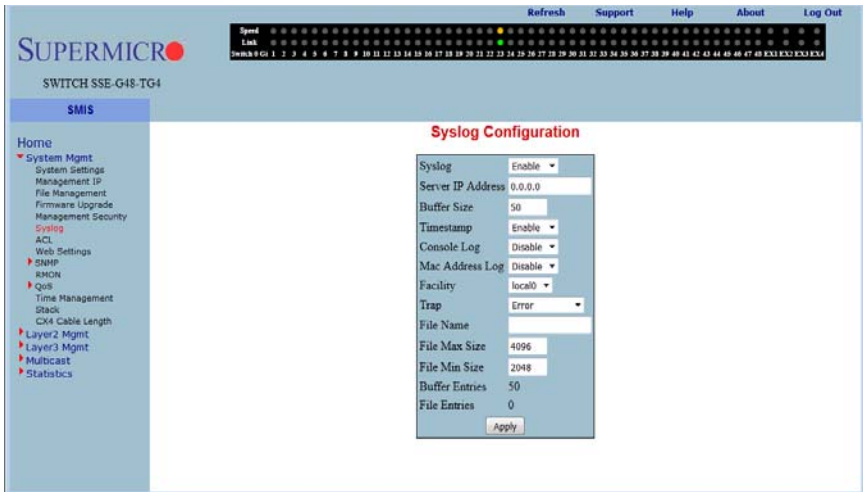
The above steps will generate the certificate file **cert.pem**.

5. Open the generated certificate file *cert.pem* and delete the first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--).
6. Join all the remaining lines as single lines to avoid line breaks being processed and copy/paste these joined texts in the ENTER CERTIFICATE text box back in the SSL CONFIGURATION page.
7. Click the CONFIGURE button.

This configures the certificate and saves it to flash memory.

Syslog

Figure 5-15. Syslog Configuration Page



Clicking the LOGGING tab brings up the SYSLOG CONFIGURATION page (Figure 5-15), which allows you to configure logging parameters. The parameters for this page are shown in Table 5-9.

Table 5-9. Syslog Configuration Page Parameters

Parameter	Description
Syslog	This parameter enables or disables the Syslog feature.
Server IP Address	This parameter specifies the Syslog server IP address. Make sure the Server IP is reachable.
Buffer Size	The buffer size is specified in log entries. Max entries buffered is 200 .
Timestamp	This parameter allows you to enable or disable the adding of a time stamp to the log messages.
Console Log	This parameter allows you to enable or disable logging to the console.
MAC Address Log	Enable or disable logging of the MAC address table update in syslog. By default MAC address logging is disabled.
Facility	This parameter allows you to select supported facilities. The switch supports syslog standard supported facilities LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 and USER.
Traps	This parameter helps you to select a particular trap type. The following types of traps are supported ALERTS, CRITICAL, DEBUGGING, EMERGENCIES, ERROR, INFORMATIONAL, NOTIFICATION and WARNINGS.
File Max Size	Specifies the maximum size of the file entries. The default is 4096 .
File Min Size	Specifies the minimum size of the file entries. The default size is 2048 .
Buffer Entries	Displays the currently available number of log entries in syslog buffers.
File Entries	Displays the currently available number of log entries in syslog files.

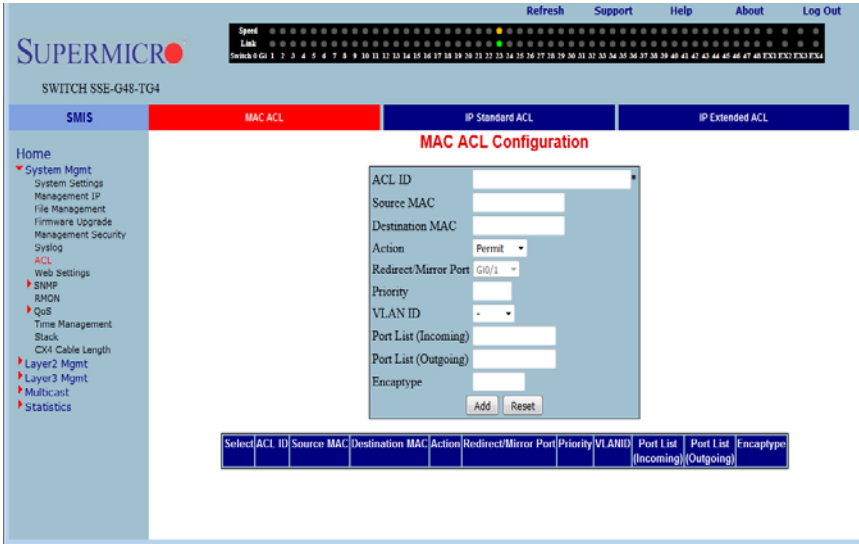
ACL

The ACL link allows you to configure the Access Control List for the switch. You can configure ACL on the following three pages:

- [MAC ACL](#)
- [IP Standard ACL](#)
- [IP Extended ACL](#)

MAC ACL

Figure 5-16. MAC ACL Configuration Page



Clicking the MAC ACL tab brings up the MAC ACL CONFIGURATION page (Figure 5-16), which displays the various parameters to configure the MAC Access List. The parameters for this page are shown in Table 5-10.

Table 5-10. MAC ACL Configuration Page Parameters

Parameter	Description
ACL ID	This specifies the unique ID for the access list. Valid range is 1 to 32768. The factory default is blank.
Source and Destination MAC	This specifies both the Source MAC Address and Destination MAC Address, for which the access list must be applied. Both the Source and Destination MAC Addresses must be configured for the status of the access list to be active. The factory default is blank.
Action	This specifies the action to be taken for the access list. The factory default is Permit . <ul style="list-style-type: none"> • Permit: Forwards packets which meet the ACL criteria. • Deny: Drops packets which meet the ACL criteria. • Redirect: Forces packets which meet the ACL criteria to specified port.
Redirect Port	This specifies the selected ports that packets meeting ACL criteria can be redirected to. Ports can be provided as a range (for example Gi0/1 or Ex0/1). The factory default is Gi0/1 .

Table 5-10. MAC ACL Configuration Page Parameters (Continued)

Parameter	Description
Priority	The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one set of filter rules. The higher value of "Filter Priority" implies a higher priority. The valid value is 1 to 255, and the factory default is 1.
VLAN ID	This specifies the VLAN ID for which the access list has to be applied.
Port List (Incoming)	This specifies the incoming physical ports, if this ACL has to be ports specific. (For example Gi0/1-10 or Gi0/1). The factory default is blank.
Encapsulation	This specifies the encapsulation type in the packet. It could be any value between 1 and 65535. The factory default is blank.
Protocol	This chooses the protocol type to be checked in the packet to apply this ACL. The factory default is blank.

IP Standard ACL

Figure 5-17. IP Standard ACL Configuration Page

The screenshot displays the 'IP Standard ACL Configuration' page. At the top, there is a status bar with 'Speed' and 'Link' indicators. Below that, the 'SUPERMICR' logo and 'SWITCH SSE-G48-TG4' are visible. The navigation menu on the left includes 'Home', 'System Mgmt', 'System Settings', 'Management IP', 'File Management', 'Firmware Upgrade', 'Management Security', 'Syslog', 'ACL', 'Web Settings', 'SNMP', 'RMON', 'QoS', 'Time Management', 'Stack', 'CX4 Cable Length', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The 'ACL' section is expanded, showing 'MAC ACL', 'IP Standard ACL' (highlighted in red), and 'IP Extended ACL'. The main configuration area is titled 'IP Standard ACL Configuration' and contains a form with the following fields: 'ACL ID' (text input), 'Action' (dropdown menu set to 'Permit'), 'Redirect/Mirror Port' (dropdown menu set to 'Gi0/1'), 'Priority' (text input), 'Source IP Address' (text input), 'Subnet Mask' (text input), 'Destination IP Address' (text input), 'Subnet Mask' (text input), 'Port List (Incoming)' (text input), and 'Port List (Outgoing)' (text input). Below the form are 'Add' and 'Reset' buttons. At the bottom, there is a table with the following columns: 'Select', 'ACL ID', 'Action', 'Redirects/Mirror Port', 'Priority', 'Source IP', 'Subnet Mask', 'Destination IP', 'Subnet Mask', 'Port List (Incoming)', and 'Port List (Outgoing)'.

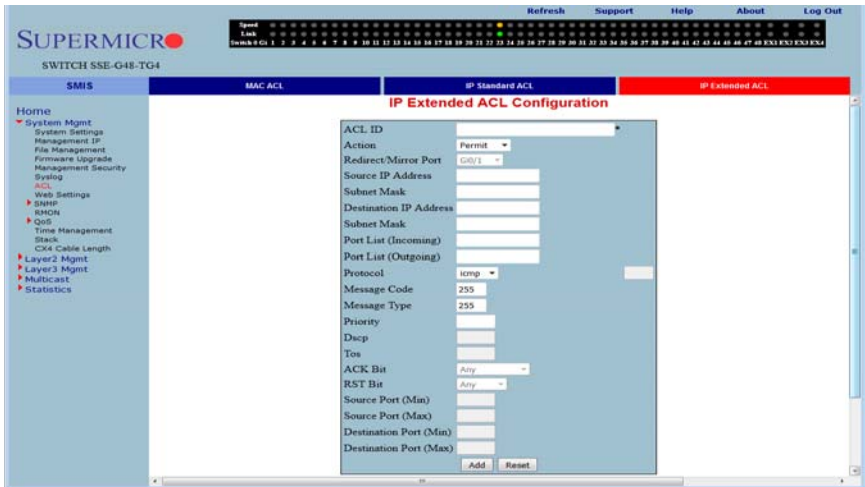
Clicking the IP STANDARD ACL (Access Control List) tab brings up the IP STANDARD ACL CONFIGURATION page (Figure 5-17), which displays the various parameters to configure the Standard IP access lists. The parameters for this page are shown in Table 5-11.

Table 5-11. IP Standard ACL Configuration Page Parameters

Parameter	Description
ACL Number	This specifies the unique ID for the access list. The valid range is between 1 and 32768. The factory default is blank.
Action	This specifies the action to be taken for the access list. The factory default is Permit . <ul style="list-style-type: none"> • Permit: Forwards packets which meet the ACL criteria. • Deny: Drops packets which meet the ACL criteria. • Redirect: Forces packets which meet the ACL criteria to specified port.
Priority	Specifies the priority for the access list. This value must be in the range from 1 to 255. The default priority value is 1.
Source and Destination IP Address	This specifies the IP Address of the Source and Destination, for which the access list must be applied. The factory default is blank.
Subnet Mask	This specifies the Source and Destination Address Mask corresponding to the IP Address.
Ports List (Incoming)	This specifies the incoming physical ports if this ACL has to be port specific (for example Gi0/1-10 or Gi0/1). The factory default is blank.
Ports List (Outgoing)	This specifies the outgoing physical ports if this ACL has to be port specific (for example Gi0/1-10 or Gi0/1). The factory default is blank.

IP Extended ACL

Figure 5-18. IP Extended ACL Page



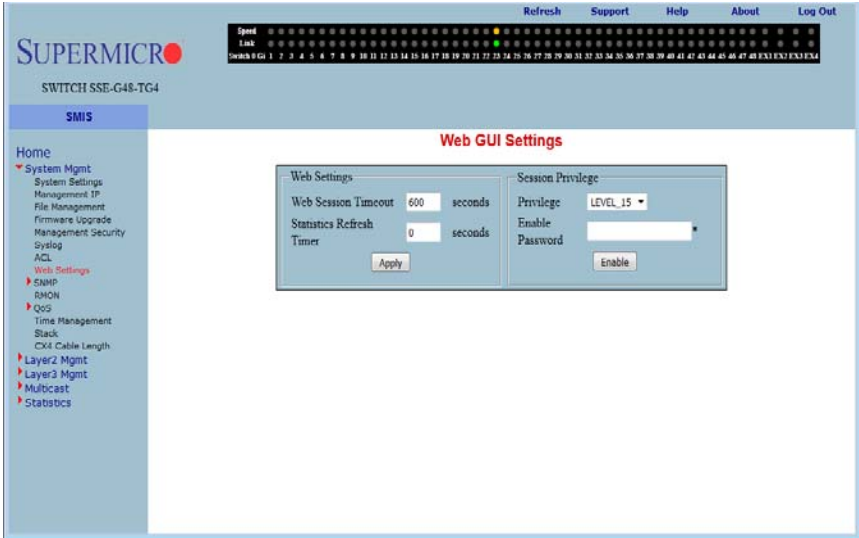
Clicking the IP EXTENDED ACL tab brings up the IP EXTENDED ACL CONFIGURATION page (Figure 5-18), which displays the various parameters required to configure the Extended IP access lists. The parameters for this page are shown in Table 5-12.

Table 5-12. IP Extended ACL Configuration Page Parameters

Parameter	Description
ACL Number	This specifies the unique ID for the access list. The valid range is between 1 to 32768. The factory default is blank.
Subnet Mask	This specifies the Address Mask corresponding to the IP Address.
Action	This specifies the action to be taken for the access list. The factory default is Permit . <ul style="list-style-type: none"> • <i>Permit</i>: Forwards packets which meet the ACL criteria. • <i>Deny</i>: Drops packets which meet the ACL criteria. • <i>Redirect</i>: Forces packets which meet the ACL criteria to specified port.
Source and Destination IP Address	This parameter specifies the IP Address for which the access list must be applied.
Ports List (Incoming)	This specifies the incoming physical ports if this ACL has to be port specific (for example <i>Gi0/1-10</i> or <i>Gi0/1</i>). The factory default is blank.
Ports List (Outgoing)	This specifies the outgoing physical ports if this ACL has to be port specific (for example <i>Gi0/1-10</i> or <i>Gi0/1</i>). The factory default is blank.
Protocol	This chooses the protocol type to be checked in the packet to apply this ACL. The factory default is icmp .
Message Code	This specifies the Message Code to be checked for ICMP Packets. The valid value is 255, which is also the factory default.
Message Type	This specifies the Message Type to be checked for ICMP Packets. The valid value is 255, which is also the factory default.
Priority	The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter's rules. The higher value of "Filter Priority" implies a higher priority. The valid value is 1 to 32768, while the factory default is 1.
DSCP	This specifies the Differentiated Services Code Point (DSCP) value assigned to the classified traffic. The valid value is 0 to 63, and the factory default is blank.
TOS	Type of service (TOS) can be <i>Max-reliability</i> , <i>Max Throughput</i> , <i>Min-delay</i> , <i>Normal</i> or a range of values from 0 to 7. The factory default is blank.
ACK Bit	This specifies the TCP ACK bit to be checked against the packet. It can be <i>Establish</i> , <i>Non-establish</i> or <i>Any</i> .
RST Bit	This specifies the TCP RST bit to be checked against the packet. It can be <i>Set</i> , <i>Notset</i> or <i>Any</i> .
Source Port (Min)/(Max)	This specifies the min/max TCP/UDP source port from which the access list has to be applied.
Destination Port (Min)/(Max)	This parameter specifies the min/max TCP/UDP destination port from which the access list has to be applied.
Other	This is only visible user to choose the Protocol as "other". The allowed value ranges are 1 to 255. The default value is 1.

WEB Settings

Figure 5-19. Web GUI Settings Page



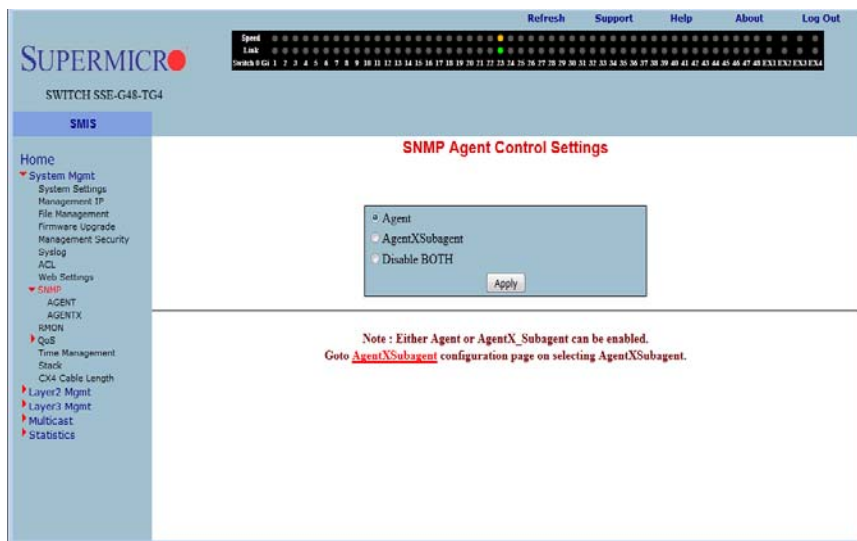
Clicking the WEB SETTINGS link brings up the WEB GUI SETTINGS page (Figure 5-19), which displays all basic Web GUI settings. The parameters for this page are shown in Table 5-13.

Table 5-13. Web GUI Settings Page Parameters

Parameter	Description
Session timeout	This timeout value is used to automatically logout inactive user sessions. The default value is 5-minutes (600-seconds).
Statistics Refresh Timer	The statistics pages (grouped under "Statistics" node in left side tree) can be set to auto refresh based on this Statistics Refresh Timer. The default value zero means no auto refresh by default.
Session Privilege	This displays the current privilege level of the logged in user. You can choose to enter another privilege level using this configuration if you have the Enable password for the required privilege levels. The Enable Passwords for different levels are configurable in the Enable Password parameter on the Management Security web page.

SNMP

Figure 5-20. SNMP Agent Control Settings Page



Clicking the SNMP link brings up the SNMP AGENT CONTROL SETTINGS page (Figure 5-20). SMIS supports the **SNMP Agent** or **SNMP AgentX Sub-agent**. The SNMP Agent or AgentX Sub-agent can be enabled or both can be disabled.

The SNMP Agent provides the following sub-page configurations shown in the table below.

Table 5-14. SNMP Agent Configuration Pages

Configuration Page	Description
Community	This page allows you to configure the SNMP community including the COMMUNITY INDEX, NAME, SECURITY NAME, CONTEXT NAME, TRANSPORT TAG and STORAGE TYPE.
Group	This page allows you to configure SNMP groups including GROUP NAME, SECURITY NAME, SECURITY MODEL and STORAGE TYPE.
Group Access	This page allows you to configure SNMP group's access parameters including GROUP NAME, SECURITY MODEL, SECURITY LEVEL, STORAGE TYPE, AND READ, WRITE and NOTIFY VIEW.
View	This page allows you to configure an SNMP view tree including VIEW NAME, SUB TREE, MASK, TYPE OF THE VIEW and STORAGE TYPE.
Target Address	This page allows you to configure the SNMP target including TARGET NAME, TARGET IP, TRANSPORT TAG, PARAM and STORAGE TYPE.

Table 5-14. SNMP Agent Configuration Pages (Continued)

Configuration Page	Description
Target Parameter	This setting allows you to configure SNMP target parameters including PARAMETER NAME, MP MODEL, SECURITY MODEL, NAME, LEVEL and STORAGE TYPE.
User	This setting allows you to configure SNMP security including user name, AUTHENTICATION PROTOCOL, AUTHENTICAITON KEY, PRIVACY PROTOCOL, PRIVACY KEY and STORAGE TYPE.
Trap Manager	This setting allows you to configure SNMP trap notifications including NOTIFY NAME, NOTIFY TAG, NOTIFY TYPE and STORAGE TYPE.

Community

Figure 5-21. SNMP Community Settings Page

The screenshot shows the 'SNMP Community Settings' page in the SUPERMICRO web management utility. The page has a navigation menu on the left with options like 'System Mgmt', 'System Settings', 'Management IP', 'File Management', 'Firmware Upgrade', 'Management Security', 'Syslog', 'ACL', 'Web Settings', 'SNMP', 'AGENT', 'AGENTX', 'RMON', 'QoS', 'Time Management', 'Stack', 'CX4 Cable Length', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The main content area is titled 'SNMP Community Settings' and contains a form with the following fields: Community Index, Community Name, Security Name, Context Name, Transport Tag, and Storage Type (set to 'Volatile'). Below the form is a table with the following data:

Select	Community Index	Community Name	Security Name	Context Name	Transport Tag	Storage Type
<input type="checkbox"/>	NETMAN	NETMAN	none			Volatile
<input type="checkbox"/>	PUBLIC	PUBLIC	none			Volatile

Buttons for 'Add', 'Reset', 'Apply', and 'Delete' are located at the bottom of the table.

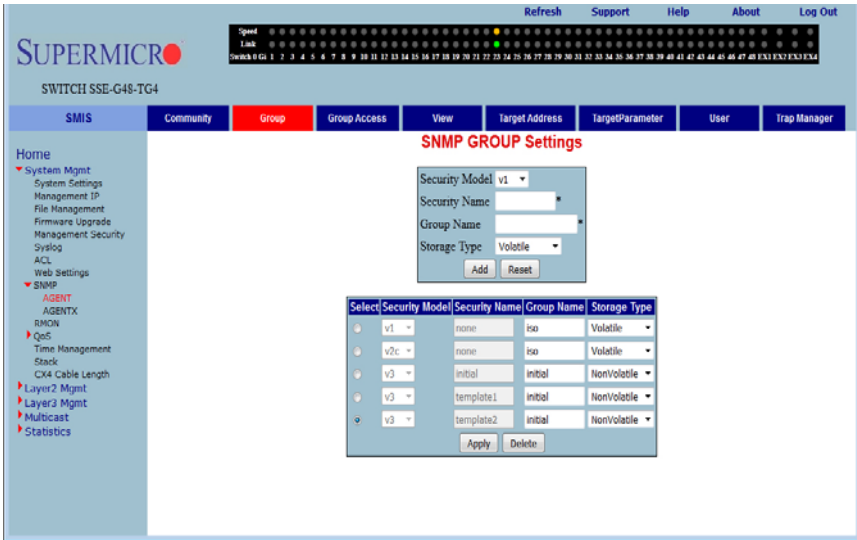
Clicking the COMMUNITY tab brings up the SNMP COMMUNITY SETTINGS page (Figure 5-21), which allows you to add SNMP managers or remove existing managers.. The parameters for this page are shown in Table 5-15.

Table 5-15. SNMP Community Settings Page Parameters

Parameter	Description
Community index	This parameter sets the COMMUNITY INDEX identifier.
Community name	This parameter sets the COMMUNITY NAME string.
Security Name	This parameter sets the User Name String.
Context Name	This parameter sets the CONTEXT NAME that the management information is accessed from when using the community string, which is specified by the corresponding instance of the SNMP community name.
Transport Tag	This parameter sets the TRANSPORT TAG Identifier.
Storage Type	This parameter sets the <i>Volatile Storage</i> or <i>Non-volatile Storage</i> setting.

Group

Figure 5-22. SNMP Group Settings Page



Clicking the GROUP tab brings up the SNMP GROUP SETTINGS page (Figure 5-22). This page helps you map a combination of the SECURITY MODEL and the SECURITY NAME into a GROUP NAME, which is used to define an access control policy. In addition, this page displays the STORAGE TYPE of the Group Table. The parameters for this page are shown in Table 5-16.

Table 5-16. SNMP Group Settings Page Parameters

Parameter	Description
Security Model	This parameter allows you to select from <i>version 1</i> , <i>version 2</i> or <i>version 3</i> for the SECURITY MODEL used.
Security Name	Use this parameter to specify the SECURITY NAME string.
Group Name	Use this parameter to specify the GROUP NAME string.
Storage Type	Use this parameter to specify whether the STORAGE TYPE is <i>volatile</i> or <i>non-volatile</i> .

Group Access

Figure 5-23. SNMP Group Access Settings Page

The screenshot shows the 'SNMP Group Access Settings' page. At the top, there is a status bar with 'Speed' and 'Link' indicators. Below that is the 'SUPERMICR' logo and the device model 'SWITCH SSE-G48-TG4'. A navigation bar contains tabs for 'SMIS', 'Community', 'Group', 'Group Access' (selected), 'View', 'Target Address', 'TargetParameter', 'User', and 'Trap Manager'. The left sidebar lists various management options, with 'SNMP' expanded to show 'AGENT', 'AGENTX', 'RMON', 'QoS', 'Time Management', 'Stack', 'CX4 Cable Length', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The main area is titled 'SNMP Group Access Settings' and contains a form with the following fields: 'Group Name' (text input), 'Security Model' (dropdown menu showing 'v1'), 'Security Level' (dropdown menu showing 'NoAuthentication'), 'Read View' (text input), 'Write View' (text input), 'Notify View' (text input), 'Storage Type' (dropdown menu showing 'Volatile'), and 'Context' (text input). Below the form are 'Add' and 'Reset' buttons. Below the form is a table with the following columns: 'ALL', 'Group Name', 'Security Model', 'Security Level', 'Read View', 'Write View', 'Notify View', 'Storage Type', and 'Context'. The table contains five rows of data:

ALL	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Storage Type	Context
<input type="checkbox"/>	iso	v1	noauth	iso	iso	iso	Volatile	
<input type="checkbox"/>	iso	v2c	noauth	iso	iso	iso	Volatile	
<input type="checkbox"/>	initial	v3	noauth	restricted	restricted	restricted	NonVolatile	
<input type="checkbox"/>	initial	v3	auth	iso	iso	iso	NonVolatile	
<input type="checkbox"/>	initial	v3	priv	iso	iso	iso	NonVolatile	

At the bottom of the table are 'Apply' and 'Delete' buttons.

Clicking the GROUP ACCESS tab brings up the SNMP GROUP ACCESS SETTINGS page (Figure 5-23), which displays the access rights of groups. Each entry is indexed by a GROUP NAME, a Context Prefix, a SECURITY MODEL and a SECURITY LEVEL. A proper view name (READ, WRITE and MODIFY) must be used for access control checking. It also displays the STORAGE TYPE of the Group Access table. An SNMP Group has to be created prior to the Group Access configuration. The parameters for this page are shown in Table 5-17.

Table 5-17. SNMP Group Access Settings Page Parameters

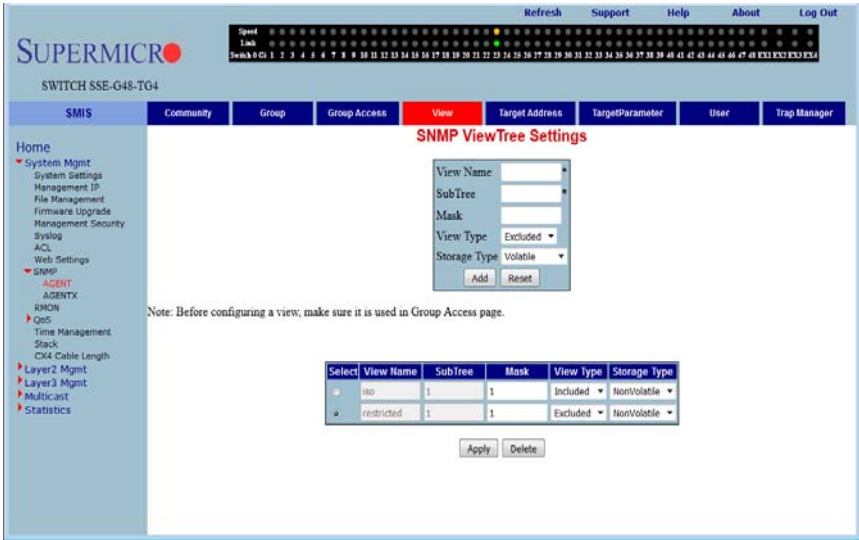
Parameter	Description
Group Name	This parameter allows you to specify the GROUP NAME string.
Security Model	This parameter allows you to specify whether SNMP <i>version v1</i> , <i>v2</i> or <i>v3</i> is used. <i>Version 3</i> is the most secure model as it allows packet encryption with the private key word.
Security Level	With this parameter the no-authentication option disables authentication. The AUTHENTICATION option enables <i>Message digest (MD5)</i> or <i>Secure Hash Algorithm (SHA)</i> packet authentication. The PRIVATE option selects both AUTHENTICATION and PRIVACY.
Read View	This parameter allows you to specify the READ VIEW identifier.
Write View	This parameter allows you to specify the WRITE VIEW identifier.
Notify View	This parameter allows you to specify the NOTIFY VIEW identifier.

Table 5-17. SNMP Group Access Settings Page Parameters (Continued)

Parameter	Description
Storage Type	Use this parameter to specify whether the STORAGE TYPE is <i>volatile</i> or <i>non-volatile</i> .
Context	Use this parameter to configure an SNMP context name that identifies this group.

View

Figure 5-24. SNMP View Tree Settings Page



Clicking the VIEW tab brings up the SNMP VIEW TREE SETTINGS page (Figure 5-24), which allows configuration of view trees. A SUBTREE when combined with the corresponding instance of a MASK defines a family of view subtrees. The VIEW NAME is the name for a family of view subtrees. This page also displays the STORAGE TYPE of the VIEWTREE table. SNMP Group and SNMP Access settings have to be created prior to the Group View configuration. The parameters for this page are shown in Table 5-18.

Table 5-18. SNMP View Tree Settings Page Parameters

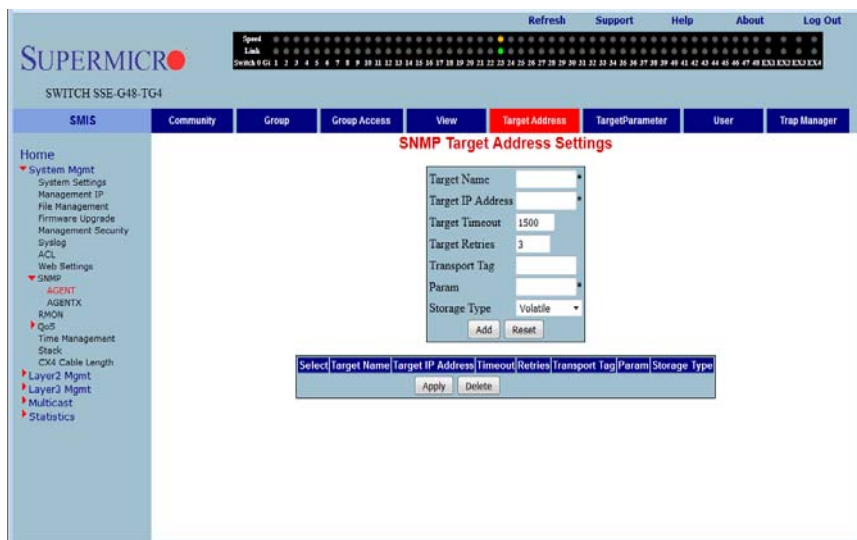
Parameter	Description
View Name	This parameter specifies a View Name string.
SubTree	This parameter specifies a tree OID.
Mask	This parameter specifies an OID mask.

Table 5-18. SNMP View Tree Settings Page Parameters (Continued)

Parameter	Description
View Type	This parameter specifies whether a View Type is <i>Included</i> or <i>Excluded</i> .
Storage Type	Use this parameter to specify whether the Storage Type is <i>volatile</i> or <i>non-volatile</i> .

Target Address

Figure 5-25. SNMP Target Address Settings Page



Clicking the TARGET ADDRESS tab brings up the SNMP TARGET ADDRESS SETTINGS page (Figure 5-25), which configures SNMP target address parameters. The parameters for this page are shown in Table 5-19.

Table 5-19. SNMP Target Address Settings Page Parameters

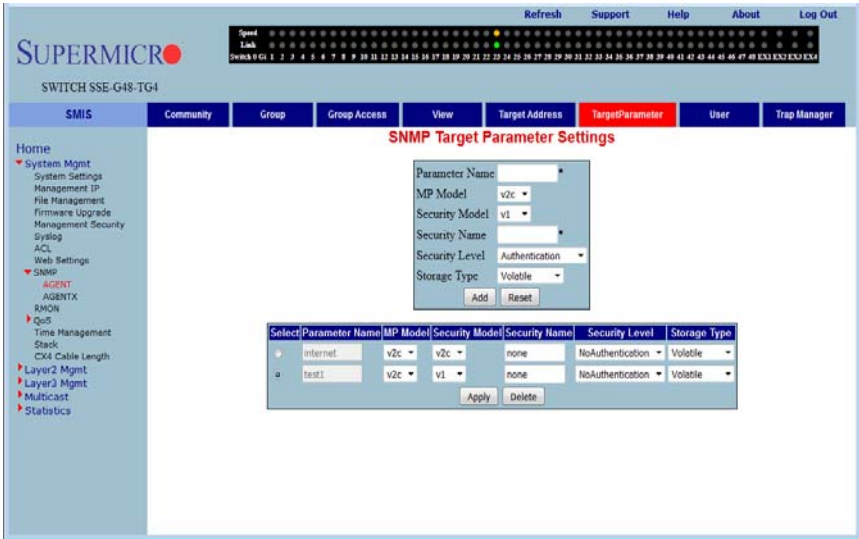
Parameter	Description
Target Name	This parameter specifies a Target Name as a unique identifier.
Target IP Address	The Target IP Address specifies a target address to be used in the generation of SNMP operations.
Target Timeout	Target Timeout specifies the maximum round trip for communicating with the Target IP Address.
Target Retries	Target Retries specifies the number of attempts to be made when no response is received
Transport Tag	The Transport Tag value is used to select a target address for a particular operation.

Table 5-19. SNMP Target Address Settings Page Parameters (Continued)

Parameter	Description
Param	Param contains SNMP parameters to be used when generating messages to be sent to a transport address.
Storage Type	Use this parameter to specify whether the Storage Type is <i>volatile</i> or <i>non-volatile</i> .

Target Parameter

Figure 5-26. SNMP Target Parameter Settings Page



Clicking the TARGET PARAMETER tab brings up the SNMP TARGET PARAMETER SETTINGS page (Figure 5-26), which configures SNMP Target Address parameters. The parameters for this page are shown in Table 5-20.

Table 5-20. SNMP Target Parameter Settings Page Parameters

Parameter	Description
Parameter Name	The target parameter is a unique name that specifies SNMP target information to be used in the generation of SNMP messages.
MP Model	The Message Processing (MP) Model is used when generating SNMP messages using this entry.
Security Model	The Security Model is used when generating SNMP messages using this entry.
Security Name	The Security Name identifies the current Parameter Name, on whose behalf SNMP messages will be generated.

Table 5-20. SNMP Target Parameter Settings Page Parameters (Continued)

Parameter	Description
Security Level	Security Level specifies the level of security used when generating SNMP messages.
Storage Type	Storage Type can be configured as Volatile or Non-Volatile.
Engine ID	This parameter displays the SNMP Engine ID.

User

Figure 5-27. SNMP Security Settings Page

The screenshot shows the 'SNMP Security Settings' page in the SUPERMICR web management utility. The page has a navigation bar with tabs for 'Community', 'Group', 'Group Access', 'View', 'Target Address', 'TargetParameter', 'User', and 'Trap Manager'. The 'User' tab is selected. The main content area contains a form for adding or editing a user. The form fields are: User Name (text input), Authentication Protocol (dropdown menu set to 'No Authentication'), Authentication Key (text input), Privacy Protocol (dropdown menu set to 'No Privacy'), Privacy Key (text input), and Storage Type (dropdown menu set to 'Volatile'). There are 'Add' and 'Reset' buttons below the form. Below the form is a table with the following data:

Select	Engine Id	User Name	Authentication Protocol	Privacy Protocol	Storage Type
<input type="radio"/>	80:00:08:1c:04:46:53	initial	No Authentication	No Privacy	Volatile
<input type="radio"/>	80:00:08:1c:04:46:53	template1	HMAC-MD5	No Privacy	Volatile
<input type="radio"/>	80:00:08:1c:04:46:53	template2	HMAC-MD5	DES	Volatile

Buttons for 'Apply' and 'Delete' are located below the table.

Clicking the USER tab brings up the SNMP SECURITY SETTINGS page (Figure 5-27), which configures users configured in the SNMP for the User-based Security Model. The parameters for this page are shown in Table 5-21.

Table 5-21. SNMP Security Settings Page Parameters

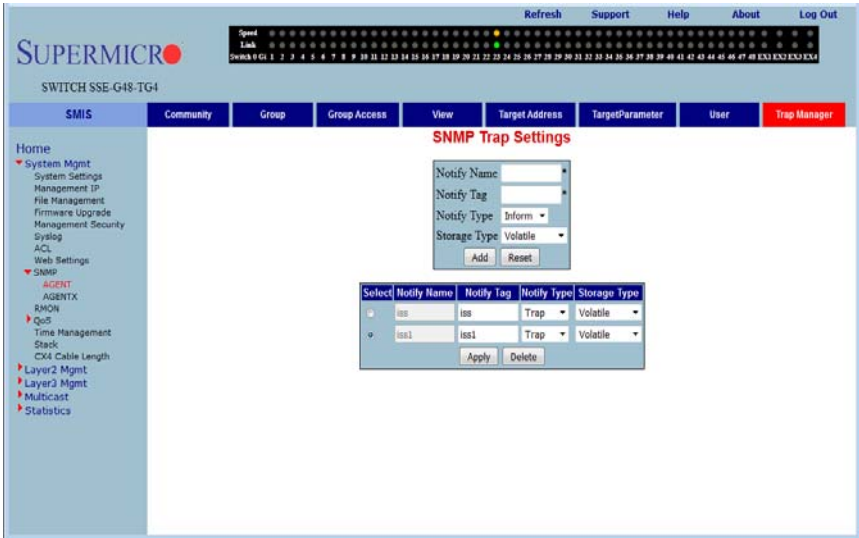
Parameter	Description
User Name	User Name is the (User-based Security) model dependent security ID.
Authentication Protocol	The Authentication Protocol is used for authentication.
Authentication Key	The Authentication Key is the secret authentication key used for messages sent on behalf of this user to/from the SNMP.
Privacy Protocol	Privacy Protocol is an indication of whether or not messages sent on behalf of this user to/from the SNMP are protected from disclosure, and if so, the type of privacy protocol that is used.

Table 5-21. SNMP Security Settings Page Parameters (Continued)

Parameter	Description
Privacy Key	Privacy Key is an indication of whether or not messages sent on behalf of this user to/from the SNMP are protected from disclosure.
Storage Type	Storage Type can be configured as Volatile or Non-Volatile.

Trap Manager

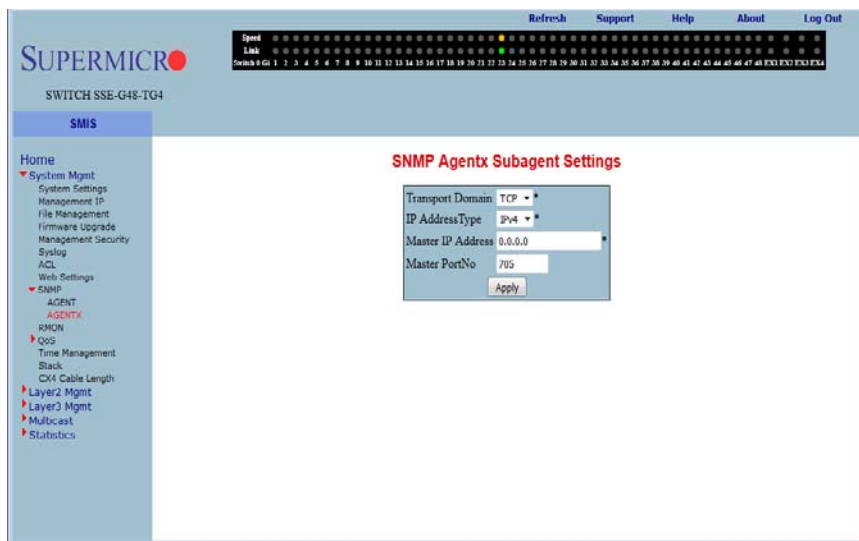
Figure 5-28. SNMP Trap Settings Page



Clicking the TRAP MANAGER tab brings up the SNMP TRAP SETTINGS page (Figure 5-28), which configures the set of management targets that must receive notifications. The parameters for this page are shown in Table 5-22.

Table 5-22. SNMP Trap Settings Page Parameters

Parameter	Description
Notify Name	Notify Name is a unique identifier associated with the entry.
Notify Tag	Notify Tag contains a single tag value, which is used to select entries in the Target Address table. Any entry in the Target Address table that contains a tag value equal to the value of an instance of this Trap Manager, is selected.
Notify Type	The type of notification of the SNMP Trap Settings can be configured as <i>Trap</i> or <i>Inform</i> .
Storage Type	Storage Type can be configured as <i>Volatile</i> or <i>Non-Volatile</i> .

SNMP AgentX**Figure 5-29. SNMP AgentX Subagent Settings Page**

Clicking the AGENTX link brings up the SNMP AGENTX SUBAGENT SETTINGS page (Figure 5-29), which allows you to configure SNMP Agentx sub-agent parameters. The parameters for this page are shown in Table 5-23.

Table 5-23. SNMP AgentX Subagent Settings Page Parameters

Parameter	Description
Transport Domain	This parameter allows you to specify the TCP.
IP Address Type	This parameter specifies <i>IPv4</i> or <i>IPv6</i> for the IP ADDRESS TYPE.
Master IP Address	This parameter specifies the Master Agent IP address.
Master Port No	This parameter specifies the Master Port number. Allowed values range from 0 to 65535. The default value is 705 .

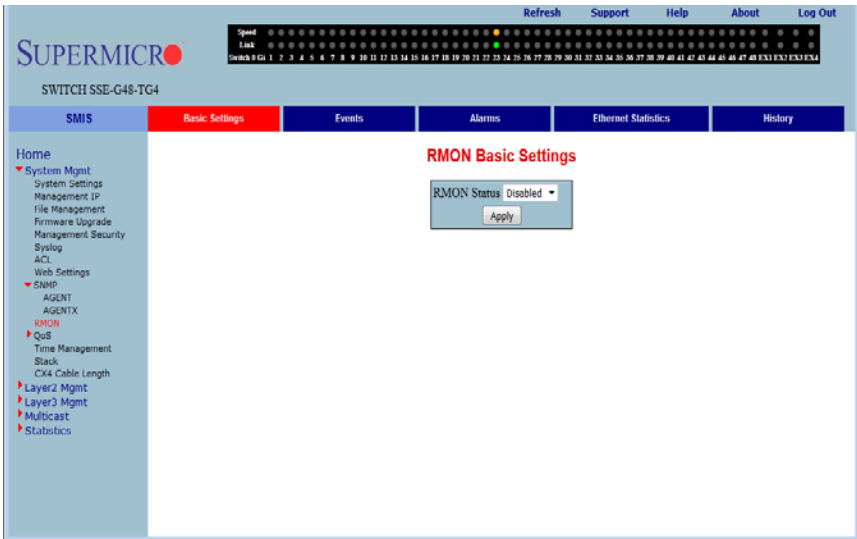
RMON

The following pages can be used to set RMON (Remote Monitoring) features and settings:

- [Basic Settings](#)
- [Events](#)
- [Alarm](#)
- [Ethernet Statistics](#)
- [History](#)

Basic Settings

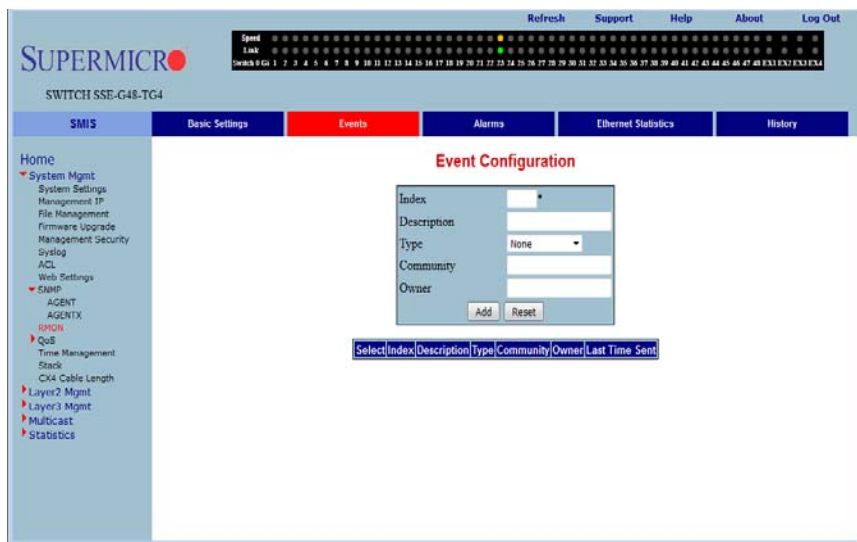
Figure 5-30. RMON Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the RMON BASIC SETTINGS page (Figure 5-30), which enables/disables the RMON feature using the RMON Status parameter.

Events

Figure 5-31. Event Configuration Settings Page



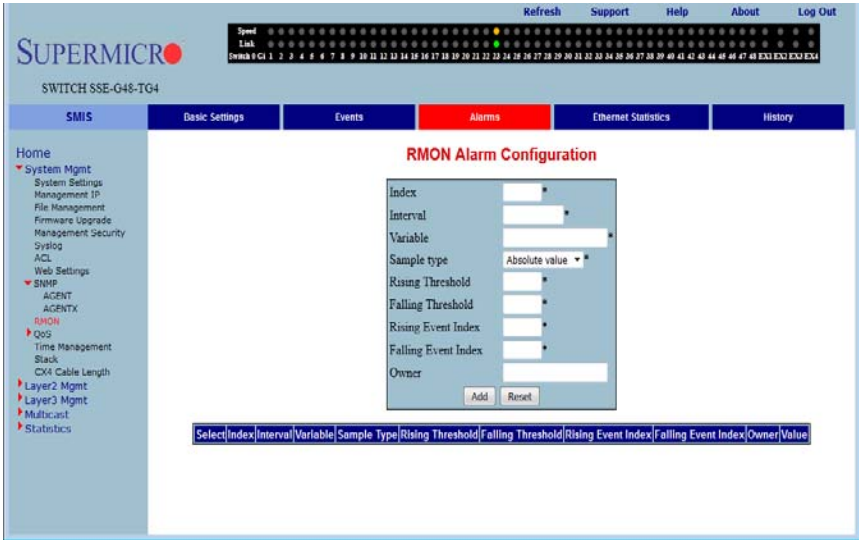
Clicking the EVENTS tab brings up the EVENT CONFIGURATIONS page (Figure 5-31), which configures RMON events. The parameters for this page are shown in Table 5-24.

Table 5-24. Event Configuration Page Parameters

Parameter	Description
Index	This parameter specifies the index to the Events table.
Description	This parameter specifies a brief description of the event.
Type	This parameter specifies the event configured. This can be a <i>Log</i> , an <i>SNMP Trap</i> , <i>Both</i> , or <i>None</i> . For the event type to display, <i>TRAP and Log</i> and <i>TRAP Community</i> must be configured.
Community	This parameter specifies the SNMP community string used for this trap. This is relevant when an SNMP trap is requested for an event. For event type to display, <i>TRAP and Log</i> and <i>TRAP Community</i> must be configured. Also make sure the configured community is active before adding an event on that community.
Owner	This parameter indicates the owner of this event.
Last Time Sent	Denotes the time this event entry last generated an event.

Alarm

Figure 5-32. RMON Alarm Configuration Page



Clicking the ALARM tab brings up the RMON ALARM CONFIGURATION page (Figure 5-32), which configures RMON Alarm parameters. The parameters for this page are shown in Table 5-25.

Table 5-25. RMON Alarm Configuration Page Parameters

Parameter	Description
Index	This parameter specifies the table index. This value must be in the range from 1 to 65535.
Interval	This parameter specifies the time interval for which the alarm monitors the variable. This value must be in the range from 1 to 4294967296.
Variable	This parameter specifies the MIB object on which the alarm is set.
Sample Type	You can set this parameter to an <i>Absolute Value</i> or as just an <i>Incremental Value</i> of the timer.
Rising Threshold	If the startup alarm is set as <i>Rising Alarm</i> and this threshold is reached, an alarm is raised. This value ranges between 0 and 2147483647.
Falling Threshold	If the startup alarm is set as <i>Falling Alarm</i> and this threshold is reached, an alarm is raised. This value ranges between 0 and 2147483647. The falling threshold must be less than the rising threshold.
Rising Event Index	Indicates the index of the event to be raised when the RISING THRESHOLD is reached. This value must be in the range from 0 to 65535.

Table 5-25. RMON Alarm Configuration Page Parameters (Continued)

Parameter	Description
Falling Event Index	Indicates the index of the event to be raised when the FALLING THRESHOLD is reached. This value must be in the range from 0 to 65535.
Owner	Specifies the owner of the alarm.

Ethernet Statistics

Figure 5-33. Ethernet Statistics Configuration Page

The screenshot shows the 'Ethernet Statistics Configuration' page. The navigation menu on the left includes 'Home', 'System Mgmt', 'System Settings', 'Management IP', 'File Management', 'Firmware Upgrade', 'Management Security', 'Syslog', 'ACL', 'Web Settings', 'SNMP', 'AGENT', 'AGENTX', 'RMON', 'QoS', 'Time Management', 'Stack', 'CX4 Cable Length', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The 'Ethernet Statistics' tab is active. The configuration form includes an 'Index' field, a 'Port' dropdown menu (set to G0/1), and an 'Owner' text field. Below the form is a table with the following columns: Select, Index, Port, Bytes, Pkts, Scast, Mcast, Under sized, Over sized, Frag ments, Jabbs, CRC errors, Collisions, 64, 128, 256, 512, 1024, and Owner.

Clicking the ETHERNET STATISTICS tab brings up the ETHERNET STATISTICS CONFIGURATION page (Figure 5-33), which configures RMON Ethernet statistics parameters. The parameters for this page are shown in Table 5-26.

Table 5-26. Ethernet Statistics Configuration Page Parameters

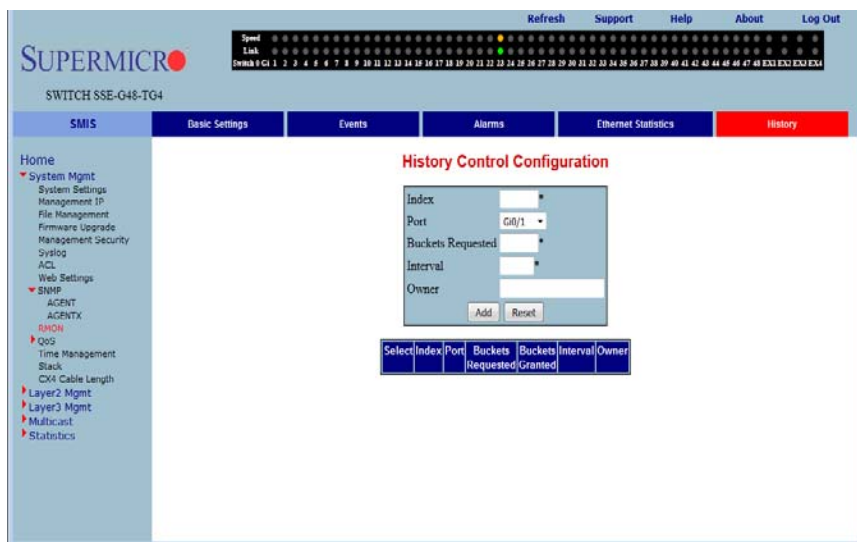
Parameter	Description
Index	This parameter specifies the index to the table. This value must be in the range from 0 to 65535.
Port	This parameter specifies the Ethernet Port.
Octets	This parameter specifies the total number of octets received from the network.
Packets	This parameter specifies the total number of packets received from the network.
Broadcast Packets	This parameter specifies the total number of broadcast packets received from the network.

Table 5-26. Ethernet Statistics Configuration Page Parameters (Continued)

Parameter	Description
Multicast Packets	This parameter specifies the total number of multicast packets received from the network.
Owner	This parameter specifies the owner string.
Undersized Packets	Displays the number of undersized packets received from the network.
Oversized Packets	Displays the number of oversized packets received from the network.
Fragments	Displays the number of fragments received from the network.
Jabbers	Displays the number of jabbers in the network.
CRC	Displays the number of packets received with CRC errors from the network.
Collisions	Displays the number of Collisions in the network.
64 Octets	Displays the number of Ethernet packets received with size 64 octets or less.
65-127 Octets	Displays the number of Ethernet packets received with size between 65 to 127 octets.
128-255 Octets	Displays the number of Ethernet packets received with size between 128 to 255 octets.
256-511 Octets	Displays the number of Ethernet packets received with size between 256 to 511 octets.
512-1023 Octets	Displays the number of Ethernet packets received with size between 512 to 1023 octets.
1024-1518 Octets	Displays the number of Ethernet packets received with size between 1024 to 1518 octets.

History

Figure 5-34. History Control Configuration Page



Clicking the HISTORY tab brings up the HISTORY CONTROL CONFIGURATION page (Figure 5-34), which configures RMON history configuration parameters. The parameters for this page are shown in Table 5-27.

Table 5-27. History Control Configuration Page Parameters

Parameter	Description
Index	This parameter specifies the index to the table.
Data Source	This parameter specifies the SNMP object ID of the variable for which the history is being collected.
Buckets Requested	Indicates the number of buckets to be configured for collecting the RMON statistics. This value must be in the range from 1 to 65535.
Interval	This parameter specifies the time interval between two successive polls to collect the statistics. This value must be in the range from 1 to 3600.
Owner	Denotes the owner of the RMON group of statistics.
Buckets Granted	Denotes the number of buckets granted for collecting the RMON statistics.
Status	This parameter specifies the status of the History Control entry as either <i>Valid</i> or <i>Invalid</i> .

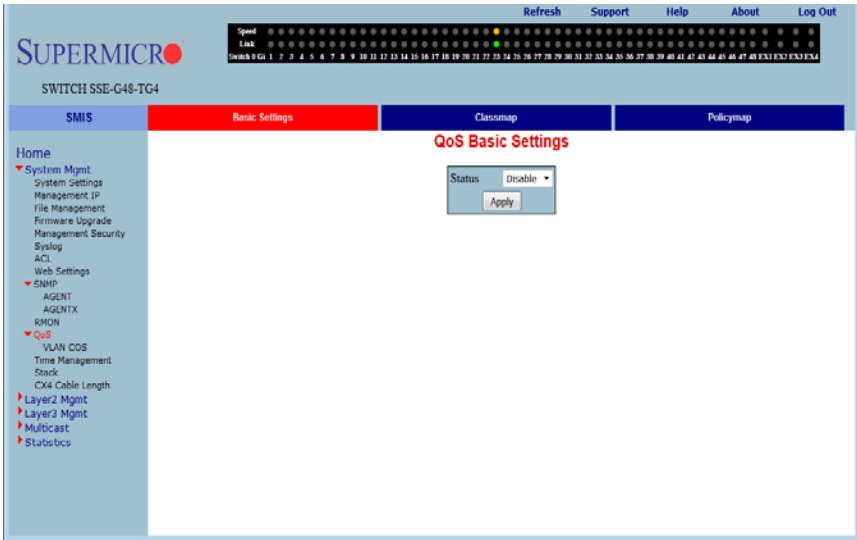
QoS

The QoS link of the System page opens the QoS Basic Settings page. This page allows you to configure QoS through following pages:

- [Basic Settings](#)
- [Classmap](#)
- [Policymap](#)

Basic Settings

Figure 5-35. QOS Basic Settings Page



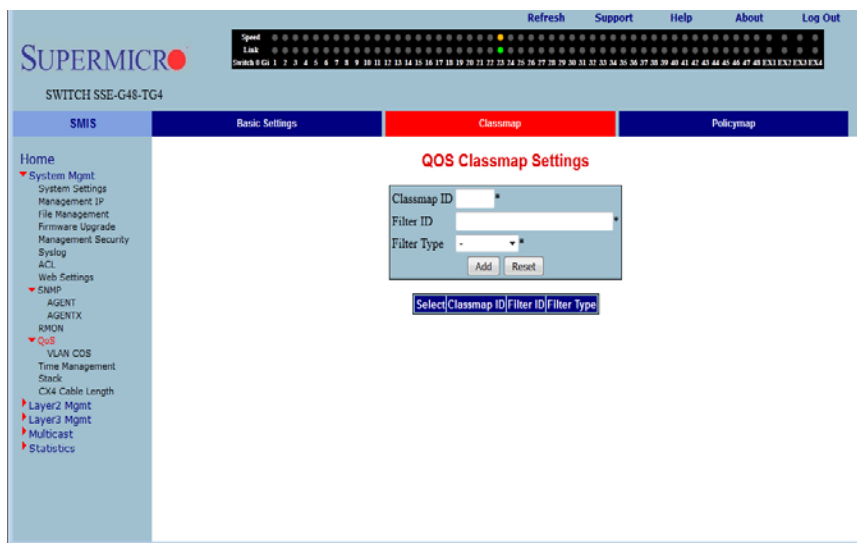
Clicking the BASIC SETTINGS tab brings up the QOS BASIC SETTINGS page (Figure 5-35), which allows you to configure QOS basic settings parameters. The parameters for this page are shown in Table 5-28.

Table 5-28. QOS Basic Settings Page Parameters

Parameter	Description
System Control	With this parameter SYSTEM CONTROL can <i>Start</i> or <i>Shutdown</i> QoS.
Status	This parameter allows enabling/disabling of the QoS status.

Classmap

Figure 5-36. QOS Classmap Settings Page



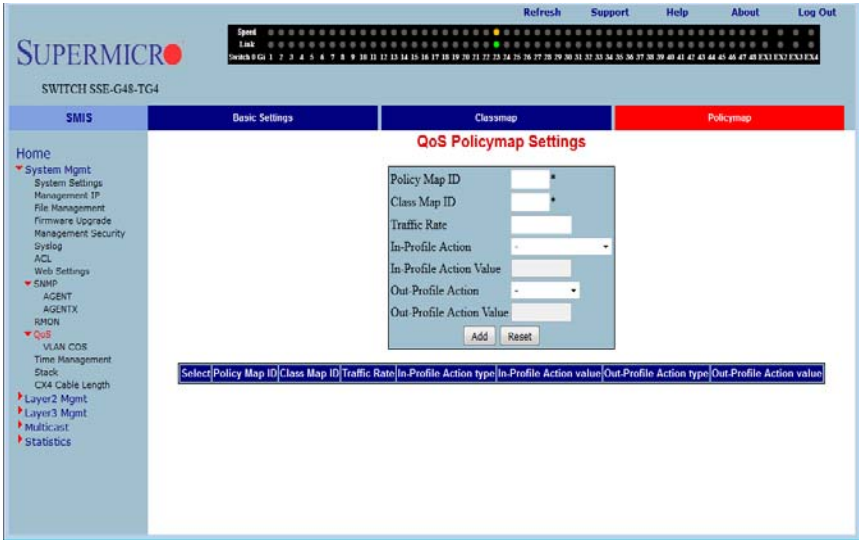
Clicking the CLASSMAP tab brings up the QOS CLASSMAP SETTINGS page (Figure 5-36), which is used to classify the stream of traffic. The parameters for this page are shown in Table 5-29.

Table 5-29. QOS Classmap Settings Page Parameters

Parameter	Description
Classmap ID	This parameter specifies a unique ID for the Classmap. It must be in the range from 1 to 65535.
Filter ID	This parameter specifies the unique Filter ID associated with this Classmap.
Filter Type	This parameter specifies the filter type associated with the Classmap. It can be set as either <i>MAC filter (1)</i> or <i>IP filter (2)</i> .

Policymap

Figure 5-37. QOS Policymap Settings Page



Clicking the POLICYMAP tab brings up the QOS POLICYMAP SETTINGS page (Figure 5-37), which is used to specify action for a specified classmap. The parameters for this page are shown in Table 5-30.

Table 5-30. QOS Policymap Settings Page Parameters

Parameter	Description
Policy Map ID	This parameter specifies the unique ID for Policymap. The value ranges between 1 and 65535.
Class Map ID	This parameter specifies the CLASS MAP ID to associate with Policymap.
Traffic Rate	This parameter specifies the TRAFFIC RATE of data that has to be applied. The value ranges between 1 and 65535.
In-Profile Action	This parameter specifies the action to be applied on matched data, and can be specified as either <i>Policy DSCP</i> or <i>Policy Precedence</i> .
Out-Profile Action	This parameter specifies the action to be applied on out-of-profile data, and can be specified as either <i>Policy DSCP</i> or <i>Drop</i> .
In-Profile Action Value	The IN-PROFILE ACTION VALUE can be specified from 0 to 7 for DSCP, or from 0 to 63 for IP Precedence.
Out-Profile Action Value	The OUT-PROFILE ACTION VALUE can be specified as <i>Drop</i> or from 0 to 63 for DSCP.

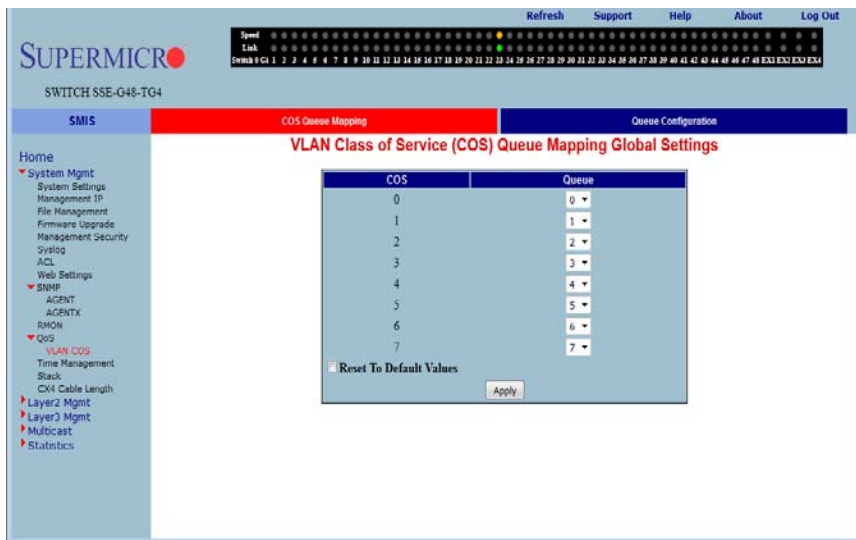
VLAN COS

The VLAN COS page opens the VLAN Class of Service (COS) Que Mapping Global Settings page. This page allows you to configure VLAN COS through the following pages:

- [COS Queue Mapping](#)
- [Queue Configuration](#)

COS Queue Mapping

Figure 5-38. VLAN Class of Service (COS) Queue Mapping Global Settings



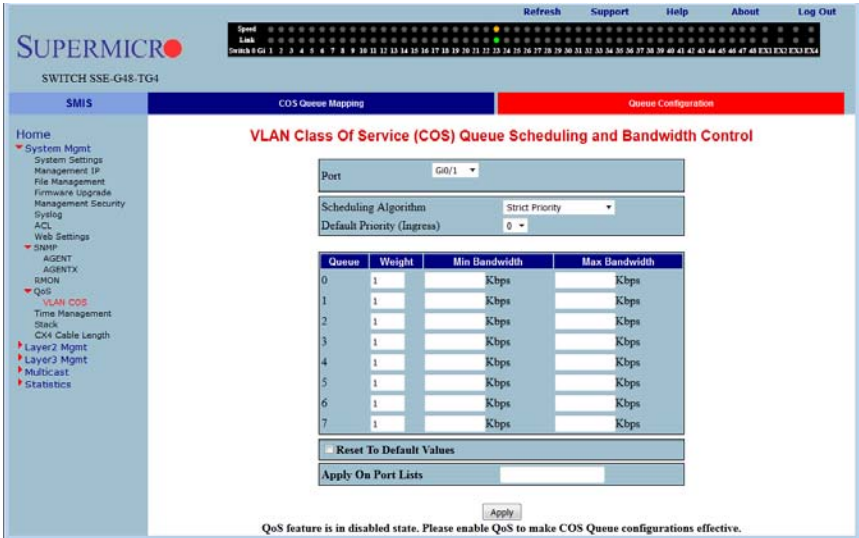
Clicking the COS QUEUE MAPPING tab brings up the VLAN CLASS OF SERVICE (COS) QUEUE MAPPING GLOBAL SETTINGS page (Figure 5-38), which configures Class Of Server (COS) Queue Mapping. The parameters for this page are shown in Table 5-31.

Table 5-31. VLAN COS Queue Mapping Global Settings Page Parameters

Parameter	Description
Queue	This parameter allows you to assign a class of service to a specific queue number from 0 to 7.
Reset to Defaults	Sets the default values for all the configuration in this page.

Queue Configuration

Figure 5-39. VLAN Class of Service (COS) Queue Scheduling and Bandwidth Control



Clicking the QUEUE CONFIGURATION tab brings up the VLAN CLASS OF SERVICE (COS) QUE SCHEDULING AND BANDWIDTH CONTROL page (Figure 5-38), which configures VLAN COS queue scheduling and bandwidth control services. The parameters for this page are shown in Table 5-31.

Table 5-32. VLAN COS Queue Scheduling and Bandwidth Control Page Parameters

Parameter	Description
Port	This list of ports allows you to select from the port index for your selected algorithm.
Scheduling Algorithm	The SCHEDULING ALGORITHM can be selected as one of the following: <ul style="list-style-type: none"> • <i>Strict Priority</i> • <i>Round Robin</i> • <i>Weighted Round Robin</i> • <i>Deficit Round Robin</i>
Default Priority (Ingress)	This parameter allows you to select between 0 to 7 for your default priority value.
Weight	This parameter allows you to select between 0 to 15 for your COS Queue WEIGHT value.
Min Bandwidth	This parameter configures minimum bandwidth between 1 to 262143.
Max Bandwidth	This parameter configures maximum bandwidth between 1 to 262143.
COS Queue Flag	Use this parameter to set a flag for this queue.

Table 5-32. VLAN COS Queue Scheduling and Bandwidth Control Page Parameters

Parameter	Description
Reset to Defaults	Sets the default values for all the configuration in this page.
Apply On Port Lists	To apply the same configuration on multiple ports, provide the port list on this field and click on APPLY. For example the port list should be like <i>gi0/1-10, gi0/12, gi0/15</i> , and so on.

Time Management

The Time Management link of the System page opens the Time Management page. This page allows you to configure QoS through following pages:

- [NTP Settings](#)
- [Clock Settings](#)

NTP Settings

Figure 5-40. NTP Settings Page

Clicking the NTP link brings up the NTP SETTINGS page (Figure 5-40), which configures the Network Time Protocol (NTP). The parameters for this page are shown in Table 5-33.

Table 5-33. NTP Settings Page Parameters

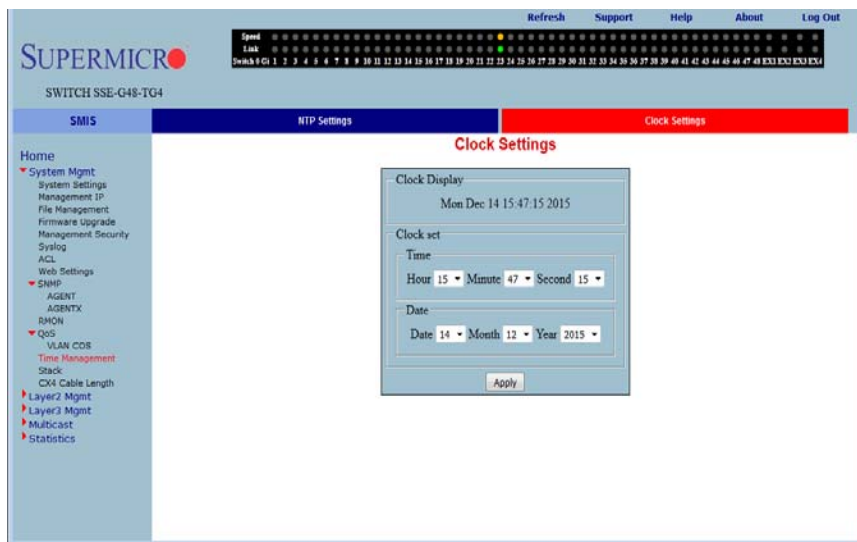
Parameter	Description
NTP Client Settings	
NTP Status	This field enables or disables NTP in the switch, and allows you to configure the NTP Servers section to enable NTP.

Table 5-33. NTP Settings Page Parameters (Continued)

Parameter	Description
Receive Server Update	The value for this parameter could be <i>Broadcast</i> or <i>Unicast</i> . To process the broadcast NTP updates from the server, choose the <i>Broadcast</i> option.
Timezone Settings	
Hour Offset	This parameter allows you to enter an hour offset from GMT for local time.
Minutes Offset	This parameter allows you to enter a minutes offset (after hour offset) from GMT for local time.
NTP Servers	
Server IP Address	Use this parameter to enter the NTP server IP address.
Key	Choose the key from the configured list. These keys are configurable in this page in the NTP Server Keys section's fields.
Preferred	This parameter allows you to choose the preferred server. Choose <i>Yes</i> if this server needs to be preferred over other configured NTP servers. You can add multiple NTP servers.
NTP Servers Keys	
Key ID	Use this parameter to select a number to identify the configured key strings.
Key String	Use this parameter to specify any string to be used as a key to handshake with NTP servers.

Clock Settings

Figure 5-41. Clock Settings Page



Clicking the CLOCK SETTINGS link brings up the CLOCK SETTINGS page (Figure 5-41), which allows to configure the Time and Date in the switch. The parameters for this page are shown in Table 5-34.

Table 5-34. NTP Settings Page Parameters

Parameter	Description
Clock Display	This display shows the time and date that the switch current has.
Clock Set	These controls allow you to set or modify the time and date. HH:MM:SS for the Time, and DD:MM::YYYY for the date.

Stack

The Supermicro Intelligent switch supports stacking of the SSE-G24-TG4 and SSE-G48-TG4 Supermicro switch units. Switch stacking is created by connecting switches in a daisy chain. One of the stacked switches is selected as a Master based on its configurations. The Master switch provides management support for the whole stack. Other switches in the stack are referred to as slave switches.

NOTE: Make sure all stacked switches are running the same version of firmware.

The Master switch manages the control plane traffic for all stacked switches. When the current master switch fails, the backup master is then selected as the current master. The Master selection algorithm is based on a priority configuration. If two switches have the same priority, the switch with the lowest MAC address is selected as the Master switch.

Enabling Stacking

By default, Supermicro switches act as stand-alone switches. This stand-alone default facilitates using 10G Ethernet ports as Extreme Ethernet ports for uplinks.

When stacking is enabled the stacking ports are dedicated for stacking purposes. Stacking can be enabled using the command `stack` with the switch identifier and priority. The detailed command syntax is explained below.

NOTE: When stacking is enabled, the switch needs to be rebooted to make it effective.

NOTE: When a switch is acting as a stand-alone switch with stacking disabled, all physical interfaces are numbered as 0/1 to 0/n. When the switch is in stacking mode, the interfaces are numbered as <switch id>/1 to <switch id> / n. In non-stacking mode, the switch ID is considered to be 0.

The interface numbers change between stacking and non-stacking cases due to the switch ID. So configurations saved for stacking are not valid for non-stacking cases and vice versa.

NOTE: If you choose stacking using the `stack` command from a non-stacking case, and the configurations are already saved for restoring the switch, it will rename the configuration file by adding a suffix `_nonstack` and will not restore this file when the switch reboots with stacking enabled.

Similarly if you choose non-stacking using the `no stack` command from the stacking case, and the configurations are already saved for restoring the switch, it will rename the configuration file by adding a suffix `_stack` and will not restore this file when the switch reboots with stacking disabled.

Adding Stacking Members

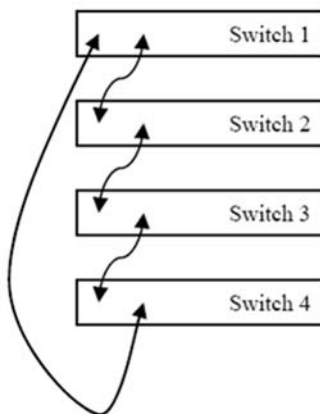
Connect the stacked switches using stacking cables. For better redundancy, connect the switches daisy chained as shown in the diagram below (Figure 5-42). This chain connectivity helps to maintain stacking in case a single link or switch fails.

Before connecting switches in stacking, make sure stacking is enabled in all switches and that the switch identifier and priorities are all configured properly.

There is no other specific configuration required to add stacked switches. If two stacking-enabled switches connect through stacking cables, they form a stack.

NOTE: Do not use the same switch ID for multiple switches on the stack.

NOTE: Do not use the same switch ID for multiple switches on the stack.

Figure 5-42. Switch Diagram

NOTE: In a stack only one switch can be configured as master. Otherwise the slave switches will not allow you to configure anything except *stacking disabled*. To login to slave switches, use a login name as "**stackuser**" and password as "**stack123**".

Removing a stacked switch

To remove a switch from stacking follow the below recommended procedure:

1. Disconnect stacking cables.
2. Reboot the removed switch as a standalone switch.
3. *Disable* stacking.
4. Reboot the switch again to operate as regular stand-alone switch.

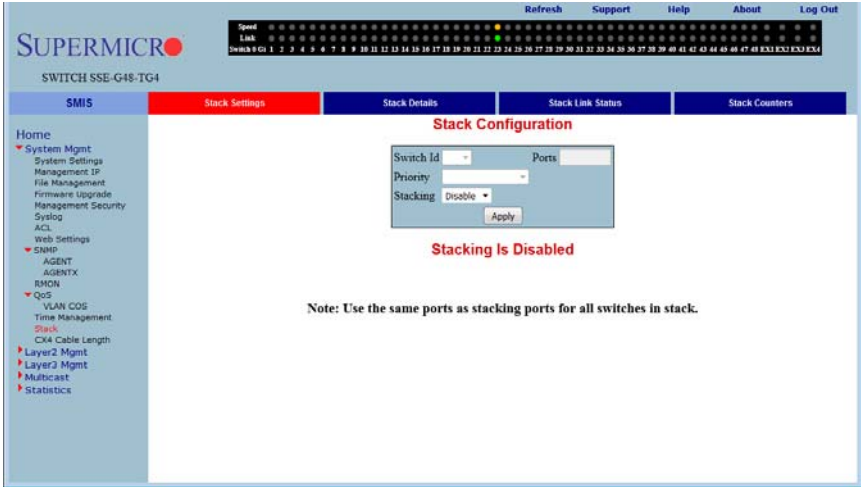
NOTE: When a switch is moved from stacking to stand-alone mode, the saved stacking configurations can not be loaded in stand-alone mode. When stacking is disabled, the switch software renames the existing configuration file to avoid automatic restoration of stacking configurations on a stand-alone switch.

The following pages are available for configuring Stack settings;

- [Stack Settings](#)
- [Stack Details](#)
- [Stack Link Status](#)
- [Stack Counters](#)

Stack Settings

Figure 5-43. Stack Configuration Page



Clicking the STACK SETTINGS tab brings up the STACK CONFIGURATION page (Figure 5-43), which configures the stacking feature. The parameters for this page are shown in Table 5-35.

Table 5-35. Stack Configuration Page Parameters

Parameter	Description
Switch ID	This parameter defines a switch identifier number for this switch. This identifier should be unique in the stack, since the number is used in referring all physical interfaces available in this switch. So for example, if this parameter is chosen as 2, the physical interfaces will be referred as <i>Gi2/1</i> , <i>Gi2/1</i> and so on. For non-stacking, stand-alone cases this switch ID is considered as zero.
Ports	Number of stacking ports. Users can choose based on their preferred stacking configuration and available XG ports. Stacking allowed ports are xg2 or xg3
Priority	This parameter chooses the priority for this switch in the Stacking Master selection. It could be configured as <i>Preferred Master</i> , <i>Backup Master</i> or <i>Preferred Slave</i> .
Stacking	This parameter enables or disables stacking. NOTE: Any change in stacking status requires a reboot of the switch.

Stack Details

Figure 5-44. Stack Details Page

The screenshot shows the SUPERMICR web interface for a SWITCH SEM-GEM-X2C. The 'Stack Details' tab is selected. The page displays the following information:

Self Status

Stack Ports	Switch Id	Stack Ip	Stack MAC	Configured State	Current State
1	1	169.254.1.1	00:00:00:09	PM	Master

Peer Status

Switch Id	Stack Ip	Stack MAC	Switch State	Card Name
-----------	----------	-----------	--------------	-----------

Clicking the STACK DETAILS tab brings up the STACK DETAILS page (Figure 5-44), which displays stacking details. The parameters for this page are shown in Table 5-36.

Table 5-36. Stack Details Page Parameters

Parameter	Description
Self Status	
Stack Ports	This is the number of stacking ports configured in this switch.
Switch ID	This parameter is used to specify the switch identifier of this switch.
Stack IP	This parameter is used to specify the IP address of this switch. This IP address is used to communicate between stack member switches.
Stack MAC	This parameter is used to specify the MAC address of this switch. This MAC address is used to communicate between stack member switches.
Configured State	This parameter is used to specify the priority of this switch.
Current State	This parameter is used to specify the current status of this switch as <i>Master</i> or <i>Slave</i> .
Peer Status – The following parameters display information about all connected stack Slave switches.	
Switch ID	This parameter is used to specify the switch identifier of the Slave switch.
Stack IP	This parameter is used to specify the IP address of the Slave switch. This IP address is used to communicate between stack member switches.

Table 5-36. Stack Details Page Parameters (Continued)

Parameter	Description
Stack MAC	This parameter is used to specify the MAC address of the Slave switch. This MAC address is used to communicate between stack member switches.
Switch State	This parameter is used to specify the current status of the Slave switch.
Card Name	This parameter is used to specify the type of Slave switch.

Stack Link Status

Figure 5-45. Stack Link Status Page



Clicking the STACK LINK STATUS tab brings up the STACK LINK STATUS page (Figure 5-45), which displays stacking link status. The parameters for this page are shown in Table 5-37.

Table 5-37. Stack Link Status Page Parameters

Parameter	Description
Port	This parameter displays the stacking ports of the module configured in this switch.
Status	This shows the status of stacking ports as either Up or Down.

Stack Counters

Figure 5-46. Stack Counter Details Page

The screenshot shows the SUPERMICR web management utility interface. The top navigation bar includes 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. The main navigation menu on the left lists various system and network management options, with 'Stack Counters' highlighted in red. The main content area displays the 'Stack Counter Details' page, which contains two tables of statistics for port 1.

Port	InOctet	InUcast	InDiscard	InErrors	InHCOctet
1	0	0	0	0	0

Port	OutOctet	OutUcast	OutDiscard	OutErrors	OutHCOctet
1	0	0	0	0	0

Clicking the STACK COUNTERS tab brings up the STACK COUNTERS DETAILS page (Figure 5-46), which displays statistics for stacking ports. The parameters for this page are shown in Table 5-38.

Table 5-38. Stack Counter Details Page Parameters

Parameter	Description
Port	This parameter displays the stacking port identifier.
Received Statistics	
InOctet	This parameter displays the number of bytes received.
InUcast	This parameter displays the number of unicast packets received.
InDiscard	This parameter displays the number of received packets that were discarded.
InErrors	This parameter displays the number of packets received with errors.
InHCOctet ^a	This parameter displays the number of bytes received with HC.
Transmit Statistics	
OutOctet	This parameter displays the number of bytes transmitted.
OutUcast	This parameter displays the number of unicast packets transmitted.
OutDiscard	This parameter displays the number of packets discarded in transmission.
OutErrors	This parameter displays the number of packets transmitted got errors.
OutHCOctet ^a	This parameter displays the number of bytes transmitted with HC.

- a. HC refers to the High Capacity of the counter used. The regular counter is 32-bit, whereas the HC counter is 64-bit.

CX4 Cable Length

Stacking is supported with Supermicro CX-4 cables only. The CX-4 cable used for stacking should be no more than 3-meters in length, because stacking internally runs at 12-Gbps and therefore requires a more robust signal than longer cable lengths might provide reliably. The industry standard stacking cable length is 3-meters.

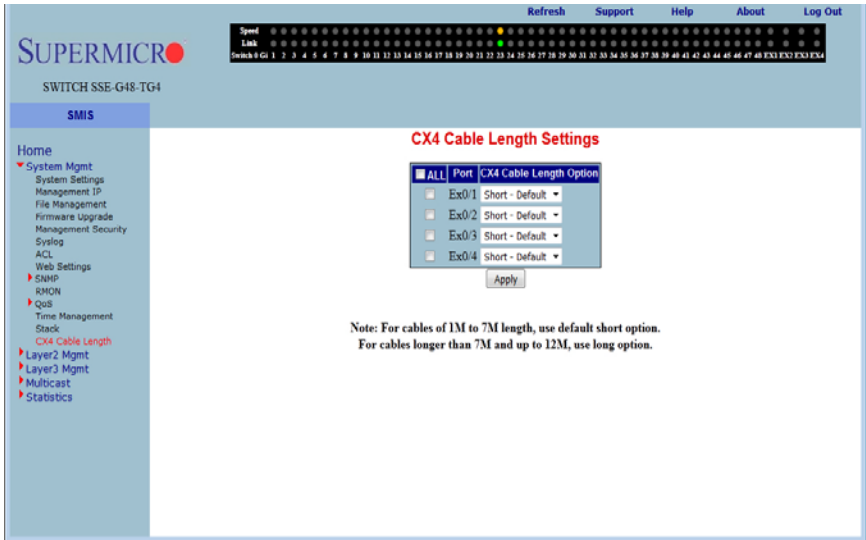
NOTE: For stacking ports, you do not need to configure CX4 cable length. It is fixed as "short" for stacking ports.

NOTE: Using any CX4 cable other than one from Supermicro may give unreliable performance and is not supported. Use CBL-0474L for 1-meter connections or CBL-0389L-01 for 3-meter connections

When used for 10G Ethernet uplinks, the CX-4 ports can be from 1-meter to 12-meters in length; the maximum CX-4 cable length supported on Supermicro switches is 12-meters.

It is acceptable to use a 1-meter stacking cable for port 1 and a 12-meter uplink cable for port 2. You will only need to configure the long cable preference for port 2. Do this by selecting the Port Number in the CX4 CABLE LENGTH screen (Figure 5-47) and then selecting the "long" option.

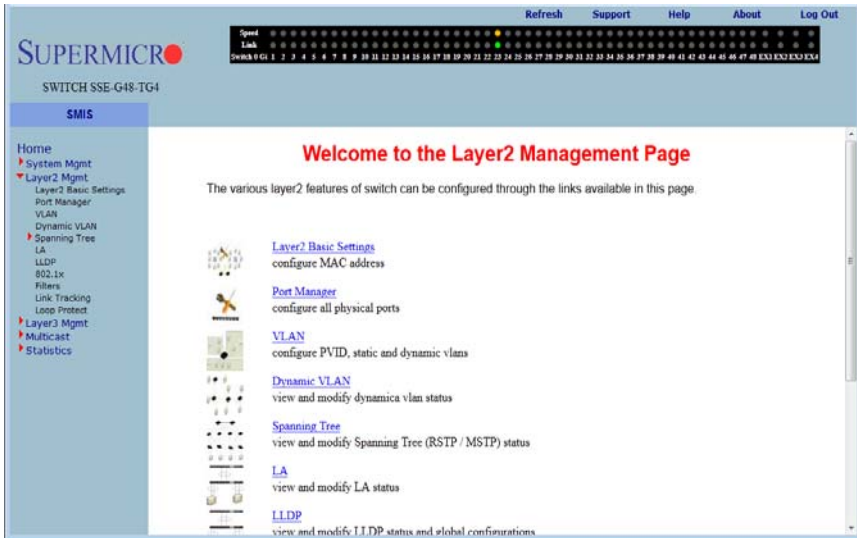
Figure 5-47. Configuring CX4 Cable Length



This configuration is done on an individual port basis. Thus, you can use *short* for one port and *long* for the other port. Alternatively you might use both *short* or, if neither are for stacking, both can be *long* cables.

5-5 Layer 2 Management

Figure 5-48. Layer2 Management Page

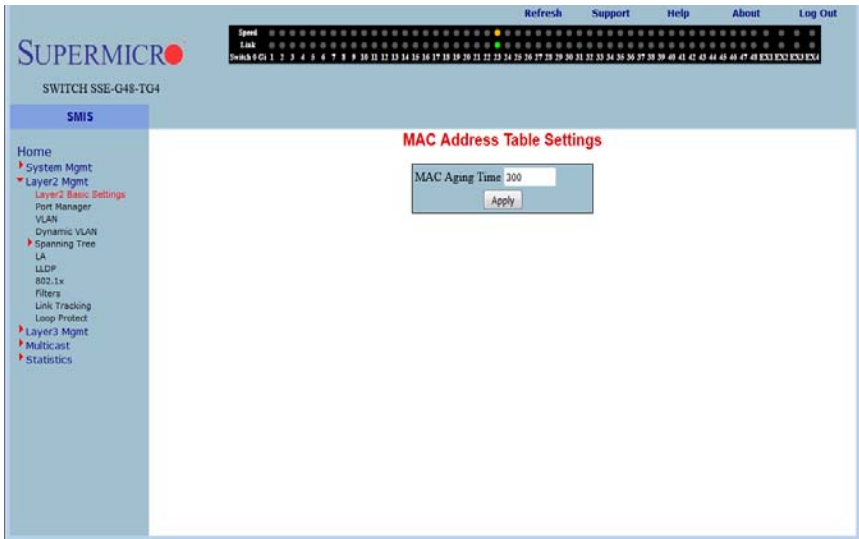


The LAYER2 MANAGEMENT page (Figure 5-48) contains the following links for Layer2 controls:

- [Layer 2 Basic Settings](#)
- [Port Manager](#)
- [VLAN](#)
- [Dynamic VLAN](#)
- [RSTP](#)
- [MSTP](#)
- [Link Aggregation \(LA\)](#)
- [802.1x](#)
- [Filters](#)
- [Link Tracking](#)
- [Loop Protect](#)

Layer 2 Basic Settings

Figure 5-49. MAC Address Table Settings Page



Clicking the LAYER2 BASIC SETTINGS link brings up the MAC ADDRESS TABLE SETTINGS page (Figure 5-49), which gives you the option to change MAC aging time. MAC address confirmation can be done with this time interval.

Port Manager

The PORT MANAGER link has links to the following web pages:

- [Basic Settings](#)
- [Port Monitoring](#)
- [Port Control](#)
- [Storm Control/Rate Limiting](#)
- [Protected Ports](#)

NOTE: In all port based configuration pages, the port number group links are provided on the top.

In the normal standalone operation of the switch, there is only one link and the corresponding port configuration is displayed below it.

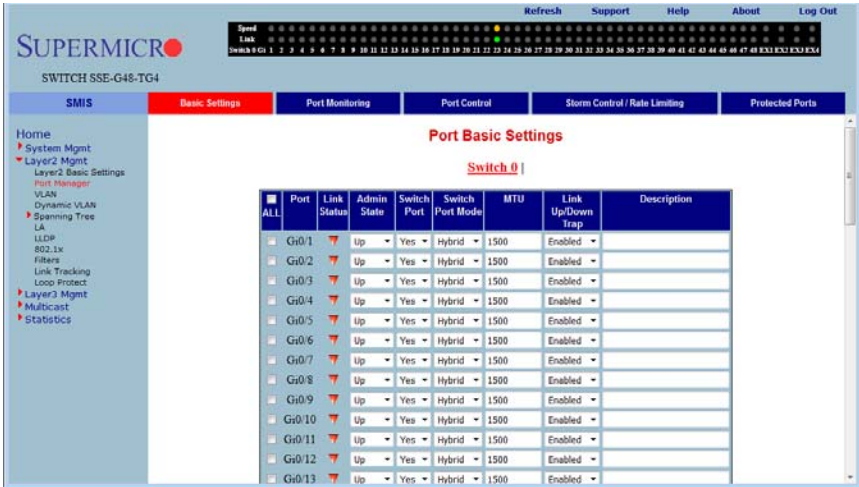
In case of stacking, multiple groups of port links are displayed. These links provide the configuration of ports from different stack member switches. To view the configuration of ports from a particular stack member switch, select the corresponding port links. For example, if three switches having switch identifier as 1, 2, and 3 are stacked together, the links will be as follows.

Gi1/1-Ex1/2 | Gi2/1-Ex2/2 | Gi3/1-Ex3/2

So to view the ports of switch 2, you need to select the Gi2/1-Ex2/2 link.

Basic Settings

Figure 5-50. Port Basic Settings Page



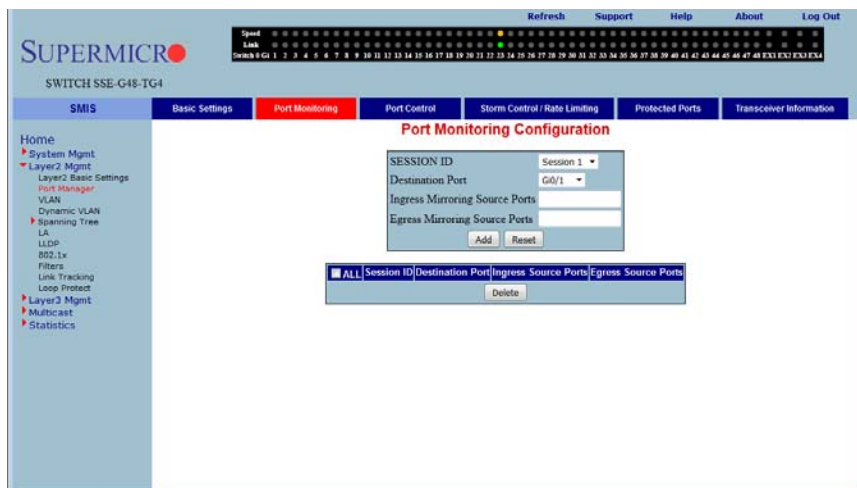
Clicking the BASIC SETTINGS tab brings up the PORT BASIC SETTINGS page (Figure 5-50), which allows you to configure port status and mode information. This page also helps configuring priority and MTU. The parameters for this page are shown in Table 5-39.

Table 5-39. Port Basic Settings Page Parameters

Parameter	Description
Port	This displays the port number.
Link status	This column shows the physical link status as an UP or Down arrow. A green up arrow indicates that the status of the port is up, while the red down arrow indicates that the status of the port is down.
Admin State	This parameter allows you to administratively configure the Admin state as <i>Up</i> or <i>Down</i> .
Default User Priority	This parameter allows you to set the priority from 0 to 7.
Switch Port	By default, all ports are switch ports for layer 2 switching. To configure a port as a layer 3 routed port, choose <i>No</i> .
Switch Port Mode	Using this control allows you to set the access mode as either <i>Trunk</i> or <i>Hybrid</i> .
MTU	This sets the MTU value. The Minimum is 1500 and the Maximum is 9216. A port must be administratively down to change the MTU. Jumbo frames of up to 9210 bytes are supported on 1G and 10G links.
Link Up/Down Trap	This parameter enables or disables SNMP trap generation for port up and down events.
Description	The user can specify a description for each port.

Port Monitoring

Figure 5-51. Port Monitoring Configuration Page



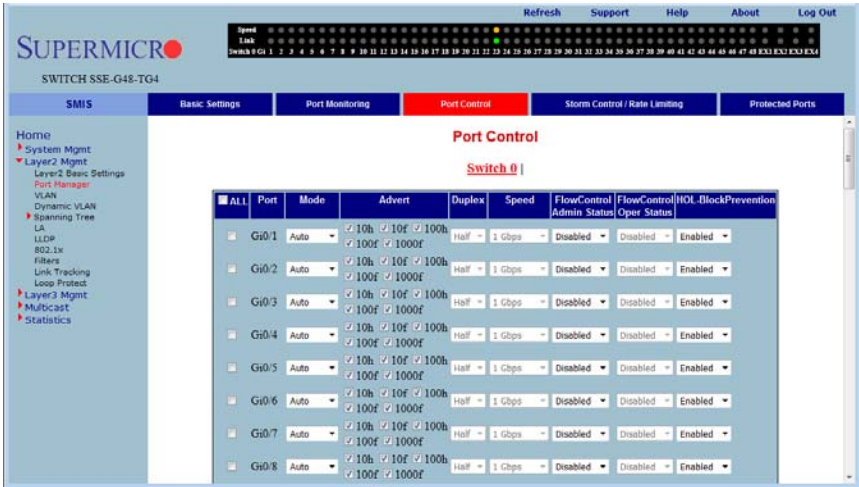
Clicking the PORT MONITORING tab brings up the PORT MONITORING CONFIGURATION page (Figure 5-51), which allows you to enable or disable monitoring on port interface. The parameters for this page are shown in Table 5-40.

Table 5-40. Port Monitoring Configuration Page Parameters

Parameter	Description
Status	This parameter enables or disables the port monitoring.
Port	This displays the port number.
Destination Interface	This parameter allows you to select the port number for the Destination.
Source Interface	This parameter allows you to select the port number for the Source.
Receive Monitoring	This parameter enables or disables the receive monitoring.
Transmit Monitoring	This parameter enables or disables the transmit monitoring.

Port Control

Figure 5-52. Port Control Page



Clicking the PORT CONTROL tab brings up the PORT CONTROL page (Figure 5-52), which allows you to change port parameters for ports that you select by clicking on the check box in front of them (or checking ALL to select all ports). The parameters for this page are shown in Table 5-41.

Table 5-41. Port Control Page Parameters

Parameter	Description
Mode	This parameter allows you to select either <i>Auto</i> or <i>NoNegot</i> for your port mode.
Advert	For each selected port you may choose to click on a check box for <i>10h</i> , <i>10f</i> , <i>100h</i> , <i>100f</i> or <i>1000f</i> Advert options.
Duplex	This parameter allows you to select either <i>Half</i> or <i>Full</i> options for Duplex if you have already selected <i>NoNegot</i> for the Mode option. This option is unavailable if the Auto mode option was selected.
Speed	This parameter allows you to select either <i>1 Gbps</i> , <i>10 Mbps</i> or <i>100 Mbps</i> options for port speed if you have already selected <i>NoNegot</i> for the Mode option. This option is unavailable if the Auto mode option was selected.
FlowControl Admin Status	This parameter allows you to select either <i>Disabled</i> , <i>Transmit</i> , <i>Receive</i> or <i>Both</i> options for Flow Control Admin Status.
FlowControl Oper Status	This parameter only provides information on what the Flow Control Oper Status is and is not configurable on this page.
HOL-Block Prevention	This parameter allows you to select either <i>Enabled</i> or <i>Disabled</i> options for HOL-Block Prevention for the port.

Storm Control/Rate Limiting

Figure 5-53. Storm Control/Rate Limiting Page

The screenshot shows the SUPERMICR web interface for a SWITCH SSE-G48-TG4. The 'Storm Control / Rate Limiting' tab is selected. The page title is 'Storm Control / Rate Limiting' and it is for 'Switch 0'. A table lists 13 ports (Gt0-1 to Gt0-13) with the following parameters:

ALL	Port	Storm Control			Egress Rate Limit	
		DLF Level pps	Broadcast Level pps	Multicast Level pps	Egress Port Rate Limit Kbps	Port Burst Size Kbits
<input type="checkbox"/>	Gt0-1	0	0	0	0	0
<input type="checkbox"/>	Gt0-2	0	0	0	0	0
<input type="checkbox"/>	Gt0-3	0	0	0	0	0
<input type="checkbox"/>	Gt0-4	0	0	0	0	0
<input type="checkbox"/>	Gt0-5	0	0	0	0	0
<input type="checkbox"/>	Gt0-6	0	0	0	0	0
<input type="checkbox"/>	Gt0-7	0	0	0	0	0
<input type="checkbox"/>	Gt0-8	0	0	0	0	0
<input type="checkbox"/>	Gt0-9	0	0	0	0	0
<input type="checkbox"/>	Gt0-10	0	0	0	0	0
<input type="checkbox"/>	Gt0-11	0	0	0	0	0
<input type="checkbox"/>	Gt0-12	0	0	0	0	0
<input type="checkbox"/>	Gt0-13	0	0	0	0	0

Clicking the STORM CONTROL/RATE LIMITING tab brings up the STORM CONTROL/RATE LIMITING page (Figure 5-53), which allows you to configure specific parameters of the port. You can choose between *Auto-negotiation* and *No-negotiation* for a port. If *No-negotiation* is chosen, then the speed of the link, FlowControl and duplex modes can be configured. The parameters for this page are shown in Table 5-42.

Table 5-42. Storm Control/Rate Limiting Page Parameters

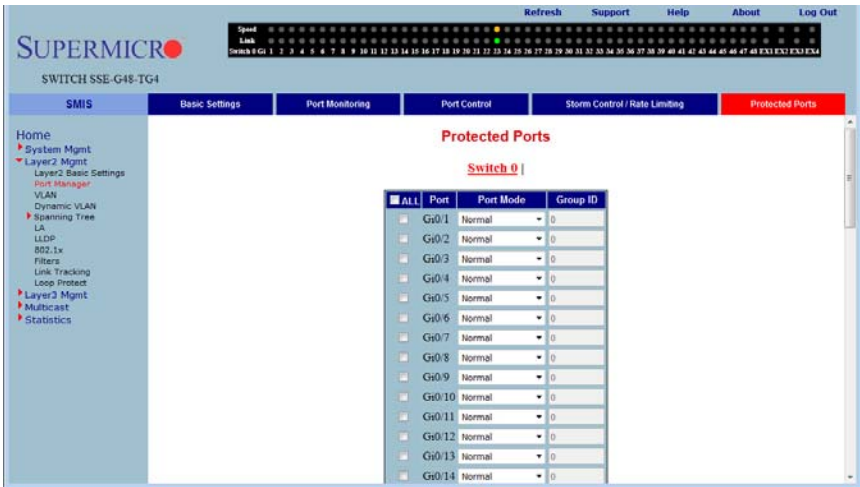
Parameter	Description
Port	This parameter displays the port number.
Mode	This parameter allows you to select either <i>Auto Negotiation</i> or <i>No-negotiation</i> .
Duplex	This parameter allows you to select either <i>Full Duplex</i> or <i>Half Duplex</i> .
Speed	This parameter allows you to select the speed as <i>10 Mbps</i> , <i>100 Mbps</i> or <i>1 Gb/s</i> .
Flow Control Admin Status	This parameter allows you to specify the Flow Control Admin Status as either <i>Disabled</i> , <i>Trasmit Flow Control Enabled</i> , <i>Receive Flow Control Enabled</i> or both <i>Transmit and Receive Flow Control Enabled</i> .
Flow Control Operation Status	This parameter displays the status of the flow control.
HOL Block Prevention	This parameter allows you to enable or disable Head of Line block prevention.
The following parameters are configurable for Ingress Rate Limiting.	
DLF Level	This parameter allows you to specify the destination lookup failure packets per second.
Broadcast Level	This parameter allows you to specify the broadcast packets per second.

Table 5-42. Storm Control/Rate Limiting Page Parameters (Continued)

Parameter	Description
Multicast Level	This parameter allows you to specify the multicast packets per second.
The following parameters are configurable for Egress Rate Limiting.	
Egress Port Rate Limit	This parameter allows you to specify the egress limit of packets per second.
Egress Port Burst Size	This parameter allows you to specify the egress limit of packet burst size.

Protected Ports

Figure 5-54. Protected Ports Page



Clicking on the Protected Ports tab brings up the PROTECTED PORTS page (Figure 5-54). The PROTECTED PORTS page allows configuration of the port specific protected parameters. You can choose between non-protected or protected for a port. If you choose a protected port, it can be a standalone or a single group member. The parameters for this page are shown in Table 5-43.

Table 5-43. Protected Ports Page Parameters

Parameter	Description
Port	Port number.
Port Mode	This helps to configure the mode as Normal or Protected port or Protected Group.
Group ID	Choose the group identifier. This is enabled only in the Protected Group mode. 0 means the standalone protected port.

VLAN

The VLAN link allows to configure the VLAN information. VLAN configuration information has been provided in the following pages:

- [Basic Settings](#)
- [Port Settings](#)
- [Static VLANs](#)
- [Protocol Group](#)
- [Port Protocol](#)
- [MAC VLAN](#)
- [Wildcard](#)

Basic Settings

Figure 5-55. VLAN Basic Settings Page

The screenshot shows the 'VLAN Basic Settings' page in the SUPERMICRO web management utility. The page title is 'VLAN Basic Settings'. Below the title is a table with the following parameters:

Garp System Control	MAC Based On All Ports	Port and Protocol Based On All Ports	Dynamic Vlan Status	Dynamic Multicast Oper Status	Maximum VLAN ID	Maximum Supported VLANs	Number of VLANs in the System
Start	Disabled	Enabled	Disabled	Disabled	4069	1024	1

Below the table is an 'Apply' button. A note at the bottom of the page reads: 'Note : To Shutdown GARP, Dynamic Vlan & Dynamic Multicast should be disabled.'

Clicking the BASIC SETTINGS tab brings up the VLAN BASIC SETTINGS page (Figure 5-55), which displays VLAN global configuration information. The parameters for this page are shown in Table 5-44.

Table 5-44. VLAN Basic Settings Page Parameters

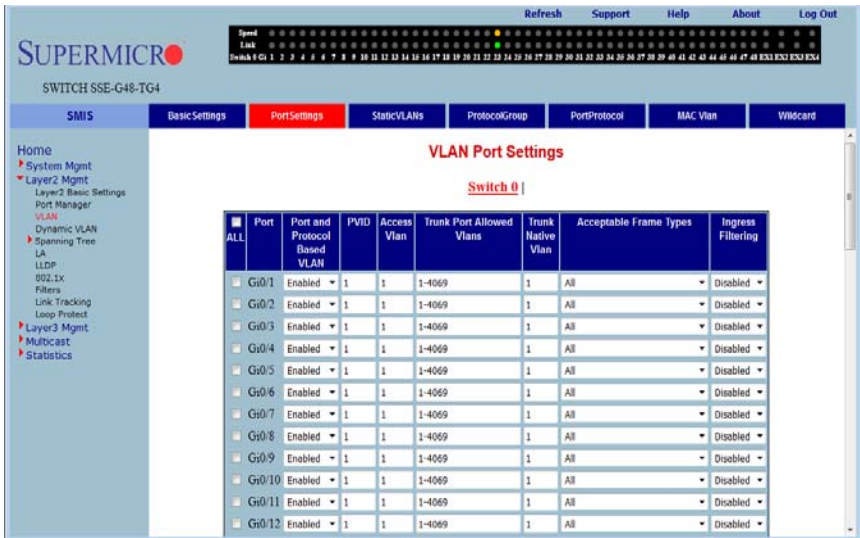
Parameter	Description
Garp System Control	This parameter starts or shuts down GARP in the switch.
Learning Mode	This parameter specifies the Learning Mode (<i>Independent, Shared, Hybrid</i> or <i>VLAN Learning</i>).

Table 5-44. VLAN Basic Settings Page Parameters (Continued)

Parameter	Description
MAC Based on All Ports	This parameter enables or disables the per Port MAC based classification.
Port and Protocol Based on all Ports	This parameter enables or disables the per Port Protocol based classification. The user can enable/disable per-port protocol based Classification. In addition, the Basic Settings page provides the configuration of Bridge Mode (Customer/ Provider) and Priority for tunneled STP BPDUs. When the user configures Bridge Mode to Provider , the Port Protocol based classification and MAC-based classification on all ports must be disabled.
Dynamic VLAN Oper Status	Use this setting to enable/disable VLAN operational status.
Dynamic Multicast Oper Status	Use this setting to enable/disable multicast operational status.
Maximum VLAN ID	This parameter specifies the largest (4069) valid VLAN ID, which this switch can accept, above which all will be discarded.
Maximum Supported VLANs	This parameter specifies the maximum number of VLANs that this device can scale.
Number of VLANs in the System	This parameter specifies the active number of VLANs configured in the device.

Port Settings

Figure 5-56. VLAN Port Settings Page



Clicking the PORT SETTINGS tab brings up the VLAN PORT SETTINGS page (Figure 5-56), which is used 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 ACCEPTABLE FRAME TYPES (accept *Tagged Frame Alone* or *All frames*).

The other configurations provided in this page are, enabling/disabling per Port MAC based classification and Port Protocol based classification, enabling/disabling of tunneling and enabling/disabling of STP BPDU Tunneling. To enable STP BPDU Tunneling on an interface, you must first enable tunneling on that interface. Users can configure the Access VLAN, Trunk port allowed VLANs and the Trunk Native VLAN.

Static VLANs

Figure 5-57. Static VLAN Configuration Page

The screenshot displays the 'Static VLAN Configuration' page. At the top, there is a status bar with 'Speed' and 'Link' indicators. Below that is a navigation menu with 'SMIS' selected. The main navigation tabs include 'Basic Settings', 'Port Settings', 'Static VLANs' (highlighted in red), 'Protocol Group', 'Port Protocol', 'MAC Vlan', and 'Wildcard'. The left sidebar shows a tree view with 'Home' expanded to 'Layer2 Mgmt', then 'VLAN', and 'Static VLAN' selected. The main content area has a title 'Static VLAN Configuration' and a form with fields for 'VLAN ID', 'VLAN Name', 'Tagged Ports', 'Untagged Ports', and 'Forbidden Ports', along with 'Add' and 'Reset' buttons. Below the form is a table with columns: 'ALL', 'VLAN ID', 'VLAN Name', 'Member Ports', 'Tagged Ports', 'Untagged Ports', and 'Forbidden Ports'. The table contains one entry for VLAN 1.

ALL	VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Forbidden Ports
<input checked="" type="checkbox"/>	1		Gi0/1-48, Ex0/1-4		Gi0/1-48, Ex0/1-4	

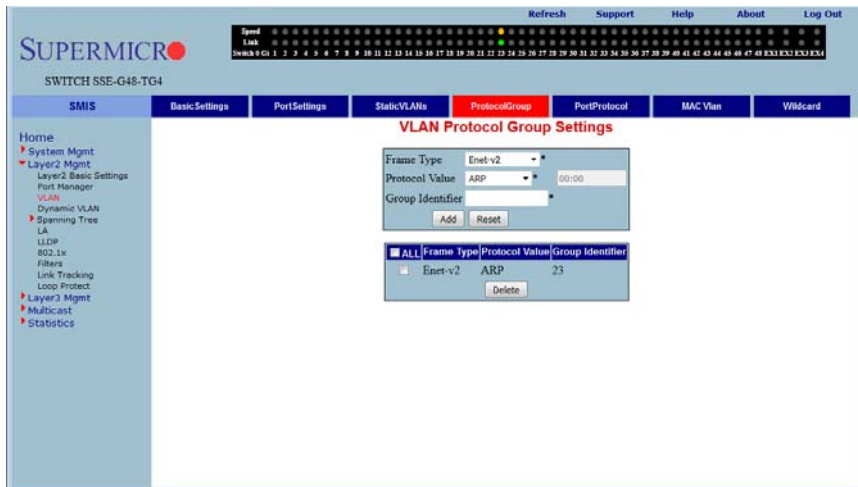
Clicking the STATIC VLANs tab brings up the STATIC VLAN CONFIGURATION page (Figure 5-57), which allows you to configure the VLAN related information statically.

Using the first table you can create new entries for uncreated VLANs. VLAN ID is the mandatory field in configuring a VLAN. You can also enter a VLAN NAME, TAGGED PORT LIST, UNTAGGED PORT and the FORBIDDEN PORTS for a VLAN.

The second table displays the VLAN configurations saved in the switch.

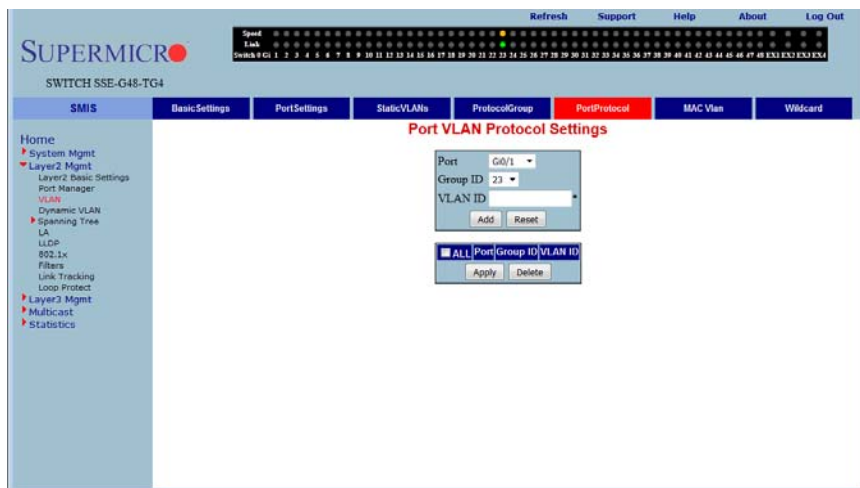
Protocol Group

Figure 5-58. VLAN Protocol Group Settings Page



Clicking the PROTOCOL GROUP tab brings up the VLAN PROTOCOL GROUP SETTINGS page (Figure 5-58), which is used to map Protocol Templates to Protocol Group Identifiers.

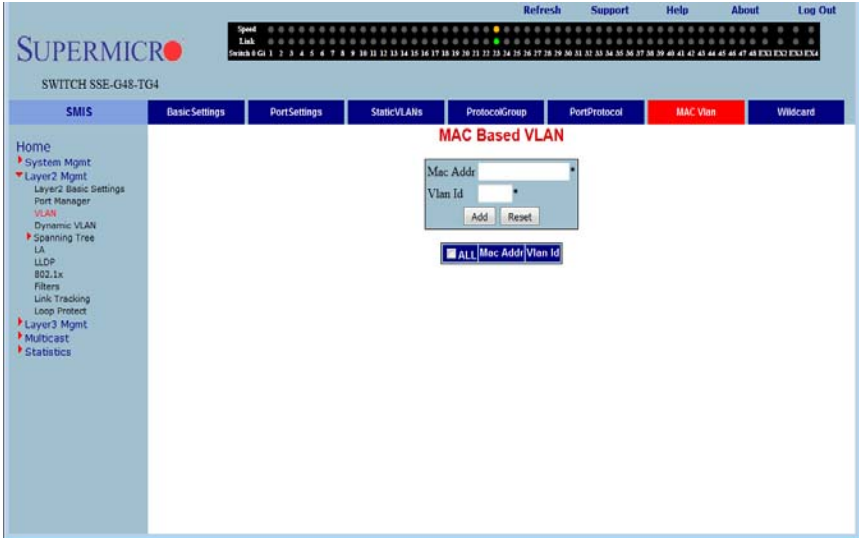
The FRAME TYPE gives you the data-link encapsulation format. The PROTOCOL VALUE is the value of the protocol in a protocol template. The GROUP ID represents a group of protocols that are associated together.

Port Protocol**Figure 5-59. Port VLAN Protocol Settings**

Clicking the Port PROTOCOL tab brings up the PORT VLAN PROTOCOL SETTINGS page (Figure 5-59), which displays a table used for Port and Protocol based VLAN classification. The GROUP ID designates a group of protocols in the Protocol Group Database. The VLAN ID is the ID associated with a group of protocols for each port.

MAC VLAN

Figure 5-60. MAC Based VLAN Settings Page



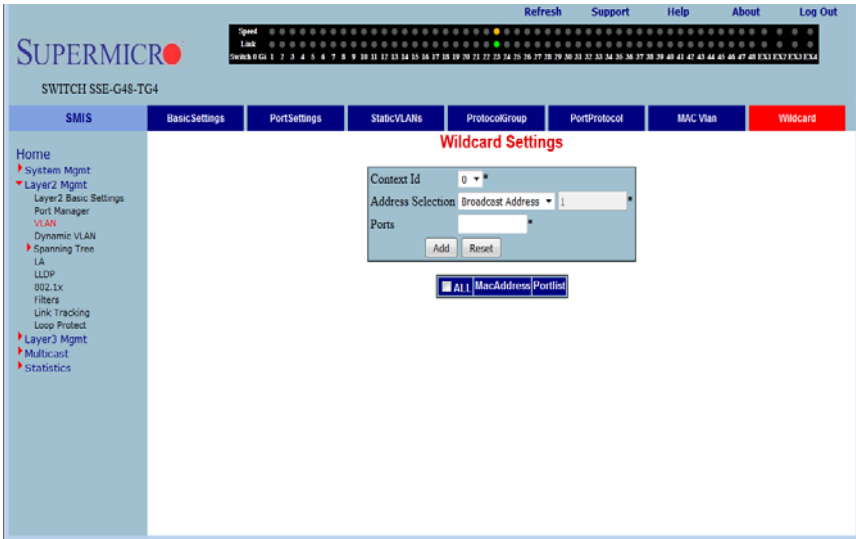
Clicking the MAC VLAN tab brings up the MAC BASED VLAN page (Figure 5-60), which allows you to add the MAC Address and Vlan ID to VLANs system. The parameters for this page are shown to you in Table 5-45.

Table 5-45. VLAN Port MAC Map Page Parameters

Parameter	Description
Mac Addr	This parameter allows you to enter MAC Address.
Vlan ID	This parameter allows you to manually enter the VLAN ID. The value ranges from 1 to 4069.

Wildcard

Figure 5-61. Wildcard Settings Page



Clicking the WILDCARD tab brings up the WILDCARD SETTINGS page (Figure 5-61), which configures wildcard MAC addresses and ports for VLANs. The parameters for this page are shown in Table 5-46.

Table 5-46. Wildcard Settings Page Parameters

Parameter	Description
Context ID	This parameter allows you to select the CONTENT ID.
Address Selection	Use this parameter to select the address type.
Ports	This parameter allows you to enter a port.

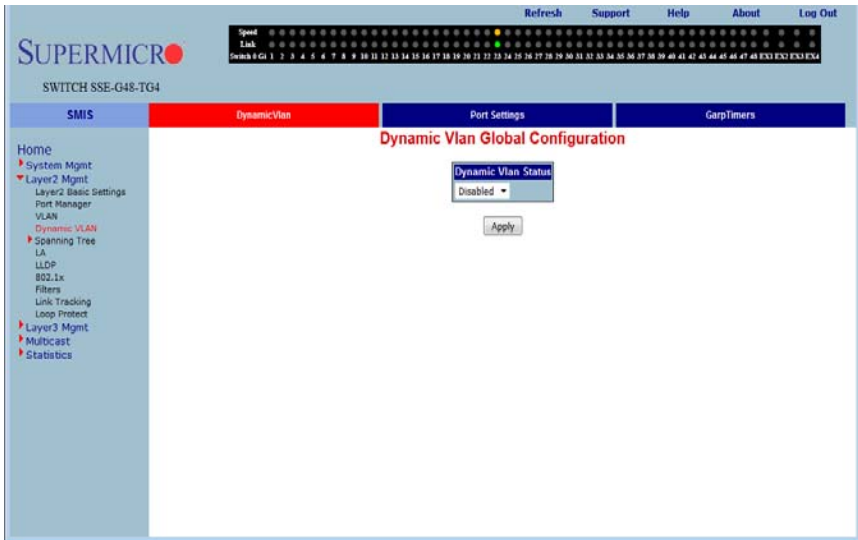
Dynamic VLAN

The Dynamic VLAN link allows you to configure the Dynamic VLAN information. Dynamic VLAN configuration information has been provided in the following pages

- [Dynamic VLAN](#)
- [Port Settings](#)
- [GARP Timers](#)

Dynamic VLAN

Figure 5-62. Dynamic VLAN Global Configuration Page



Clicking the DYNAMIC VLAN tab brings up the DYNAMIC VLAN GLOBAL CONFIGURATION page (Figure 5-62), which allows you to enable or disable Dynamic VLAN.

Port Settings

Figure 5-63. Dynamic VLAN Port Configuration Page

The screenshot shows the SUPERMICR web management interface for a SWITCH SSE-G48-TG4. The 'Port Settings' tab is active. The main content area displays the 'Dynamic Vlan Port Configuration' for 'Switch 0'. A table lists 14 ports (Gr0.1 to Gr0.14). Each port has a checkbox on the left, and two dropdown menus for 'Dynamic Vlan Status' and 'Restricted VLAN Registration', both currently set to 'Disabled'.

ALL	Port	Dynamic Vlan Status	Restricted VLAN Registration
<input type="checkbox"/>	Gr0.1	Disabled	Disabled
<input type="checkbox"/>	Gr0.2	Disabled	Disabled
<input type="checkbox"/>	Gr0.3	Disabled	Disabled
<input type="checkbox"/>	Gr0.4	Disabled	Disabled
<input type="checkbox"/>	Gr0.5	Disabled	Disabled
<input type="checkbox"/>	Gr0.6	Disabled	Disabled
<input type="checkbox"/>	Gr0.7	Disabled	Disabled
<input type="checkbox"/>	Gr0.8	Disabled	Disabled
<input type="checkbox"/>	Gr0.9	Disabled	Disabled
<input type="checkbox"/>	Gr0.10	Disabled	Disabled
<input type="checkbox"/>	Gr0.11	Disabled	Disabled
<input type="checkbox"/>	Gr0.12	Disabled	Disabled
<input type="checkbox"/>	Gr0.13	Disabled	Disabled
<input type="checkbox"/>	Gr0.14	Disabled	Disabled

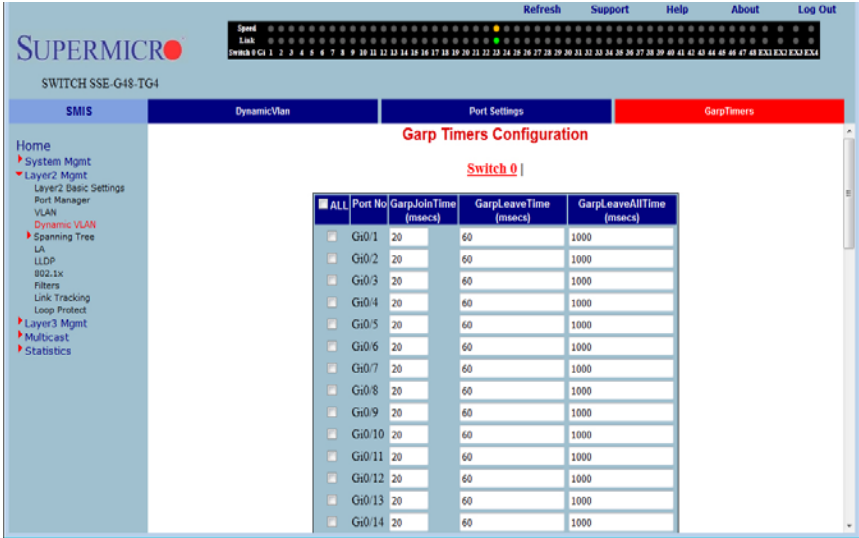
Clicking the PORT SETTINGS link brings up the DYNAMIC VLAN PORT CONFIGURATION page (Figure 5-63), which allows you to configure parameters for Dynamic VLAN ports. The parameters for this page are shown in Table 5-47.

Table 5-47. Dynamic VLAN Port Configuration Page Parameters

Parameter	Description
Port	This parameter displays the Port Number, which can be selected by the check box to the left of the column.
Dynamic VLAN Status	Use this parameter to enable/disable the DYNAMIC VLAN STATUS.
Restricted VLAN Registration	This parameter allows you to enable/disable RESTRICTED VLAN REGISTRATION.

GARP Timers

Figure 5-64. Garp Timers Configuration Page



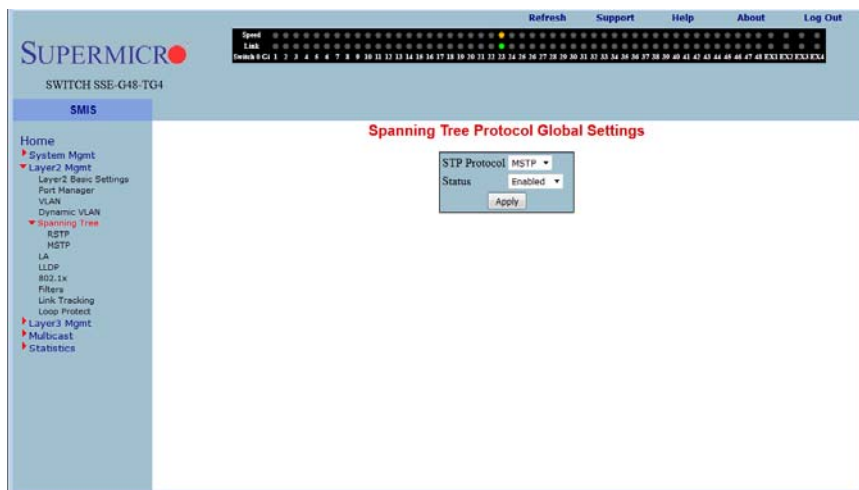
Clicking the GARP TIMERS tab brings up the GARP TIMERS CONFIGURATION page (Figure 5-64), which displays the various parameters for changing Garp times. The parameters for this page are shown in Table 5-48.

Table 5-48. Garp Timers Configuration Page Parameters

Parameter	Description
Port No	This parameter displays the Port Number.
Garp Join Time (msecs)	This parameter configures GARP join time in milli seconds. The value ranges from 1 to 1073741810. The default value is 200 milli seconds.
Garp Leave Time (msecs)	This parameter configures GARP leave time in milli seconds. The value ranges from 1 to 2147483630. The default value is 600 milli seconds.
Garp Leave All Time (msecs)	This parameter configures GARP leave all time in milli seconds. The value ranges from 1 to 2147483640. The default value is 10000 milli seconds.

Spanning Tree

Figure 5-65. Spanning Tree Protocol Global Settings Page



SPANNING TREE link brings up the SPANNING TREE PROTOCOL GLOBAL SETTINGS page (Figure 5-65), which supports configuration of RSTP or MSTP. The parameters for this page are shown in Table 5-49.

Table 5-49. Spanning Tree Protocol Global Settings Page

Parameter	Description
STP Protocol	This parameter modifies the protocol as either <i>RSTP</i> or <i>MSTP</i>
Status	This parameter <i>Enables</i> or <i>Disables</i> the spanning tree protocol status.

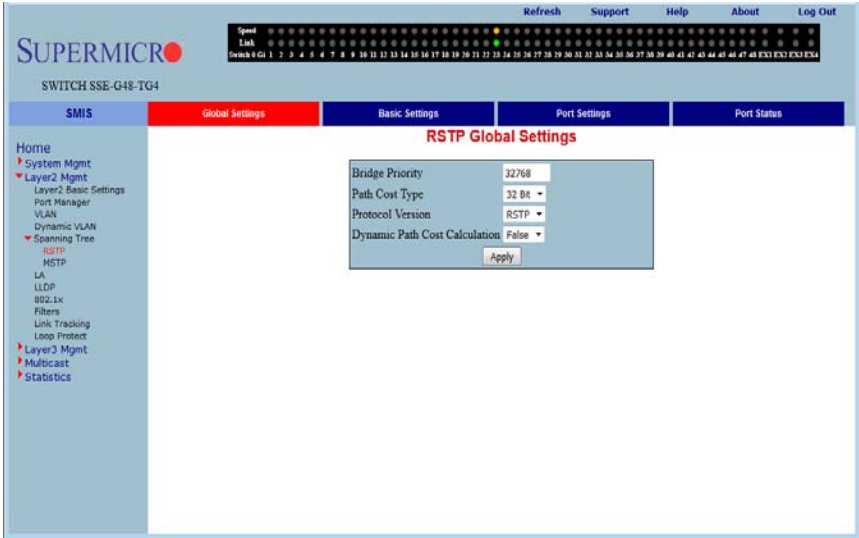
RSTP

The RSTP link provides links to the following configuration pages:

- [Global Settings](#)
- [Basic Settings](#)
- [Port Settings](#)
- [Port Status](#)

Global Settings

Figure 5-66. Global Configuration Page



Clicking the GLOBAL SETTINGS tab brings up the GLOBAL CONFIGURATION page (Figure 5-66), which allows you to configure RSTP global parameters. The parameters for this page are shown in Table 5-50.

Table 5-50. Global Configuration Page Parameters

Parameter	Description
Bridge Priority	This parameter specifies the Priority value assigned to the bridge that is used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768 .
Path Cost Type	This parameter allows configuration of the Path Cost Type to either <i>16 Bit</i> or <i>32 Bit</i> .
Protocol Version	This allows you to configure the Protocol Version as either <i>RSTP</i> or <i>MSTP</i> .
Dynamic Path Cost Calculation	This parameter allows you enable or disable the dynamic path cost calculation.

Basic Settings

Figure 5-67. RSTP Configuration Page

The screenshot shows the RSTP Configuration page with the following table:

Select	Context Id	Priority	Version	Tx Hold Count	Default Path Cost Type	Max Age	Hello Time	Forward Delay
0		32768	RSTP Compatible	6	32 Bit	20	2	15

Note : The following Relation should be observed
 $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Clicking the BASIC SETTINGS tab brings up the RSTP CONFIGURATION page (Figure 5-67), which displays the various parameters for RSTP configuration. The parameters for this page are shown in Table 5-51.

Table 5-51. RSTP Configuration Page Parameters

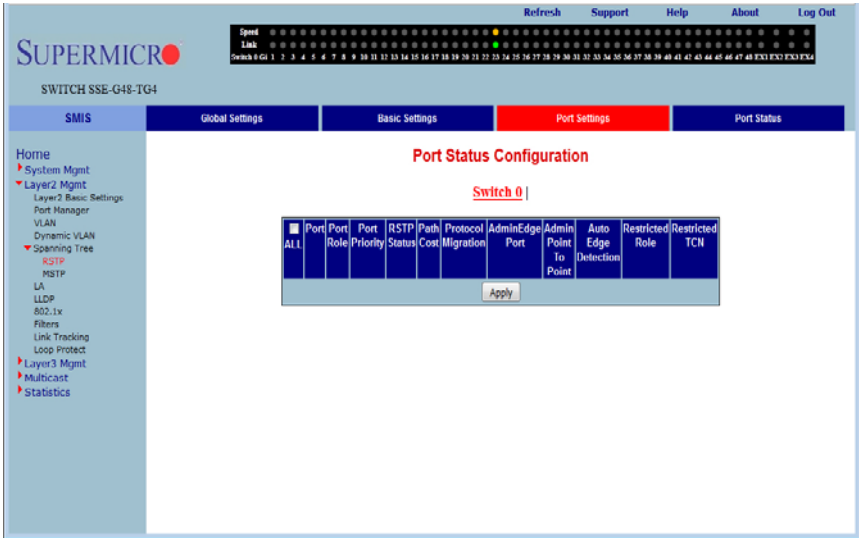
Parameter	Description
Select Control	This parameter allows you to select RSTP Global Settings to use in the switch.
Context ID	This parameter shows the unique ID of RSTP Global Settings.
Priority	This parameter specifies the Bridge priority, which can be used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768 .
Version	This parameter allows you to choose to run the protocol in <i>RSTP</i> or <i>STP</i> compatible version.
Tx Hold Count	This parameter specifies the maximum number of packets that can be sent in a given interval. This is configured to avoid flooding. Transmit hold count value may be from 1 to 10. The default value is 6.
Default Path Cost Type	This parameter allows you to configure the path cost either as a <i>16-bit</i> value or a <i>32-bit</i> value. This is provided mainly for backward compatibility with STAP.
Maximum Age (Seconds)	This specifies the time period for which the information received in the RSTP BDPDU is valid. The max age values from 6 to 40 seconds. The default value is 20 .

Table 5-51. RSTP Configuration Page Parameters (Continued)

Parameter	Description
Hello Time	This parameter specifies administrative value of hello time for the port. Hello time may be 1 or 2 seconds. The default value is 2.
Forward Delay	This parameter specifies how fast a port changes its spanning state when moving towards the Forwarding state. Forwarding time values from 4 to 30 seconds. The default value is 15.

Port Settings

Figure 5-68. Port Status Configuration Page



Clicking the PORT SETTINGS tab brings up the PORT STATUS CONFIGURATION page (Figure 5-68), which allows you to set the configuration per port related to RSTP. The parameters for this page are shown in Table 5-52.

Table 5-52. Port Status Configuration Page Parameters

Parameter	Description
Port	This parameter specifies the port identifier.
Port Role	This parameter enables or disables the RSTP protocol status on a particular port.
Port Priority	This parameter specifies the port priority used in role selection. Port priority values from 0 to 240. The default priority value is 128.
RSTP Status	This parameter specifies the RSTP protocol status that can be enabled/disabled on the particular port.

Table 5-52. Port Status Configuration Page Parameters (Continued)

Parameter	Description
Path Cost	This parameter specifies the path cost associated with this port. Path Cost values range from 0 to 200000000. The default path cost is calculated based on the port speed.
Protocol Migration	This parameter controls the migration from RSTP to STP, if the other side of the switch runs STP. The migration takes place only if this is Enabled.
AdminEdge Port	This parameter defines this port as an <i>Edge Port</i> or a <i>Non-edge Port</i> .
Admin Point-to-Point	This parameter allows you to configure ports explicitly as <i>Point-to-point</i> (Force true), <i>Non-point-to-point</i> or leave the decision to be made <i>Dynamically</i> (from the AL or MAC layer).
Auto Edge Detection	If this parameter is set to <i>True</i> , the edge port status is dynamically calculated.
Restricted Role	This parameter specifies the RESTRICTED ROLE status of the port.
Restricted TCN	This parameter indicates the RESTRICTED TCN status of the port.

Port Status

Figure 5-69. RSTP Port Status Page

The screenshot shows the RSTP Port Status page for Switch 0. The page has a navigation menu on the left with options like Home, System Mgmt, Layer2 Mgmt, Layer3 Mgmt, Multicast, and Statistics. The main content area displays a table of port configurations. The table has the following columns: Port, Designated Root, Designated Cost, Designated Bridge, Designated Port, Type, Role, and Port State. All ports listed (G0/1 to G0/15) have a Designated Cost of 0, a Designated Bridge of 00:00:00:00:00:00, and a Designated Port of 00:00. The Role for all ports is Disabled, and the Port State is Blocking.

Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
G0/1	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/2	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/3	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/4	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/5	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/6	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/7	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/8	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/9	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/10	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/11	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/12	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/13	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/14	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
G0/15	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking

Clicking the PORT STATUS tab brings up the RSTP PORT STATUS page (Figure 5-69), which displays RSTP port specific information. The parameters for this page are shown in Table 5-53.

Table 5-53. RSTP Port Status Page Parameters

Parameter	Description
Port	This parameter specifies the port identifier.
Designated Root	This parameter specifies the unique Bridge Identifier of the bridge that is recorded as the root for the segment to which the port is attached.
Designated Cost	This parameter specifies the path cost of the Designated Port of the segment connected to this port.
Designated Bridge	This parameter specifies the Bridge Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.
Designated Port	This parameter specifies the Port Identifier of the port on the Designated Bridge for this port's segment.
Type	This parameter specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a <i>Point-to-point</i> connection or <i>Shared Media</i> .
Role	This parameter specifies the port's current role as defined by the Spanning Tree Protocol.
Port State	This parameter specifies the port's current state as defined by application of the Spanning Tree Protocol.

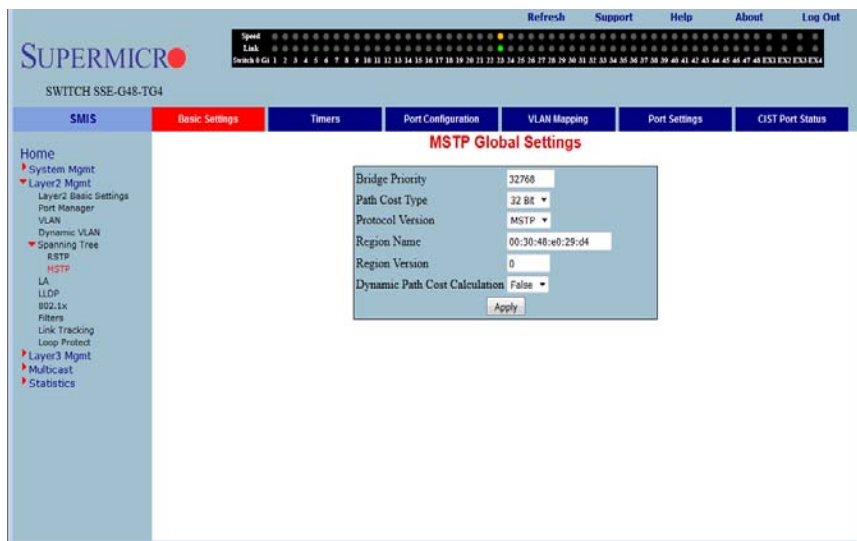
MSTP

The MSTP link leads you to the following configuration pages:

- [Basic Settings](#)
- [Timers](#)
- [Port Configuration](#)
- [VLAN Mapping](#)
- [Port Settings](#)
- [CIST Port Status](#)

Basic Settings

Figure 5-70. Global Configuration Page



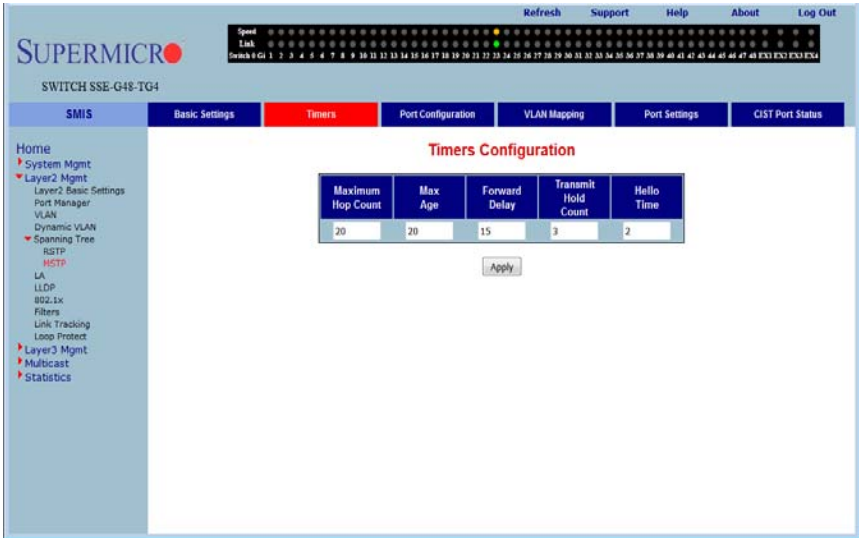
Clicking the BASIC SETTINGS tab brings up the GLOBAL CONFIGURATION page (Figure 5-70), which can access the MSTP global configuration. The parameters for this page are shown in Table 5-54.

Table 5-54. Global Configuration Page Parameters

Parameter	Description
Bridge Priority	This parameter specifies the Priority value assigned to the bridge that is used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768.
Path Cost Type	This parameter allows you to configure the path cost either as a 16-bit value or a 32-bit value. This is provided mainly for backward compatibility with STAP.
Protocol Version	This parameter specifies the protocol version number of the configuration to be used. You can choose to run the protocol in RSTP or MSTP.
Region Name	This parameter specifies the name for the Region's configuration. By default, the region name will be equal to the Bridge MAC Address.
Region Version	This parameter specifies the region version of the configuration to be used. The allowed value ranges from 0 to 65535. The default value is 0.
Dynamic Path Cost Calculation	This parameter allows you to enable or disable the Dynamic Path Cost Calculation.

Timers

Figure 5-71. Timers Configuration Page



Clicking the TIMERS tab brings up the TIMERS CONFIGURATION page (Figure 5-71), which configures the time for MAXIMUM HOP COUNT, FORWARD DELAY, MAXIMUM AGE, TRANSMIT HOLD AGE and HELLO TIME.

Port Configuration

Figure 5-72. CIST Settings Page

The screenshot shows the SUPERMICR web management utility interface. The main content area displays the 'CIST Settings' page for 'Switch 0'. The page features a table with columns for Port, Path Cost, Priority, PointToPoint Status, Edge Port, MSTP Status, Protocol Migration, Hello Time, AutoEdge Status, Restricted Role, and Restricted TCN. The table lists configurations for ports Gi0/1 through Gi0/13.

ALL	Port	Path Cost	Priority	PointToPoint Status	Edge Port	MSTP Status	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN
<input type="checkbox"/>	Gi0/1	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/2	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/3	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/4	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/5	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/6	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/7	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/8	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/9	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/10	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/11	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/12	20000	128	Auto	False	Enable	False	2	True	False	False
<input type="checkbox"/>	Gi0/13	20000	128	Auto	False	Enable	False	2	True	False	False

Clicking the PORT CONFIGURATION tab brings up the CIST SETTINGS page (Figure 5-72), which sets the configuration per Port related to MSTP. The parameters for this page are shown in Table 5-55.

Table 5-55. CIST Settings Page Parameters

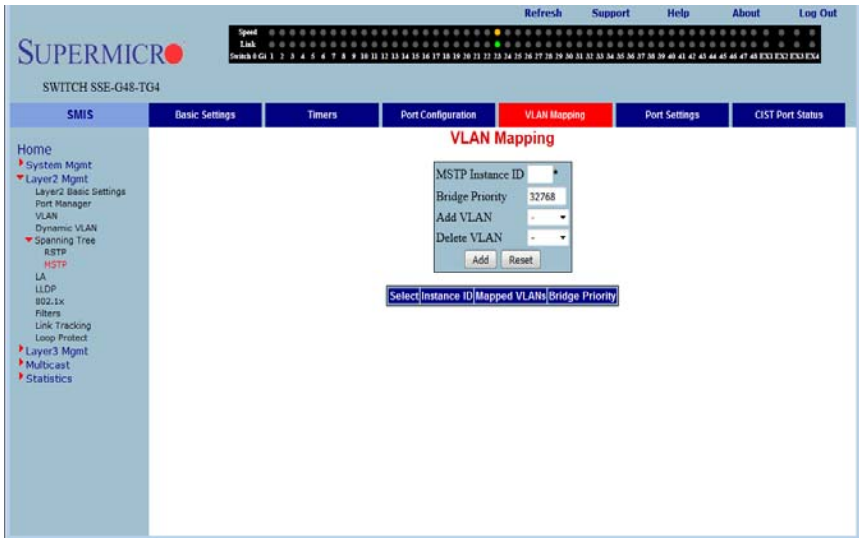
Parameter	Description
Port	This parameter specifies the port identifier.
MSTP Status	This parameter specifies the MSTP protocol status that can be enabled/disabled on the particular port.
Priority	This parameter specifies the port priority used in role selection.
Path Cost	This parameter specifies the path cost associated with this port.
Protocol Migration	This parameter controls 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 enabled.
Edge Status	This parameter must be configured if the corresponding port is an edge port.
Point-to-Point Status	This parameter allows you to configure the ports explicitly as point-to-point (<i>Force</i> true), as a non-point-to-point port, or leave the decision to be made dynamically (from the AL or MAC layer).
Hello Time (Seconds)	This parameter specifies the administrative value of Hello Time for the port.
Auto Edge Status	If set to <i>True</i> , the edge port status will be dynamically calculated.

Table 5-55. CIST Settings Page Parameters (Continued)

Parameter	Description
Restricted Role	This parameter specifies the Restricted role status of the port.
Restricted TCN	This parameter indicates the Restricted TCN status of the port.

VLAN Mapping

Figure 5-73. VLAN Mapping Page



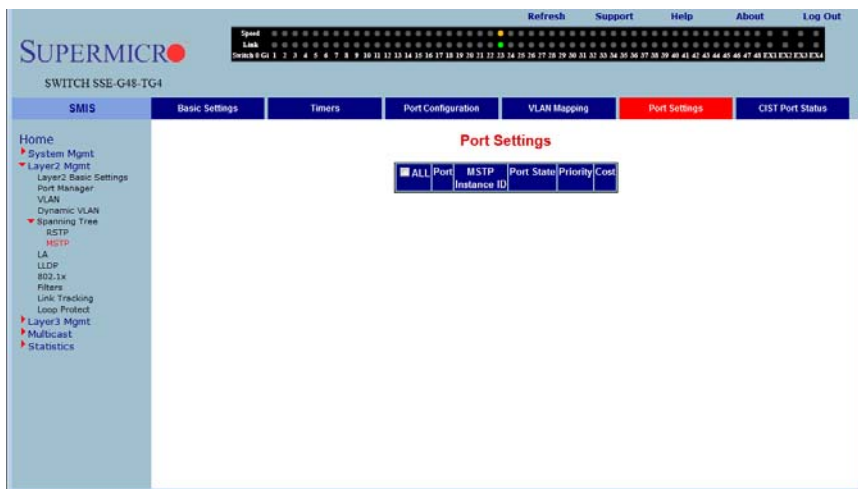
Clicking the VLAN MAPPING tab brings up the VLAN MAPPING page (Figure 5-73), whose table contains one entry for each instance of MSTP. The parameters for this page are shown in Table 5-56.

Table 5-56. VLAN Mapping Page Parameters

Parameter	Description
MSTP Instance ID	This parameter specifies the Instance ID, which is the index of the table. The allowed value ranges from 1 to 16.
Map VLAN	This parameter specifies the list of VLANs to be mapped to this instance of the spanning tree. The allowed value ranges from 0 to 61440. The default priority value is 32768
Add VLAN	This parameter specifies the list of VLANs to be mapped to this instance of the spanning tree.
Delete VLAN	This parameter specifies the list of VLANs to be unmapped from this instance of the spanning tree.

Port Settings

Figure 5-74. Port Settings Page



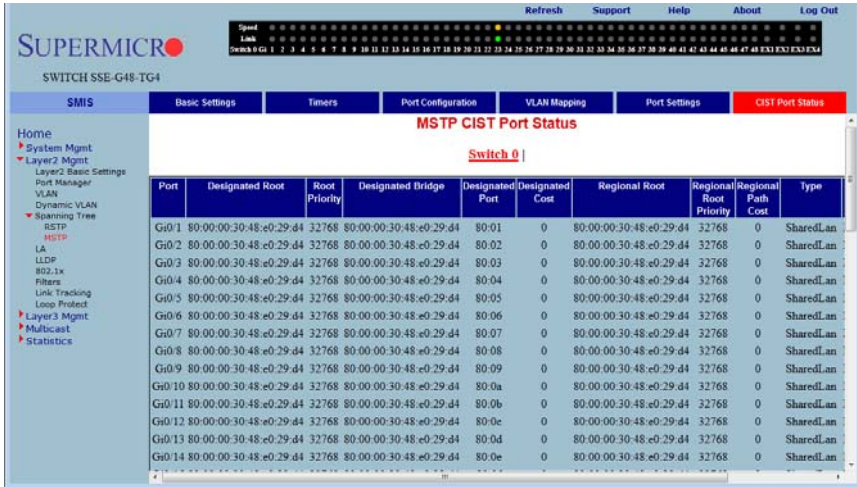
Clicking the PORT SETTINGS tab brings up the PORT SETTINGS page (Figure 5-74), which displays the various parameters for port settings. The parameters for this page are shown in Table 5-57.

Table 5-57. Port Settings Page Parameters

Parameter	Description
Port	This parameter specifies the interface index of the port on which MSTP is being run.
MSTP Instance ID	This parameter specifies the instance ID of the STP that is associated with this instance.
Port State	This parameter specifies the current state of the port.
Priority	This parameter specifies the priority related to this port.
Cost	This parameter specifies the cost associated with this port, which will be added to the cost of any path that includes this port.

CIST Port Status

Figure 5-75. MSTP CIST Port Status Page



Clicking the CIST PORT STATUS tab brings up the MSTP CIST PORT STATUS page (Figure 5-75), which displays MSTP CIST port specific information. The parameters for this page are shown in Table 5-58.

Table 5-58. MSTP CIST Port Status Page Parameters

Parameter	Description
Port	This parameter specifies the Port number.
Designated Root	This parameter specifies the unique Bridge Identifier of the Bridge recorded as the Root for the segment to which the port is attached.
Designated Bridge	This parameter specifies the Bridge Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.
Designated Port	This parameter specifies the Port Identifier of the port on the Designated Bridge for this port's segment.
Designated Cost	This parameter specifies the path cost of the Designated Port of the segment connected to this port.
Regional Root	This parameter specifies the unique Bridge Identifier of the bridge recorded as the CIST Regional Root Identifier in the configuration BPDUs transmitted.
Regional Path Cost	This parameter specifies the contribution of this port to the path cost of paths towards the CIST Regional Root, which includes this port.
Type	This parameter specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or shared media.

Table 5-58. MSTP CIST Port Status Page Parameters (Continued)

Parameter	Description
Role	This parameter specifies the ports current role as defined by the Spanning Tree Protocol.
Port State	This parameter specifies the port's current state as defined by the application of the Spanning Tree Protocol.

Link Aggregation (LA)

Link aggregation (LA) is a method of combining multiple parallel physical connections into a single logical connection(trunk), thus allowing increased bandwidth for a particular network path beyond what a single connection could sustain. By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved. For example, link aggregation provides redundancy in case one of the links fails. Link Aggregation also provides load balancing so that processing and communication activity is distributed across several links in a trunk ensuring that no single link is overwhelmed.

Other terms often used to describe this Link Aggregation method include **port trunking**, **link bundling**, **bonding**, or **teaming**. These umbrella terms encompass industry standards such as **IEEE 802.1ax** Link Aggregation Control Protocol (LACP) for wired Ethernet, or the previous **IEEE 802.3ad**, as well as various proprietary solutions. In this manual we will also refer to a particular group of aggregated links as a **Port Channel**.

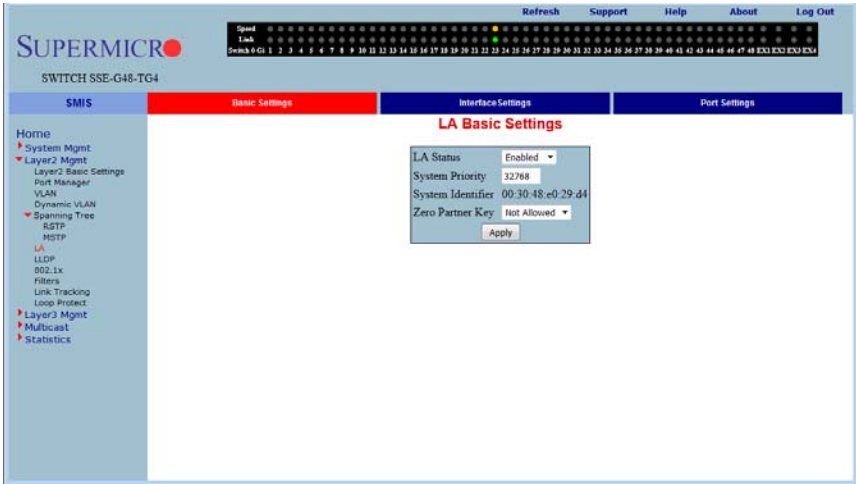
Supermicro switches support both static link aggregation and dynamic link aggregation using IEEE 802.3ad and LACP. Up to 24 Port Channels can be configured on an individual switch and each Port Channel can contain up to 8 members.

The LA link provides links to the following configuration pages:

- [Basic Settings](#)
- [Interface Settings](#)
- [Port Settings](#)

Basic Settings

Figure 5-76. LA Basic Settings Page



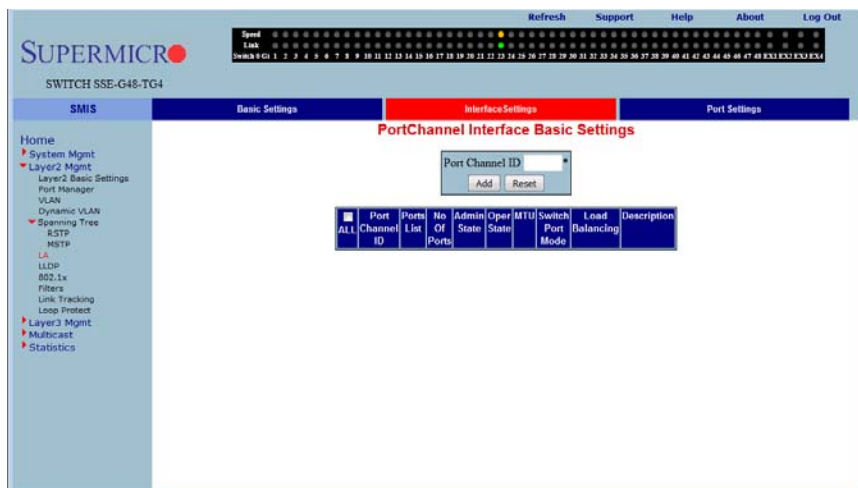
Clicking the BASIC SETTINGS tab brings up the LA BASIC SETTINGS page (Figure 5-76), which displays the various parameters for LA basic settings. The parameters for this page are shown in Table 5-59.

Table 5-59. LA Basic Settings Page Parameters

Parameter	Description
LA Status	This is used to enable or disable LA in the switch.
System Priority	This parameter specifies the priority value associated with the Actor's system ID. The allowed value ranges from 0 to 65535. The default value is 32768 .
System ID	This parameter specifies the Bridge MAC Address that is displayed. This is a read-only parameter.
Zero Partner Key	This is used to choose the partner key as <i>Allowed</i> or <i>Not Allowed</i> .

Interface Settings

Figure 5-77. Port Channel Interface Basic Settings Page



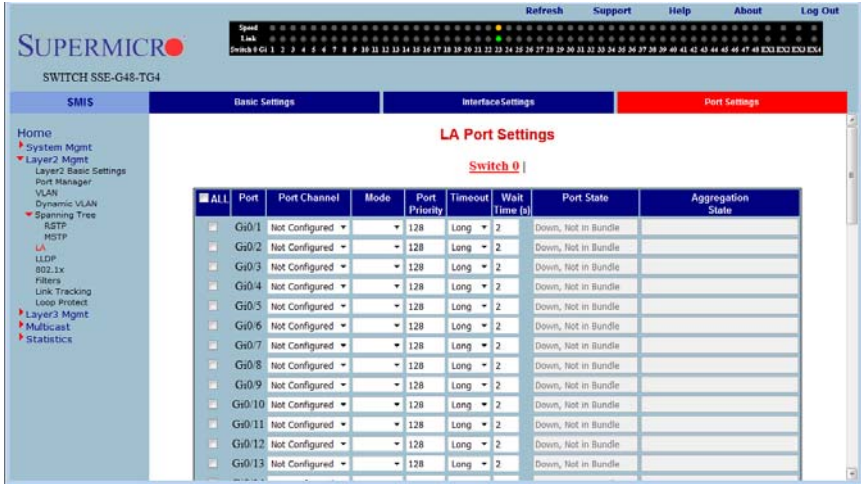
Clicking the INTERFACE SETTINGS tab brings up the PORT CHANNEL INTERFACE BASIC SETTINGS page (Figure 5-77), which allows you to configure port channels. The parameters for this page are shown in Table 5-60.

Table 5-60. Port Channel Interface Basic Settings Page Parameters

Parameter	Description
Port Channel ID	This parameter specifies the identifier of the port channel interface. The valid values are between 1 to 65535.
Port List	Displays the port list.
No of Ports	Displays the number of ports configured in LA.
Admin State	Displays administratively: port channel Up or Down.
Oper State	Displays operational status for port, Up or Down.
MTU	This parameter specifies the MTU value for this port channel. The allowed values range from 1500 to 9216. The default value is 1500.
Switch port mode	This parameter specifies the switch port mode for the port channel: <i>Access</i> , <i>Trunk</i> or <i>Hybrid</i>
Load balancing	User can either choose <i>Source MAC Address Based</i> , <i>Destination MAC Address Based</i> , <i>Source and Destination MAC Address Based</i> , <i>Source IP Address Based</i> , <i>Destination IP Address Based</i> , or <i>Source and Destination IP Address Based</i> .
Description	This parameter specifies the interface description string for this port channel.

Port Settings

Figure 5-78. LA Port Settings Page



Clicking the PORT SETTINGS tab brings up the LA PORT SETTINGS page (Figure 5-78), which configures LA properties at a per-port level. The parameters for this page are shown in Table 5-61.

Table 5-61. LA Port Settings Page Parameters

Parameter	Description
Port	This parameter specifies the Interface Name.
Port Channel	This parameter specifies the port channel.
Mode	This parameter specifies the various port modes, such as <i>On</i> , <i>Active</i> or <i>Passive</i> .
Port Priority	This parameter specifies the priority value of the Port. The allowed values are from 0 to 65535. The default is 128.
Timeout	This parameter sets the time within which LACP PDUs must be received on a port to avoid timing out of the Aggregated Link. If a <i>Long</i> timeout is chosen then the ports will time out of the Port Channel in 90-seconds. If a <i>Short</i> timeout is chosen then the ports will time out of the Port Channel in 3-seconds.
Wait Time	This parameter configures the waiting time for a port after receiving Partner information and before entering aggregation. The allowed values are from 0 to 10. The default value is 2.

Table 5-61. LA Port Settings Page Parameters (Continued)

Parameter	Description
Port State	This parameter indicates the current state of the port with respect to Link Aggregation. The possible states 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 is Up. • Standby — The Port is a member of the Port Channel but is currently in standby state. • Down — The Ports Oper-Status is Down.
Aggregation State	Specifies the state whether <i>Static</i> or <i>Dynamic</i> ..

LLDP

The LLDP link has the following configuration pages:

- [Global Settings](#)
- [Interface Settings](#)

Global Settings

Figure 5-79. LLDP Global Settings Page

The screenshot displays the LLDP Global Settings page. At the top, there is a status bar with 'Speed' and 'Link' indicators, and navigation links for 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. Below this is the 'SUPERMICRO' logo and the device identifier 'SWITCH SSE-G48-TG4'. The main navigation bar has 'SMIS' selected, with sub-tabs for 'Global Settings' (active) and 'Interface Settings'. The left sidebar menu includes 'Home', 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', and 'Statistics'. The 'LLDP Global Settings' form includes:

- LLDP Status: Disabled
- Transmit Interval: 30
- Holdtime Multiplier: 4
- Reinitialization Delay: 2
- Transmit Delay: 2
- Notification Interval: 5
- Chassis-id Subtype: MAC Address (with a value of 00:30:48:40:29:04)

An 'Apply' button is located below the form. A note at the bottom of the form states: 'If you choose "Chassis-id Subtype" option as "Chassis Component" or "Port Component" or "Locally Assigned", must provide an additional name string.'

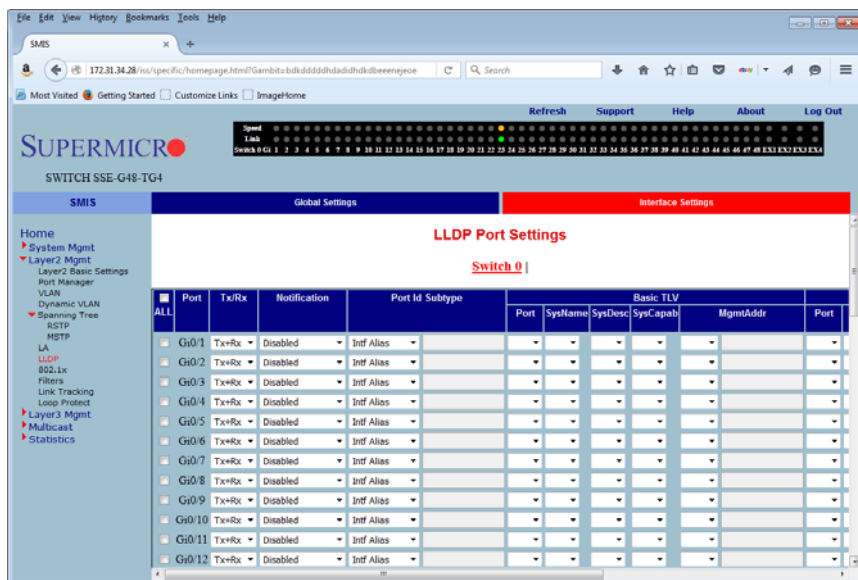
Clicking the GLOBAL SETTINGS tab brings up the GLOBAL SETTINGS page (Figure 5-79), which helps you to configure LLDP global parameters. The parameters for this page are shown in Table 5-62.

Table 5-62. LLDP Global Settings Page Parameters

Parameter	Description
LLDP Status	This parameter allows you to Enable or disable the LLDP status.
Transmit Interval	This parameter specifies the transmission frequency of LLDP updates in seconds. The allowed values are from 5 to 32768. The default is 30 seconds.
Holdtime Multiplier	This parameter specifies the multiplier value (value which is used to calculate the Time-To-Live for the LLDP advertisements). The allowed values are from 2 to 10. The default value is 4.
Reinitialization Delay	This parameter specifies the re-initialization delay (delay time taken by LLDP to re-initialize on any interface). The allowed values are from 1 to 10. The default is 2 seconds.
Transmit Delay	This parameter specifies the transmit delay (minimum amount of delay between successive LLDP frame transmissions). The allowed values are from 1 to 8192. The default is 2 seconds.
Notification Interval	This parameter specifies the notification interval (interval at which LLDP notifications are sent to NMS). The allowed values are from 5 to 3600. The default is 5 seconds.
Chassis-ID Subtype	With this parameter you can choose the Chassis-ID subtype either as a <i>Chassis Component</i> , a <i>Port Component</i> , a <i>MAC address</i> , a <i>Network Address</i> , an <i>Interface Name</i> or as <i>Locally Assigned</i> .

Interface Settings

Figure 5-80. LLDP Port Settings Page



Clicking the INTERFACE SETTINGS tab brings up the LLDP PORT SETTINGS page (Figure 5-80), which helps you to configure LLDP global parameters. The parameters for this page are shown in Table 5-63.

Table 5-63. LLDP Port Settings Page Parameters

Parameter	Description
Port	This parameter specifies the Port number
Tx/Rx	This parameter helps to configure either <i>Transmit and Receive(Tx+Rx)</i> , <i>Transmit(Tx)</i> , <i>Receive (Rx)</i> or <i>None</i> .
Notification	This parameter helps to configure either <i>Disabled</i> , <i>Remote Change</i> , <i>Mis Config</i> or <i>Both</i> .
Port ID Subtype	This parameter helps to choose a PortId subtype as either <i>Interface Alias</i> , <i>Port Component</i> , <i>Mac Address</i> , <i>Interface Name</i> or <i>Locally Assigned</i> .
Below fields are under Basis TLV .	
Port	This parameter specifies the port as either <i>Yes</i> or <i>None</i> .
SysName	This parameter specifies the system name as either <i>Yes</i> or <i>None</i> .
SysDesc	This parameter specifies the system description as either <i>Yes</i> or <i>None</i> .
SysCapab	This parameter specifies the system capability as either <i>Yes</i> or <i>None</i> .

Table 5-63. LLDP Port Settings Page Parameters

Parameter	Description
MgmtAddr	This parameter specifies the management address as either <i>All</i> or <i>IPv4</i> .
Below fields are under Dot1 TLV VLAN .	
Port	This parameter specifies the port as either <i>Yes</i> or <i>None</i> .
Protocol	This parameter specifies the protocol as either <i>All</i> or <i>VLAN ID</i> .
Name	This parameter specifies the name as either <i>All</i> or <i>VLAN ID</i> .
Below fields are under Dot3 TLV .	
MAC Phy	This parameter specifies the MAC as either <i>Yes</i> or <i>None</i> .
Link Agg	This parameter specifies the link aggregation as either <i>Yes</i> or <i>None</i> .
Max Frame	This parameter specifies the maximum frame as either <i>Yes</i> or <i>None</i> .

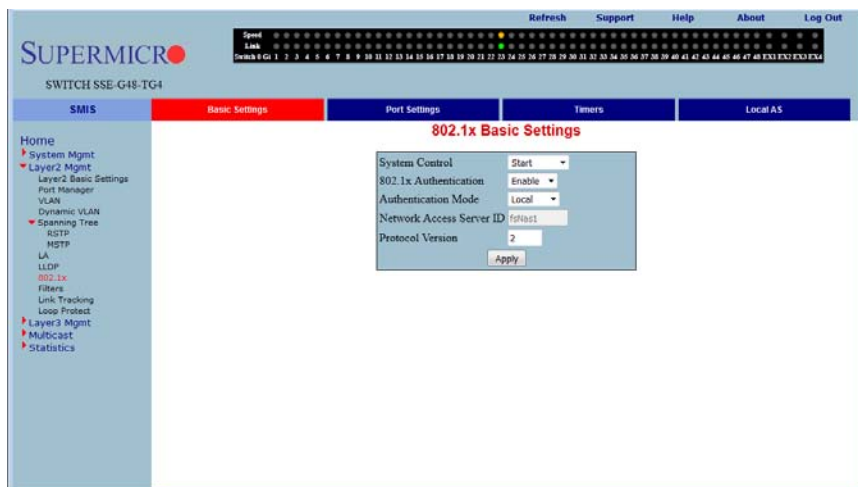
802.1x

The 802.1x link provides link to the following configuration pages:

- [Basic Settings](#)
- [Port Settings](#)
- [Timers](#)
- [Local AS](#)

Basic Settings

Figure 5-81. 802.1x Basic Settings Page



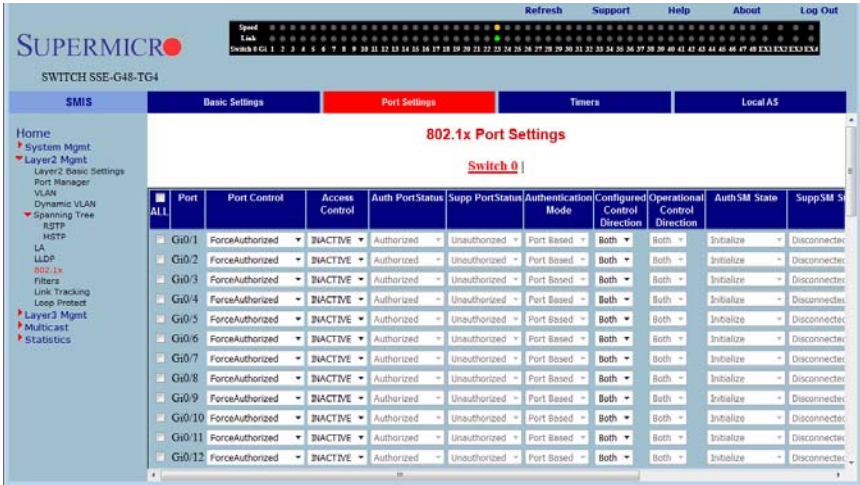
Clicking the BASIC SETTINGS tab brings up the 802.1x BASIC SETTINGS page (Figure 5-81), which displays the various 802.1x Basic Settings parameters. The parameters for this page are shown in Table 5-64.

Table 5-64. 802.1x Basic Settings Page Parameters

Parameter	Description
System Control	This parameter starts or shuts down 802.1x in the switch.
802.1x Authentication	This parameter allows enabling or disabling of the 802.1x based port security feature in the switch.
Authentication Server	This parameter specifies the Authentication Server Location as <i>Remote</i> or <i>Local</i> .
Network Access Server ID	This parameter specifies the Authenticator ID, which originates the Access-Request Packets.
Protocol Version	This parameter displays the version number.

Port Settings

Figure 5-82. 802.1x Port Settings Page



Clicking the PORT SETTINGS tab brings up the 802.1X PORT SETTINGS page (Figure 5-82), which configures security information at the individual port levels. The parameters for this page are shown in Table 5-65.

Table 5-65. 802.1x Port Settings Page Parameters

Parameter	Description
Port	This parameter specifies the Index of the port for which its fields (such as PORT CONTROL, PORT AUTHORIZATION STATUS, and so on) are configured.
Port Control	This parameter specifies the control values of the Authenticator Port. The control values can be: <ul style="list-style-type: none"> • Force Authorize - All the traffic through this port will be allowed always. • Force Unauthorized - All the traffic through this port will be blocked always. • Auto - The 802.1x authentication process will be imposed over this port.
Access Control	This parameter specifies the configuration of the Access control whether <i>Active</i> or <i>In-active</i> .
Port Authorization Status	This parameter specifies current status of the port either as <i>Authorized</i> or <i>Un-Authorized</i> .
Supp Port Status	This parameter specifies supplicant status of the Port either as <i>Authorized</i> or <i>Un-Authorized</i> .
Authentication Mode	This parameter specifies the configuration for selecting the AUTHENTICATION MODE to be <i>Port Based</i> .
Admin Control Direction	This parameter specifies whether security is to be imposed for <ul style="list-style-type: none"> • In - the incoming traffic • Both - both incoming and outgoing traffic

Table 5-65. 802.1x Port Settings Page Parameters (Continued)

Parameter	Description
Operational Control Direction	This parameter specifies the current security status.
Auth SM State	This parameter specifies authentication state machine state according to 802.1x standard protocol.
Supp SM State	This parameter specifies the supplicant state machine state as either <i>Connected</i> or <i>Disconnected</i> .
Restart Authentication	Selecting <i>True</i> will restart the authentication. Otherwise choose <i>False</i> .
Maximum Authentication Request	This parameter specifies the maximum number of authentication requests that can be sent from the authenticator before getting a response from the supplicant. The allowed ranges are 1 to 10. The default value is 2.
Re-authentication	This parameter provides configuration to enable or disable the re-authentication mechanism on the port.

Timers

Figure 5-83. 802.1x Timer Configuration Page

The screenshot displays the '802.1x Timer Configuration' page for 'Switch 0'. The page has a navigation bar with 'SMIS', 'Basic Settings', 'Port Settings', 'Timers', and 'Local AS'. A left sidebar contains a tree view with categories like 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', and 'Statistics'. The main content area shows a table with the following data:

Port	Quiet Period (secs)	Transmit Period (secs)	Re-authentication Period (secs)	Supplicant Timeout	Server Timeout	Held Period	Auth Period	Start Period	Max Start
Gig0/1	60	30	3600	30	30	60	30	30	2
Gig0/2	60	30	3600	30	30	60	30	30	2
Gig0/3	60	30	3600	30	30	60	30	30	2
Gig0/4	60	30	3600	30	30	60	30	30	2
Gig0/5	60	30	3600	30	30	60	30	30	2
Gig0/6	60	30	3600	30	30	60	30	30	2
Gig0/7	60	30	3600	30	30	60	30	30	2
Gig0/8	60	30	3600	30	30	60	30	30	2
Gig0/9	60	30	3600	30	30	60	30	30	2
Gig0/10	60	30	3600	30	30	60	30	30	2
Gig0/11	60	30	3600	30	30	60	30	30	2
Gig0/12	60	30	3600	30	30	60	30	30	2
Gig0/13	60	30	3600	30	30	60	30	30	2

Clicking the TIMERS tab brings up the 802.1X TIMER CONFIGURATION page (Figure 5-83), which configures Timer parameters at the individual port level. The parameters for this page are shown in Table 5-12.

Table 5-66. 802.1x Timer Configuration Page Parameters

Parameter	Description
Port	This parameter is the index of the port for which fields such as QUIET PERIOD, TRANSMIT PERIOD, and such are configured.
Quiet Period (Seconds)	This parameter specifies the duration for which the authenticator will be silent and will not attempt to acquire a supplicant. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 60 .
Transmit Period (Seconds)	This parameter specifies the time period used by the Authenticator State machine to define when the EAPOL PDU is to be transmitted. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 30 .
Re-authentication Period (Seconds)	This parameter specifies the time between periodic re-authentication of the supplicant. The default value is 3600 .
Supplicant Timeout	This parameter is the number of seconds that the switch waits for the retransmission of packets by the switch to the client. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 30 .
Server Timeout	This parameter is the number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 30 .
Held Period	This parameter is the number of seconds that the supplicant waits before trying to acquire the authenticator. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 60 .
Auth Period	This parameter is the number of seconds that the supplicant waits before timing-out the authenticator. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 30 .
Start Period	This parameter specifies the time period to start authentication of the supplicant. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 30 .
Max Start	This specifies the maximum number of EAPOL retries to the Authenticator. It can be configured to any value in the range from 1 to 65535 seconds. The default value is 2 .

Local AS

Figure 5-84. Local Authentication Server Configuration Page



Clicking the LOCAL AS tab brings up the LOCAL AUTHENTICATION SERVER CONFIGURATION page (Figure 5-16), which configures Local Authentication Server information. The parameters for this page are shown in Table 5-12.

Table 5-67. Local Authentication Server Configuration Page Parameters

Parameter	Description
User Name	This parameter specifies the identity of the user who is seeking authentication, and is set by a string of not more than 20 printable characters.
Password	This parameter specifies the password specific to the user name, and is set by a string of not more than 20 printable characters.
Permission	This parameter represents the allowance and denial of access. The values that can be configured are: <ul style="list-style-type: none"> Allow - When set to <i>Allow</i>, the authentication request is allowed over the set of ports in the PORT LIST. Deny - When set to <i>Deny</i>, the authentication request is NOT allowed over the set of ports in the PORT LIST.
Port List	This parameter represents the complete set of ports of the authenticator to which the user is allowed or denied access. It is based on permission.
Auth-TimeOut	This parameter specifies the timeout for authentication. The allowed ranges from 1 to 7200.

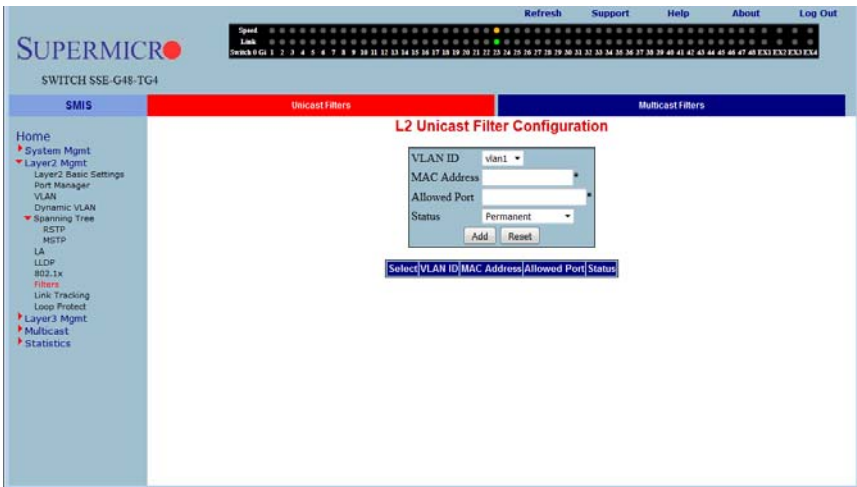
Filters

The FILTERS link allows you to configure Layer 2 packet filtering. The Layer 2 packet filtering management has the following configuration pages:

- [Unicast Filters](#)
- [Multicast Filters](#)

Unicast Filters

Figure 5-85. L2 Unicast Filter Configuration Page



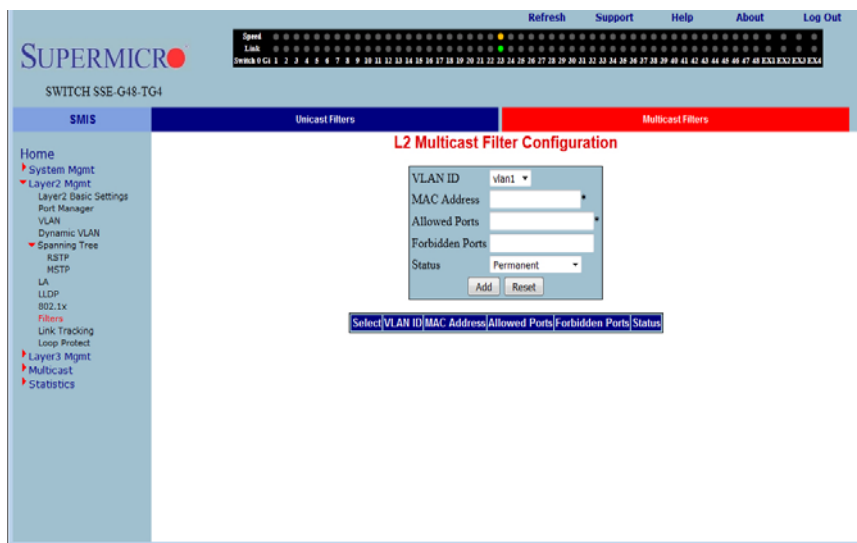
Clicking the UNICAST FILTERS tab brings up the L2 UNICAST FILTER CONFIGURATION page (Figure 5-16), which sets the filter configuration to control the unicast packets that the switch needs to process. The parameters for this page are shown in Table 5-12.

Table 5-68. L2 Unicast Filter Configuration Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN Identifier.
MAC Address	This parameter specifies the destination MAC address of the received packet.
Allowed Ports	This parameter specifies the list of ports on which the received packet, with the above set MAC address (if received from the configured port) can be forwarded.
Status	You can choose to set this configuration to any one of the following types: <ul style="list-style-type: none"> • Other – For entries currently in use, but whose conditions remain different from the following values. • Permanent – Entries that reside even after the restart of the switch. • DeleteOnReset – This deletes the entry on restart. • DeleteOnTimeout – This deletes the entry on expiration of the ageing timer.

Multicast Filters

Figure 5-86. L2 Multicast Filter Configuration Page



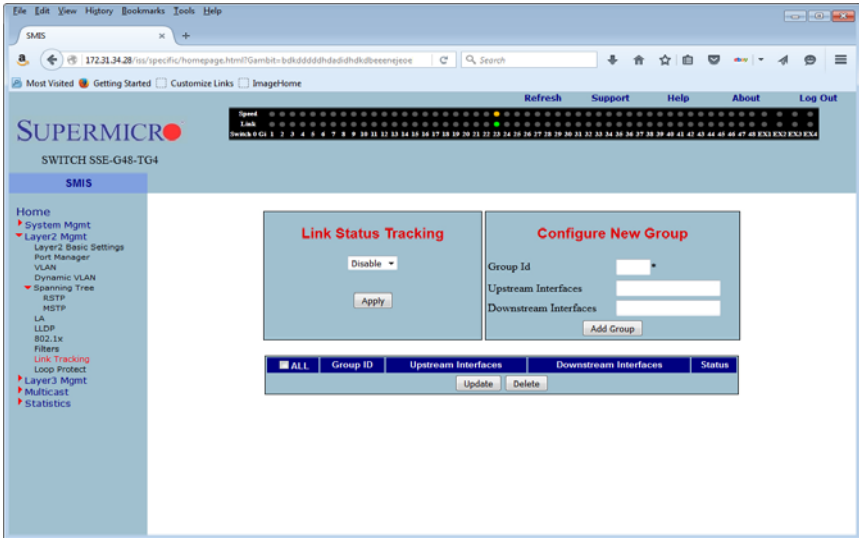
Clicking the MULTICAST FILTERS tab brings up the L2 MULTICAST FILTER CONFIGURATION page (Figure 5-16), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-12.

Table 5-69. L2 Multicast Filter Configuration Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN ID.
MAC Address	This parameter specifies the destination MAC address of the received packet.
Allowed Ports	This parameter specifies the list of ports on which the received packet, with the above set MAC address (if received from the configured port) can be forwarded.
Forbidden Ports	This parameter specifies the list of ports on which the received packet, with the above set MAC address (if received from the configured port) must NOT be forwarded.
Status	You can choose to set this configuration to any one of the following types: <ul style="list-style-type: none"> • Permanent – This configuration resides even after restart of the switch. • DeleteOnReset – This configuration deletes the entry on restart. • DeleteOnTimeout – This configuration deletes the entry on expiration of the ageing timer.

Link Tracking

Figure 5-87. Link Status Tracking/Configure New Group Page



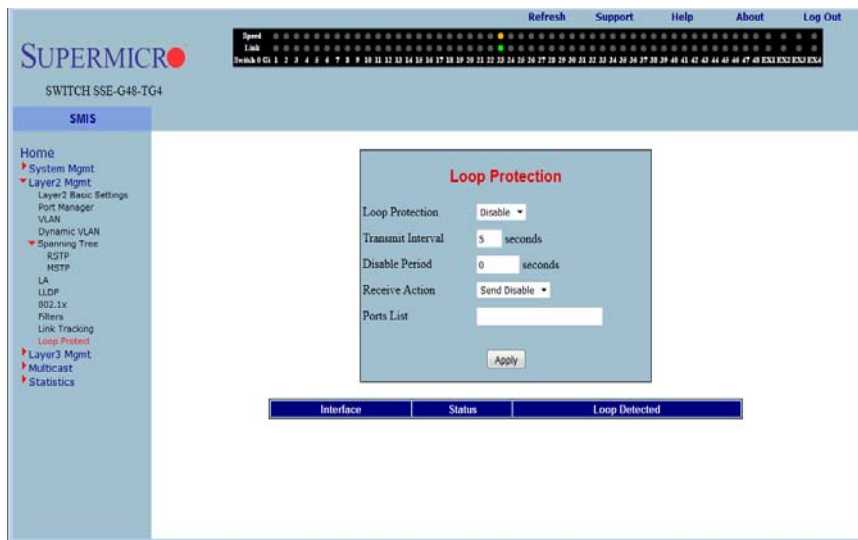
Clicking the LINK TRACKING link brings up the LINK STATUS TRACKING/CONFIGURE NEW GROUP page (Figure 5-87), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-70.

Table 5-70. Link Status Tracking/Configure New Group Page Parameters

Parameter	Description
Link Status Tracking	This parameter allows you to ENABLE and DISABLE Link Status Tracking.
Configure New Group	This parameter allows you to set the GROUP ID, UPSTREAM INTERFACES and DOWNSTREAM INTERFACES for a new group.
Group ID	This parameter specifies the group Id. The group identifiers should be valid number between 1 to 1024.
Upstream Interfaces	Each group can have one or more upstream interfaces. Physical ports (Gi/Ex) and port channel interfaces can be configured as upstream ports.
Downstream Interfaces	Each group can have one or more upstream interfaces. Physical ports (Gi/Ex) and port channel interfaces can be configured as upstream ports.
Status	This specifies the current status of link tracking up or down.

Loop Protect

Figure 5-88. Loop Protection Page



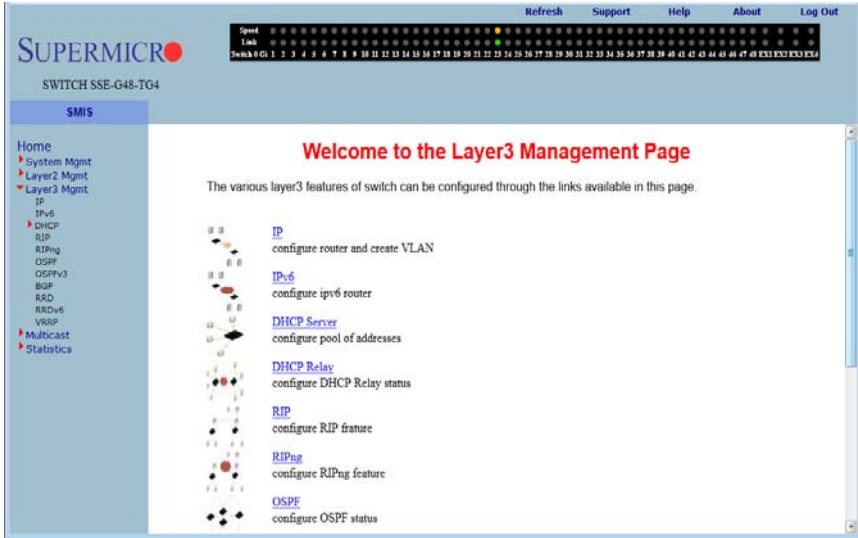
Clicking the LOOP PROTECT link brings up the LOOP PROTECTION page (Figure 5-88), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-71.

Table 5-71. Loop Protection Page Parameters

Parameter	Description
Loop Protection	This parameter allows you to ENABLE and DISABLE Loop Protection.
Transmit Interval	This parameter allows you to set the time interval in seconds. You can choose the interval between 1 to 10 seconds. The default value is 5 seconds.
Disable Period	This Parameter allows you to set the disable period in seconds. If this value is zero, the ports will be kept in the disabled state until the user enables the port by disabling, enabling loop protection on that port. The supported values are from 0 to 604800 seconds.
Receive Action	This parameter allows you to SEND DISABLE or NO DISABLE a received action.
Ports List	This parameter allows you to specify the ports list, for example <i>gi0/1-10, gi0/15, gi0/20</i> .

5-6 Layer 3 Management

Figure 5-89. Layer3 Management Page



The LAYER 3 MANAGEMENT home page (Figure 5-89) has the following links to all Layer 3 features:

- [IP](#)
- [IP V6](#)
- [DHCP Server](#)
- [DHCP Relay](#)
- [RIP](#)
- [RIPng](#)
- [OSPF](#)
- [OSPF V3](#)
- [BGP](#)
- [RRD](#)
- [RRD6](#)
- [VRRP](#)

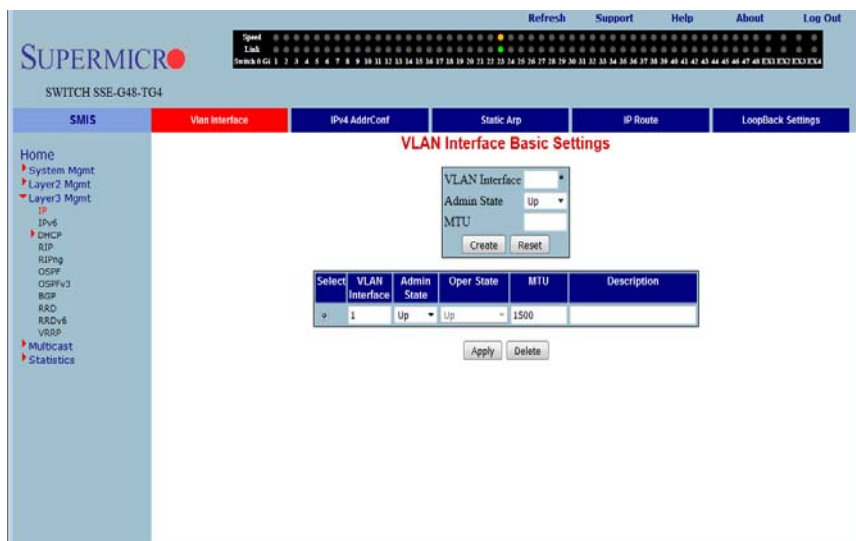
IP

The IP link enables you to perform IP related configuration. This can be done through the following pages.

- [VLAN Interface](#)
- [IPv4 AddrConf](#)
- [IP Route](#)
- [LoopBack Settings](#)

VLAN Interface

Figure 5-90. VLAN Interface Basic Settings Page



Clicking the VLAN INTERFACE tab brings up the VLAN INTERFACE BASIC SETTINGS page (Figure 5-90), which allows configuring of L3 VLAN interfaces. The parameters for this page are shown in Table 5-72.

Table 5-72. VLAN Interface Basic Settings Page Parameters

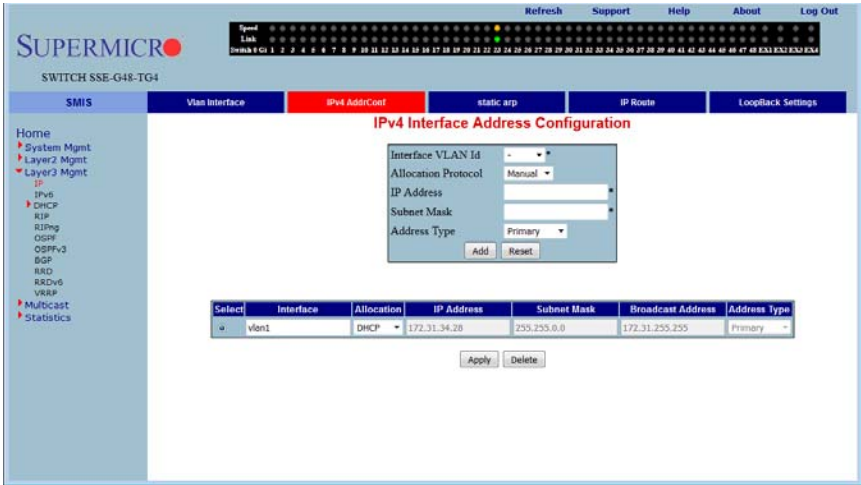
Parameter	Description
VLAN Interface	This parameter specifies the VLAN identifier.
Admin State	This parameter specifies the admin state as either <i>Up</i> or <i>Down</i> .
MTU	This parameter specifies the maximum transfer unit size in bytes. The allowed value ranges from 1500 to 9216. The default value is 1500.

Table 5-72. VLAN Interface Basic Settings Page Parameters (Continued)

Parameter	Description
Oper State	This parameter indicates status of VLAN, and whether it is <i>Up</i> or <i>Down</i> .
Description	This parameter specifies interface description string for this VLAN.

IPv4 AddrConf

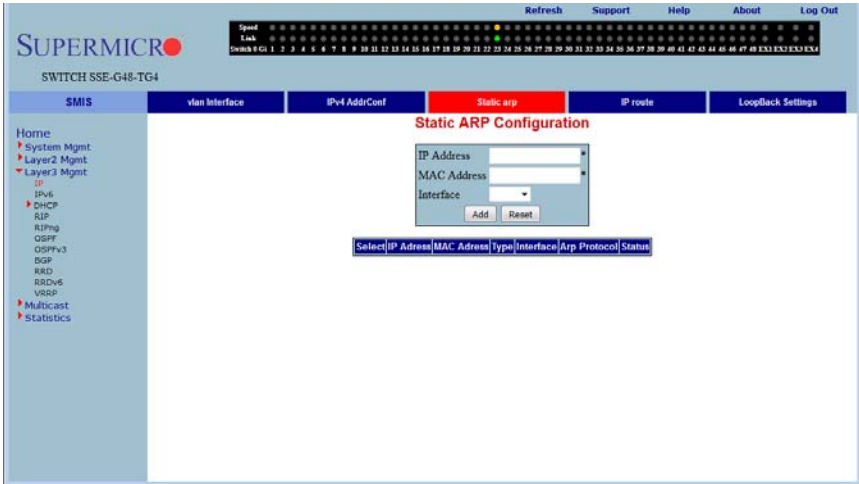
Figure 5-91. IPv4 Address Configuration Page



Clicking the IPv4 ADDR CONF tab brings up the IPv4 ADDRESS CONFIGURATION page (Figure 5-91), which allows you to configure the IP address for L3 VLANs. The parameters for this page are shown in Table 5-73.

Table 5-73. IPv4 Address Configuration Page Parameters

Parameter	Description
Interface VLAN ID	This parameter specifies the VLAN interface.
Allocation Protocol	This parameter specifies the protocol which is used to allocate IP address for the given interface. Options are either <i>Manual</i> , <i>DHCP</i> or <i>RARP</i> .
IP Address	This parameter specifies the IP Address of the specified interface.
Subnet Mask	This parameter indicates the mask for the specified IP Address.
Address Type	This parameter specifies the type of address, which can be <i>Primary</i> or <i>Secondary</i> .
Broadcast Address	This parameter displays broadcast address for the interface.

Static ARP**Figure 5-92. Static ARP Configuration Page**

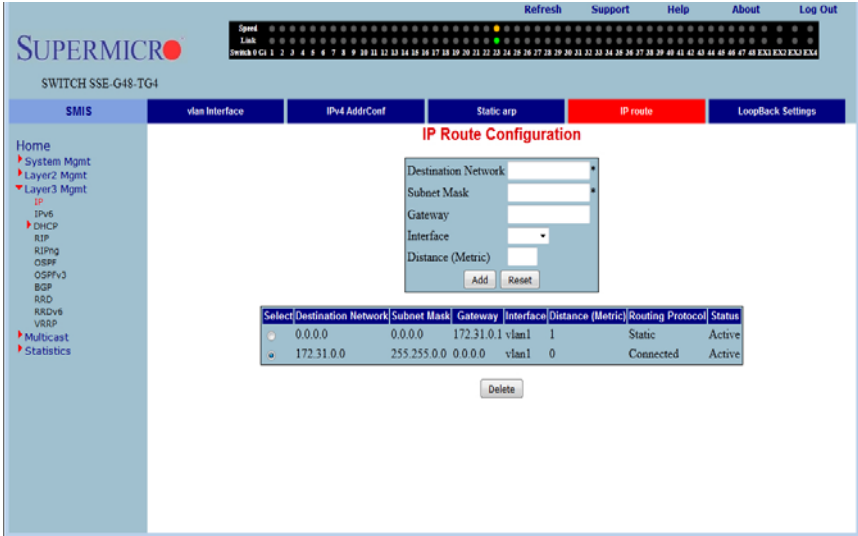
Clicking the STATIC ARP tab brings up the STATIC ARP CONFIGURATION page (Figure 5-92), which allows you to configure the IP address for L3 VLANs. The parameters for this page are shown in Table 5-74.

Table 5-74. Static ARP Configuration Page Parameters

Parameter	Description
IP Address	This parameter specifies the IP Address of the specified interface.
MAC Address	This parameter specifies the MAC Address of the specified interface.
Interface	This parameter specifies the interface to be used.

IP Route

Figure 5-93. IP Route Configuration Page



Clicking the IP ROUTE tab brings up the IP ROUTE CONFIGURATION page (Figure 5-93), which allows you to configure the static IP routes. The parameters for this page are shown in Table 5-75.

Table 5-75. IP Route Configuration Page Parameters

Parameter	Description
Destination Network	This parameter specifies the network address for which the route is being added.
Subnet Mask	This parameter indicates the subnet mask for the Destination Network address.
Gateway	This parameter denotes the Next Hop Gateway to reach the IP address.
Interface	This parameter specifies the outgoing interface.
Distance (Metric)	This parameter specifies the metric value of the destination.

LoopBack Settings

Figure 5-94. LoopBack Basic Settings Page

The screenshot displays the 'LoopBack Basic Settings' page. At the top, there is a status bar with 'Speed' and 'Link' indicators, and navigation links for 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. The main header shows 'SUPERMICR' and 'SWITCH SSE-G48-TG4'. A navigation menu on the left includes 'Home', 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'IP', 'DHCP', 'RIP', 'RIPng', 'OSPF', 'OSPFv3', 'BGP', 'RRD', 'RRDv6', 'VRRP', 'Multicast', and 'Statistics'. The 'LoopBack Settings' tab is active, showing a form with the following fields: 'LoopBack Interface' (text input), 'Interface type' (dropdown menu set to 'LoopBack'), 'Interface Status' (dropdown menu set to 'Up'), 'Ip Address' (text input), 'Subnet Mask' (text input), and 'MTU' (text input). Below the form are 'Create' and 'Reset' buttons. At the bottom, there is a table with the following columns: 'Select', 'LoopBack Interface', 'Interface Status', 'IP Address', 'Subnet Mask', 'Broadcast Address', 'Description', and 'MTU'. Below the table are 'Apply' and 'Delete' buttons.

Clicking the LOOPBACK SETTINGS tab brings up the LOOPBACK BASIC SETTINGS page (Figure 5-94), which allows you to configure loopback IP interfaces. The parameters for this page are shown in Table 5-76.

Table 5-76. LoopBack Basic Settings Page Parameters

Parameter	Description
LoopBack Interface	This parameter is the name of the loopback interface getting created.
Interface Type	This parameter is always the loopback for this configuration.
Interface Status	This parameter for the INTERFACE STATUS can be set to <i>Up</i> or <i>Down</i> .
IP Address	This parameter specifies the IP address for this loopback interface.
Subnet Mask	This parameter specifies the subnet mask for this loopback interface.

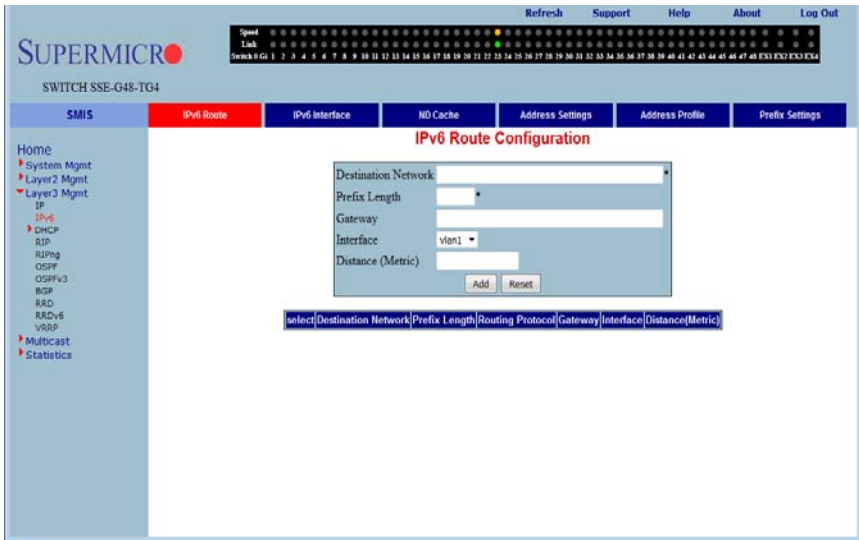
IP V6

The IPv6 link allows you to perform IPv6 related configurations. This can be accomplished through the following six pages.

- [IPv6 Route](#)
- [IPv6 Interface](#)
- [ND Cache](#)
- [Address Settings](#)
- [Address Profile](#)
- [Prefix Settings](#)

IPv6 Route

Figure 5-95. IP6 Route Configuration Page



Clicking the IPv6 ROUTE tab brings up the IPv6 ROUTE CONFIGURATION page (Figure 5-95), which configures various IP6 Route parameters. The parameters for this page are shown in Table 5-77.

Table 5-77. IP6 Route Configuration Page Parameters

Parameter	Description
Destination Network	This parameter specifies the network address for which the IPv6 route is being added.
Prefix Length	This parameter specifies the subnet mask for the above said address. The allowed value ranges between 1 to 128.

Table 5-77. IPv6 Route Configuration Page Parameters (Continued)

Parameter	Description
Routing Protocol	This parameter indicates the routing protocol through which the route was learned, if not manual. This cannot be configured.
Gateway	This parameter specifies the Next Hop Gateway to reach the IP address.
Interface	This parameter indicates the outgoing interface.
Distance (Metric)	This parameter denotes metric value of the destination. It should be in a range from 1 to 4294967295.

IPv6 Interface

Figure 5-96. IPv6 Interface Settings Page

The screenshot shows the 'IPv6 Interface Settings' page. The navigation menu on the left includes 'Home', 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'IPv6', 'DHCP', 'RIP', 'RIPng', 'OSPF', 'OSPFv3', 'BGP', 'RSD', 'RSDv6', 'VRRP', 'Multicast', and 'Statistics'. The 'IPv6' menu item is expanded, showing 'IPv6 Interface Settings'. The main content area has a title 'IPv6 Interface Settings' and a table with the following data:

Select	Port	Admin	Oper	RA Status	Hop Limit	Def. Rtr. Time	RA Rch. Time	RA Retrans. Time	Prefix Adv. Status	RA Interval	DAD Retries
o	vlan1	up	up	Disabled	64	1800	30	1	Enabled	600	1

An 'Apply' button is located below the table.

Clicking the IPv6 INTERFACE tab brings up the IPv6 INTERFACE SETTINGS page (Figure 5-96), which displays the various parameters for the IPv6 Interface. The parameters for this page are shown in Table 5-78.

Table 5-78. IPv6 Interface Settings Page Parameters

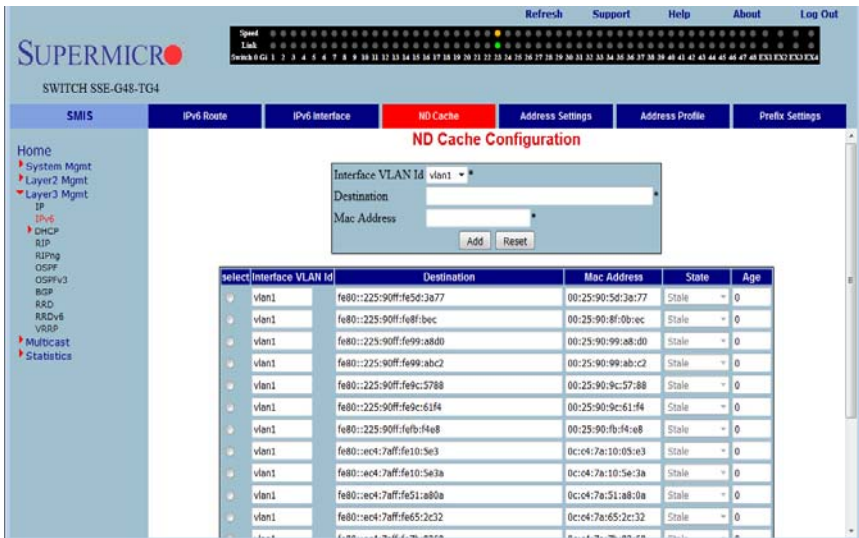
Parameter	Description
Port	This parameter specifies the Index of the VLAN interface.
Admin	This parameter indicates the Administrative Status of IPv6 on the Interface.
Oper	This parameter specifies the Operational Status of IPv6 on the given Interface, which is a read-only field.
RA Status	This parameter indicates the Router Advertisement status on the Interface.

Table 5-78. IPv6 Interface Settings Page Parameters (Continued)

Parameter	Description
Hop Limit	This parameter denotes the Hop Limit value to be placed in the Router Advertisements sent on the Interface. The allowed value ranges from 1 to 255. The default value is 64.
Def-Rtr Time	This parameter specifies the Default router lifetime to be placed in the Router Advertisements sent on the interface. The allowed value ranges from 0 to 9000. The default value is 1800.
RA Rch Time	This parameter indicates the Reachable time to be placed in the Router Advertisements sent on the interface. The allowed value ranges from 0 to 3600. The default value is 30.
RA Retrans Time	This parameter specifies the RA Retransmit time to be placed in the Router Advertisement sent on the interface. The allowed value ranges from 1 to 3600. The default value is 1.
Prefix-Adv Status	This parameter specifies the Prefix Advertisement status on the Interface.
RA Interval	This parameter specifies the minimum time in seconds allowed between sending unsolicited router advertisements. The allowed value ranges from 3 to 1800. The default value is 600.
DAD Retries	This parameter specifies the maximum number of Duplicate Address Detection retries. The allowed value ranges from 1 to 10. The default value is 1.

ND Cache

Figure 5-97. ND Cache Configuration Page



Clicking the ND CACHE tab brings up the ND CACHE CONFIGURATION page (Figure 5-97). The parameters for this page are shown in Table 5-79.

Table 5-79. ND Cache Configuration Page Parameters

Parameter	Description
Interface VLAN ID	This parameter indicates index of the VLAN interface.
Destination	This parameter specifies Destination IPv6 address.
MAC Address	This parameter denotes the physical address of the Destination address.
State	This parameter indicates the Reachability state of the entry, which is a read-only field.
Age	This parameter specifies the Age Time.

Address Settings

Figure 5-98. Address Settings Page

The screenshot shows the SUPERMICRO web management utility interface. The top navigation bar includes tabs for SMIS, IPv6 Route, IPv6 Interface, ND Cache, Address Settings (highlighted), Address Profile, and Prefix Settings. The main content area displays the 'Address Settings' page for IPv6. It features a form with the following fields: Interface VLAN Id (vlan1), Address (input field), Prefix Length (input field), and Address Type (Unicast dropdown). Below the form is a table with columns: select, Interface VLAN Id, Address, Prefix Length, and Address Type. The table contains one entry: 'vlan1' with address 'fe80::230:48ff:fe0:2994', prefix length '128', and address type 'LinkLocal'. A 'Delete' button is located below the table.

Clicking the ADDRESS SETTINGS tab brings up the ADDRESS SETTINGS page (Figure 5-98), which allows you to configure address settings for IPv6. The parameters for this page are shown in Table 5-80.

Table 5-80. Address Settings Page Parameters

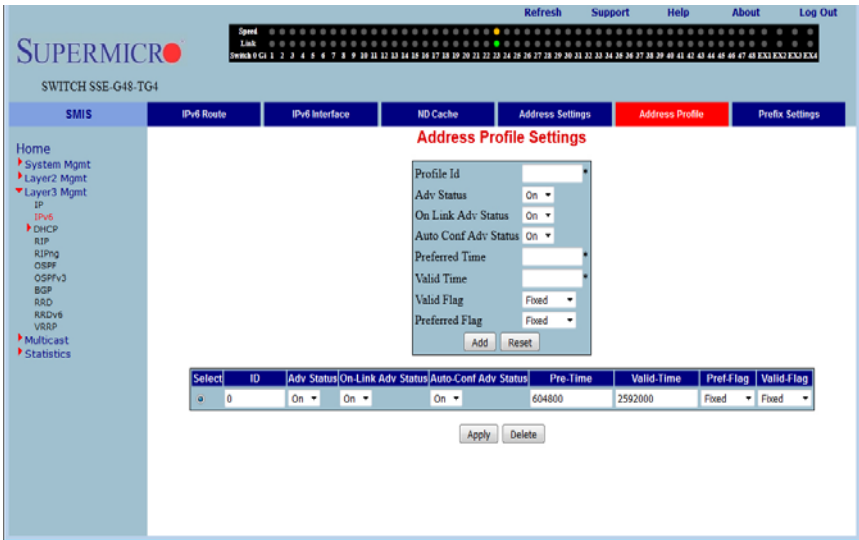
Parameter	Description
Interface VLAN ID	This parameter specifies the index of the VLAN Interface.
Address	This parameter specifies the IPv6 address.

Table 5-80. Address Settings Page Parameters (Continued)

Parameter	Description
Prefix Length	This parameter indicates the length of the prefix (in bits) associated with this entry's IPv6 address. The allowed value ranges between 1 to 128.
Address Type	This parameter specifies that the type of address can be Link-Local, Global-Unicast or Anycast.

Address Profile

Figure 5-99. Address Profile Settings Page



Clicking the ADDRESS PROFILE tab brings up the ADDRESS PROFILE SETTINGS page (Figure 5-99). The parameters for this page are shown in Table 5-81.

Table 5-81. Address Profile Settings Page Parameters

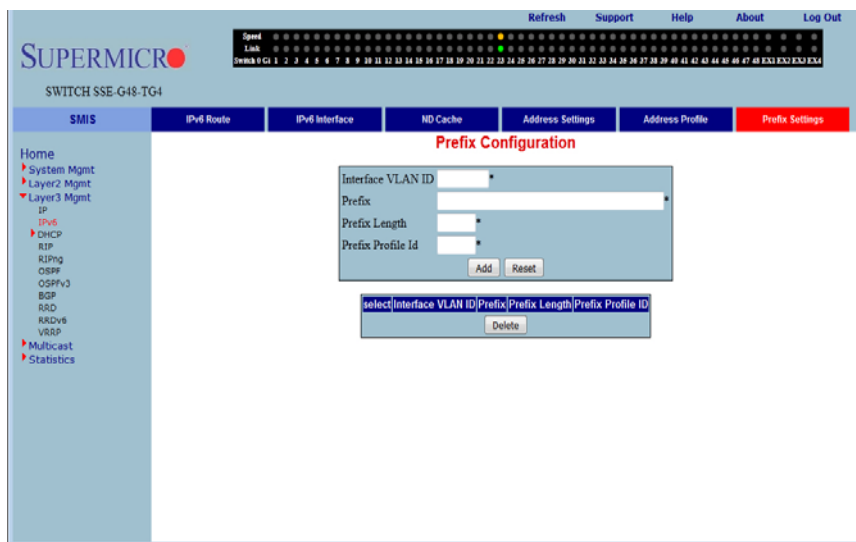
Parameter	Description
Profile ID	This parameter specifies the index of the Address Profile entry.
Adv Status	This parameter specifies the Prefix Advertise status. The allowed value ranges between 0 to 200.
On Link Adv Status	This parameter indicates the On-Link Advertise Flag status.
Auto Conf Adv Status	This parameter denotes the Autonomous Configuration Advertise Flag status.
Preferred Time	This parameter specifies the Preferred Lifetime of the prefix address that uses this profile. The allowed value ranges between 0 to 4294967295.
Valid Time	This parameter indicates the Valid Lifetime of the prefix address that uses this profile. The allowed value ranges between 0 to 4294967295.

Table 5-81. Address Profile Settings Page Parameters (Continued)

Parameter	Description
Valid Flag	This parameter specifies if the Valid Lifetime Flag is <i>Variable</i> or <i>Fixed</i> .
Preferred Flag	This parameter specifies if the Preferred Lifetime Flag is <i>Variable</i> or <i>Fixed</i> .

Prefix Settings

Figure 5-100. Prefix Configuration Page



Clicking the PREFIX SETTINGS tab brings up the PREFIX CONFIGURATION page (Figure 5-100). The parameters for this page are shown in Table 5-82.

Table 5-82. Prefix Configuration Page Parameters

Parameter	Description
Interface VLAN ID	This parameter specifies the index of the VLAN Interface. The allowed value ranges between 1 to 255.
Prefix	This parameter indicates the IPv6 address prefix to be advertised in RA.
Prefix Length	This parameter indicates the PREFIX LENGTH (in bits).
Prefix Profile ID	This parameter specifies index to the IPv6 address profile table. The allowed value ranges between 0 to 200.

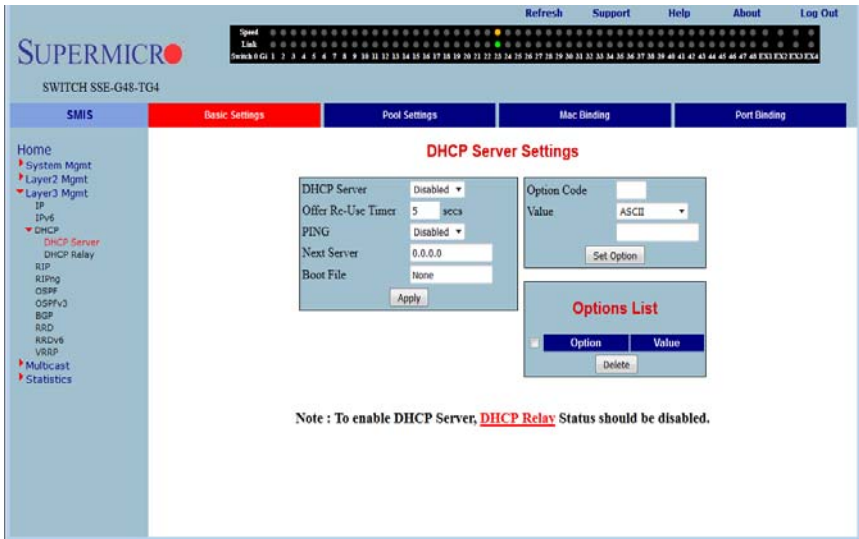
DHCP Server

The DHCP Server link helps you to manage the DHCP server in the switch through the following two pages:

- [Basic Settings](#)
- [Pool Settings](#)
- [MAC Binding](#)
- [Port Binding](#)

Basic Settings

Figure 5-101. DHCP Server Settings Page



Clicking the BASIC SETTINGS tab brings up the DHCP SERVER SETTINGS page (Figure 5-101). The parameters for this page are shown in Table 5-83.

Table 5-83. DHCP Server Settings Page Parameters

Parameter	Description
DHCP-Server	With this parameter you can enable or disable the DHCP server using this configuration.
Offer-reuse Time out (seconds)	This parameter specifies the Reuse Timeout value that can be configured in this field, which is used by DHCP. The allowed value ranges between 1 to 120. The default value is 5 seconds.
PING	Enables/disables the PING feature.
Next Server	Specifies the next server address.

Table 5-83. DHCP Server Settings Page Parameters (Continued)

Parameter	Description
Boot File	Specifies the file name for booting.
Option	Specifies the DHCP option in the range 1 to 2147483647.
Value	User can specify the Option field value as ASCII or HEX STRING or IP ADDRESS.
Option List table	This parameter displays the saved option and value in a switch.

Pool Settings

Figure 5-102. DHCP Pool Settings Page

Clicking the POOL SETTINGS link brings up the DHCP POOL SETTINGS page (Figure 5-102), which allows you to configure the IP address pool that can be used by the DHCP server to allocate IP addresses. The parameters for this page are shown in Table 5-84.

Table 5-84. DHCP Pool Settings Page Parameters

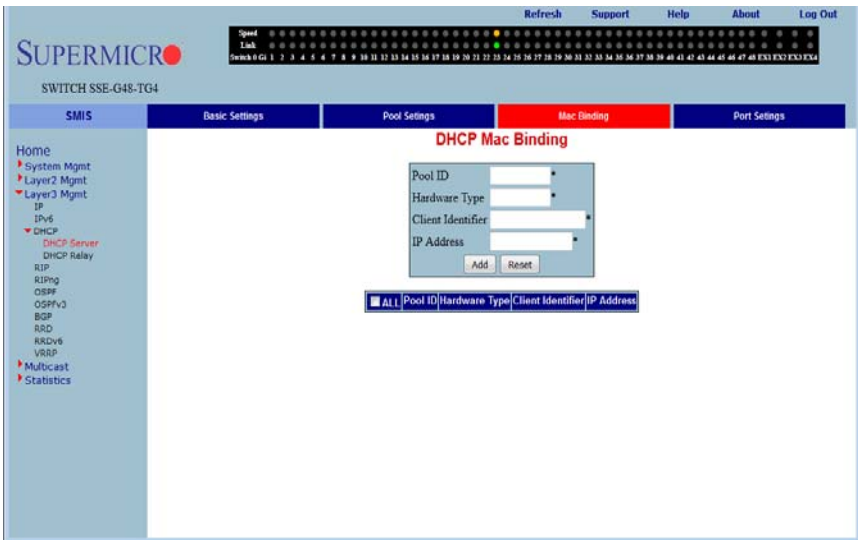
Parameter	Description
Pool ID	This parameter specifies the pool ID to index among the different subnet pools configured. The allowed value ranges between 1 and 2147483647.
Network	This parameter specifies the subnet of the IP address in the pool.
Subnet Mask	This parameter specifies the subnet mask of the IP address in the pool.
Start IP	This parameter specifies the first IP address in the address pool that is used for dynamic allocation by the DHCP server.

Table 5-84. DHCP Pool Settings Page Parameters (Continued)

Parameter	Description
End IP	This parameter specifies the last IP address in the address pool that is used for dynamic allocation by the DHCP server.
Lease Time	This parameter specifies the time interval for which the IP address is valid.
Utilization Threshold	This parameter specifies the DHCP Pool Utilization Threshold value. The allowed value ranges between 0 and 100.
Domain name	This parameter specifies the domain name for address pool.
DNS Server	This parameter specifies the IP address of DNS server for this pool.
Netbios Name Server	This parameter specifies the IP address of netbios name server for this pool.
Netbios Node	You can either choose the Netbios node to be specified as <i>Number</i> , <i>B Node</i> , <i>H Node</i> , <i>M Node</i> or <i>P Node</i> .
Default Router	Specifies the default router address for this pool.

MAC Binding

Figure 5-103. DHCP MAC Bindings Page



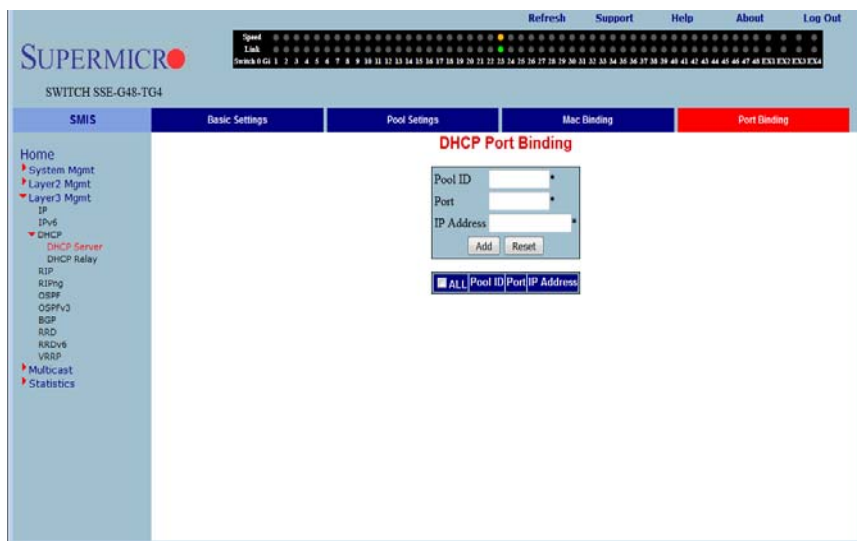
Clicking the MAC BINDINGS link brings up the DHCP MAC BINDING page (Figure 5-103), which allows you to configure parameters for DHCP MAC binding. The parameters for this page are shown in Table 5-85.

Table 5-85. DHCP MAC Binding Page Parameters

Parameter	Description
Pool ID	This parameter specifies the pool ID to index among the different subnet pools configured. The allowed value ranges between 1 and 2147483647.
Hardware Type	This parameter specifies the Hardware Type.
Client Identifier	This parameter specifies the Client Identifier.
IP Address	This parameter specifies the IP Address.

Port Binding

Figure 5-104. DHCP Port Binding Page



Clicking the PORT BINDING link brings up the DHCP PORT BINDING page (Figure 5-104), which allows you to configure parameters for DHCP Port Binding. The parameters for this page are shown in Table 5-86.

Table 5-86. DHCP Port Binding Page Parameters

Parameter	Description
Pool ID	This parameter specifies the pool ID to index among the different subnet pools configured. The allowed value ranges between 1 and 2147483647.
Port	This parameter specifies the Port.
IP Address	This parameter specifies the IP Address.

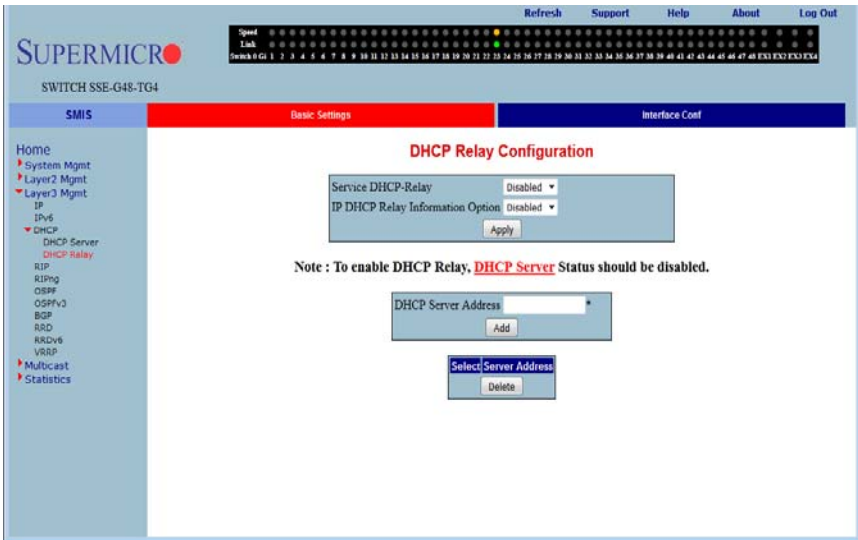
DHCP Relay

The DHCP Relay link helps you to manage the DHCP relay in the switch through the following two pages:

- [Basic Settings](#)
- [Interface Conf](#)

Basic Settings

Figure 5-105. DHCP Relay Configuration Page



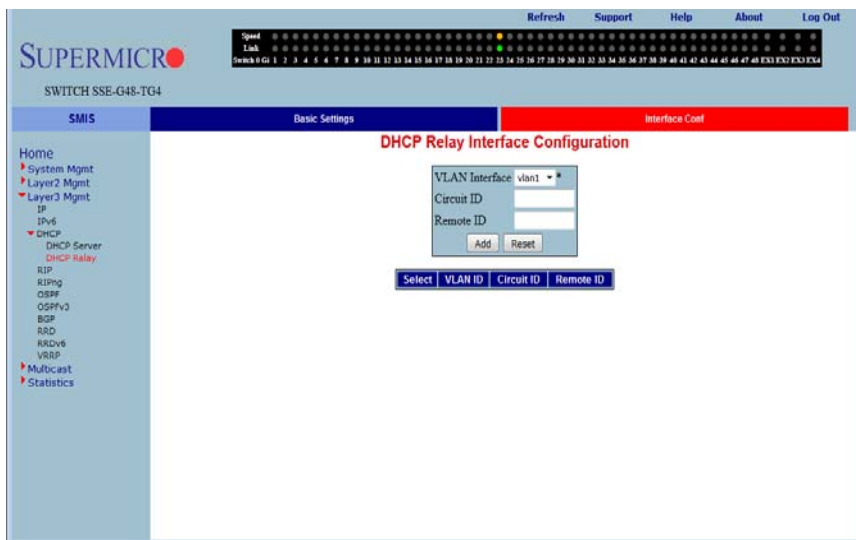
Clicking the BASIC SETTINGS tab brings up the DHCP RELAY CONFIGURATION page (Figure 5-105), which displays the various parameters for configuring the DHCP relay. The parameters for this page are shown in Table 5-87.

Table 5-87. DHCP Relay Configuration Page Parameters

Parameter	Description
Service DHCP-Relay	This parameter specifies the DHCP relay status that can be enabled or disabled in the switch using this field.
IP DHCP Relay Information Option	You can enable/disable this field to control the processing related to the Relay Agent Information options.
DHCP Server Address	This parameter indicates the IP address of the DHCP Server to which the Relay Agent needs to forward the packets from the client.

Interface Conf

Figure 5-106. DHCP Relay Interface Configuration Page



Clicking the INTERFACE CONF link brings up the DHCP RELAY INTERFACE CONFIGURATION page (Figure 5-106), which allows you to configure the DHCP relay for VLANs. The parameters for this page are shown in Table 5-88.

Table 5-88. DHCP Relay Interface Configuration Page Parameters

Parameter	Description
VLAN Interface	This parameter specifies the VLAN Interface name.
Circuit ID	This parameter specifies the DHCP Relay Circuit identifier. The allowed value ranges between 1 and 2147483647.
Remote ID	This parameter specifies the Remote identifier.

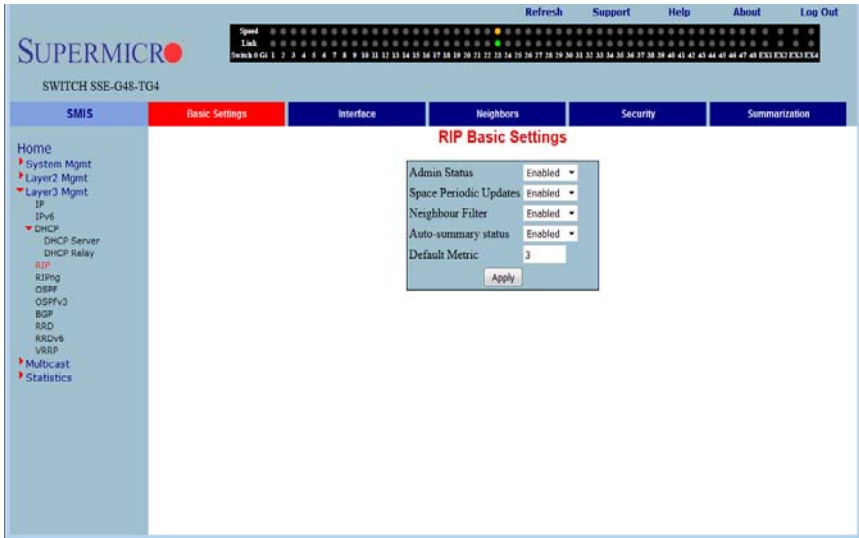
RIP

The RIP link opens the following links for configuration of RIP protocol:

- [Basic Settings](#)
- [Interface](#)
- [Neighbors](#)
- [Security](#)
- [Summarization](#)

Basic Settings

Figure 5-107. RIP Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the RIP BASIC SETTINGS page (Figure 5-107). The parameters for this page are shown in Table 5-89.

Table 5-89. RIP Basic Settings Page Parameters

Parameter	Description
Admin Status	This parameter enables/disables the admin status.
Space Periodic Updates	This parameter enables/disables the space periodic updates
Neighbor Filter	This parameter enables/disables neighbor filtering. Neighbor filtering helps you to filter routes from specific neighbors.
Auto-summary status	This parameter enables/disables the auto-summary feature.
Default metric	This parameter specifies the default metric. The allowed value ranges between 1 and 16. The default value is 3.

Interface

Figure 5-108. RIP Interface Page

The screenshot shows the SUPERMICRO web-based management utility interface. At the top, there is a status bar with 'Speed' and 'Link' indicators, and navigation links for 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. The main header identifies the device as 'SWITCH SSE-G48-TG4'. Below this, there are tabs for 'Basic Settings', 'Interface' (which is selected), 'Neighbors', 'Security', and 'Summarization'. The left sidebar contains a navigation menu with options like 'Home', 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'IP', 'IPv6', 'DHCP', 'RIP', 'OSPF', 'BGP', 'RSD', 'RRDv6', 'VRRP', 'Multicast', and 'Statistics'. The main content area is titled 'RIP Interface' and features a dropdown menu for 'Interface' set to 'vlon1' with an 'Add' button. Below this is a table with the following columns: 'Select', 'IP Address', 'Status', 'Split Horizon', 'Default Route Installation', 'Send Version', 'Receive Version', 'Route Age Timer', 'Update Timer', and 'Garbage Timer'. The table contains one row with the following values: '0', '172.31.34.28', 'Enabled', 'Poison Reverse', 'No', 'RIP1 Compatible', 'RIP1 or RIP2', '180', '30', and '120'. There are 'Apply' and 'Delete' buttons below the table.

Clicking the INTERFACE tab brings up the RIP INTERFACE page (Figure 5-108). The parameters for this page are shown in Table 5-90.

Table 5-90. RIP Interface Page Parameters

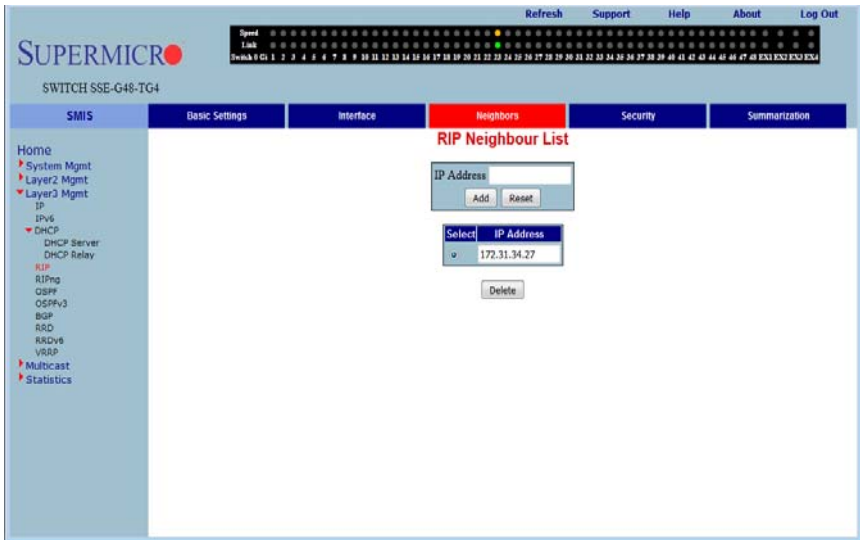
Parameter	Description
Interface	This parameter specifies the Interface ID for which RIP needs to be configured.
IP Address	This parameter specifies the IP address of the RIP interface.
Status	This parameter specifies the admin status of the interface.
Split Horizon	This parameter specifies the operational status of Split Horizon in the system.
Default Route Installation	This parameter specifies whether Default Route Installation can be done or not.
Send Version	This parameter allows selecting the RIP packets sent to be compatible to either <i>RIPV1</i> , <i>RIP1 Compatible</i> or <i>RIPV2</i> .
Receive Version	This parameter is similar to SEND VERSION, but it allows you to choose the RIP packets to be received as either <i>RIPV1</i> , <i>RIPV2</i> , both <i>RIPV1 and RIPV2</i> or <i>None</i> .
Route Age Timer	This parameter specifies the time interval after which the routes will be flushed. The allowed value ranges between 30 and 500. The default value is 180.

Table 5-90. RIP Interface Page Parameters (Continued)

Parameter	Description
Update Timer	This parameter specifies the time interval between successive RIP updates. The allowed value ranges between <i>10</i> and <i>3600</i> . The default value is 30 .
Garbage Timer	This parameter specifies the time interval after which the invalid routes will be removed from the routing table. The allowed value ranges between <i>120</i> and <i>180</i> . The default value is 120 .

Neighbors

Figure 5-109. RIP Neighbor List Page

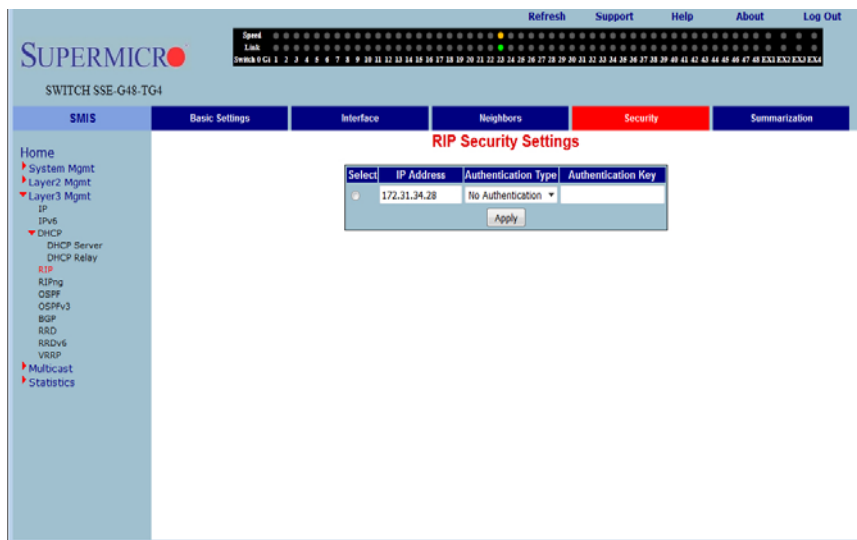


Clicking the NEIGHBORS tab brings up the RIP NEIGHBOR LIST page (Figure 5-109), which is used to configure the RIP neighbors, by configuring their IP address.

The single parameter for this page is IP ADDRESS, which specifies the IP Address of the neighbor router to which the unicast update has to be sent.

Security

Figure 5-110. RIP Security Settings Page



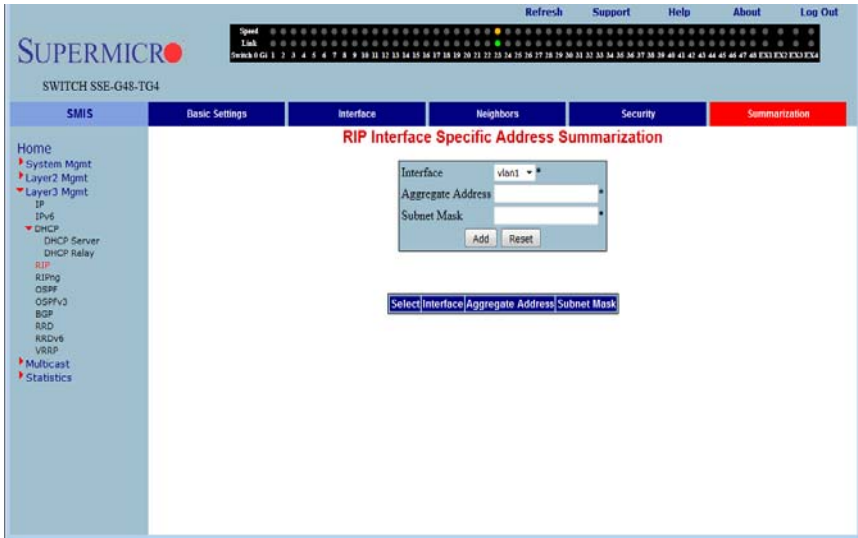
Clicking the SECURITY tab brings up the RIP SECURITY SETTING page (Figure 5-110). The parameters for this page are shown in Table 5-12.

Table 5-91. RIP Security Setting Page Parameters

Parameter	Description
IP Address	This parameter displays the active RIP interfaces. You can select the interface for which you want to configure authentication.
Authentication Type	This parameter specifies the authentication type. You can choose <i>No Authentication</i> , or <i>Simple Password</i> , or the <i>md5</i> authentication type.
Authentication Key	This parameter specifies the key used for authentication if the authentication type is other than <i>No Authentication</i> .

Summarization

Figure 5-111. RIP Interface Specific Address Summarization Page



Clicking the SUMMARIZATION tab brings up the RIP INTERFACE SPECIFIC ADDRESS SUMMARIZATION page (Figure 5-111). The parameters for this page are shown in Table 5-92.

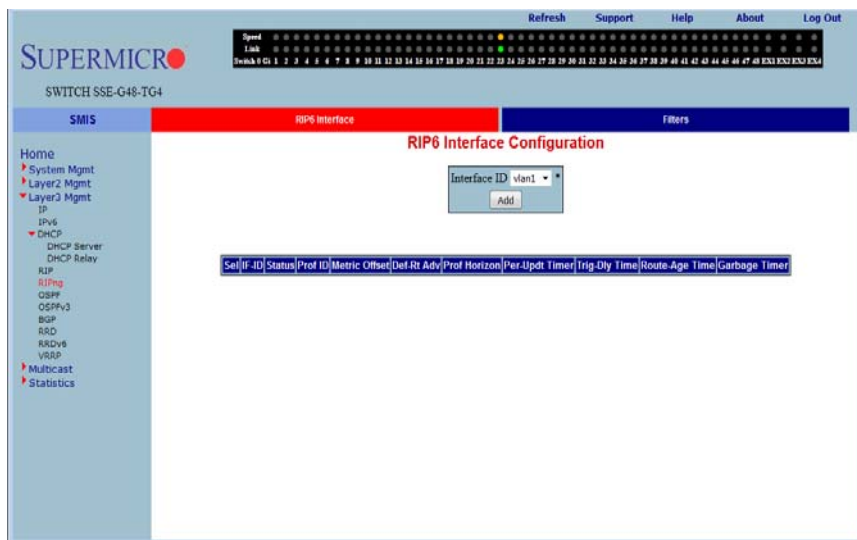
Table 5-92. RIP Interface Specific Address Summarization Page Parameters

Parameter	Description
Interface	This parameter specifies the Interface ID for which the RIP aggregate address needs to be configured.
Aggregate Address	This parameter specifies the aggregate address.
Subnet Mask	This parameter specifies the mask of the aggregate address.

RIPng

The RIP6 link allows you perform RIPV6 related configuration for the switch. This can be accomplished through the following two pages:

- [RIP6 Interface](#)
- [Filters](#)

RIP6 Interface**Figure 5-112. RIP6 Interface Configuration Page**

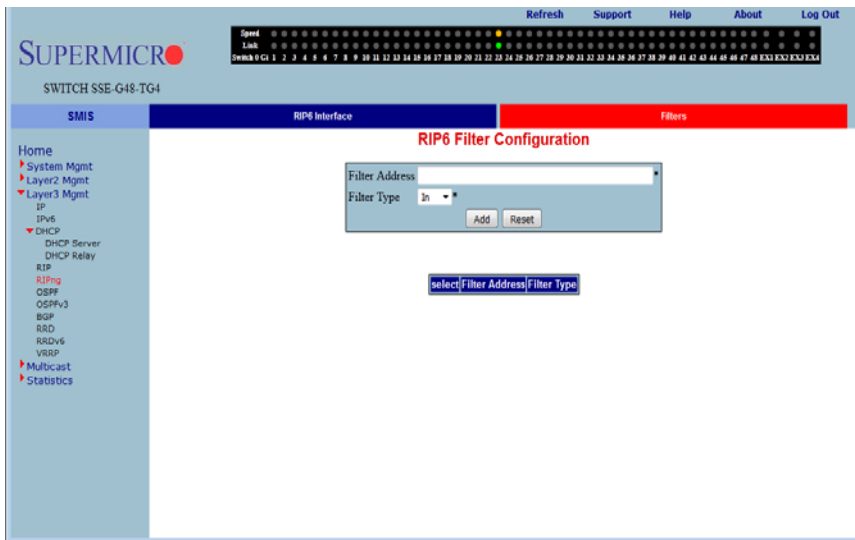
Clicking the RIP6 INTERFACE tab brings up the RIP6 INTERFACE CONFIGURATION page (Figure 5-112). The parameters for this page are shown in Table 5-93.

Table 5-93. RIP6 Interface Configuration Page Parameters

Parameter	Description
Interface ID	Specifies the Interface Id for which IPv6 needs to be configured.
Status	This parameter specifies the administration status of the interface.
Prof ID	This parameter indicates the Index of the Address Profile entry.
Metric Offset	This parameter specifies the metric for the routes that are being re-distributed.
Def Rt Adv	This parameter indicates the default router lifetime to be placed in the Router Advertisements sent on the interface.
Prof Horizon	This parameter specifies the operational status of Profile Horizon in the system.
Per-Updt Timer	This parameter specifies the time interval between successive IPv6 updates.
Trig-Dly Time	This parameter indicates the time interval in seconds by which further triggered updates are delayed, after one triggered update is sent.
Route Age Time	This parameter specifies the time interval after which, the routes are flushed.
Garbage Timer	This parameter specifies the time interval after which, the invalid routes are removed from the routing table.

Filters

Figure 5-113. RIP6 Filter Configuration Page



Clicking the FILTERS tab brings up the RIP6 FILTER CONFIGURATION page (Figure 5-113). The parameters for this page are shown in Table 5-94.

Table 5-94. RIP6 Filter Configuration Page Parameters

Parameter	Description
Filter Address	This parameter specifies the FILTER ADDRESS for the RIP6 interface.
Filter Type	This parameter specifies the FILTER TYPE for which RIP6 needs to be configured.

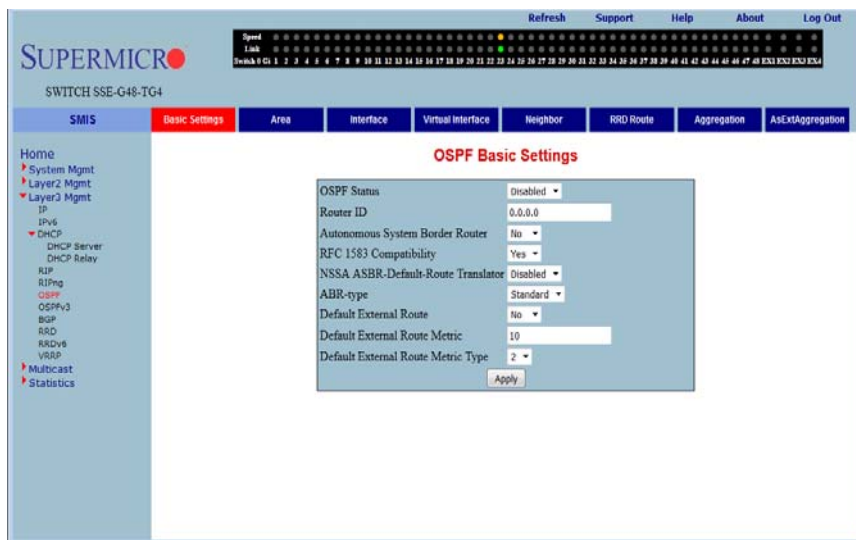
OSPF

The OSPF link allows you to configure the OSPF protocol through the following pages:

- [Basic Settings](#)
- [Area](#)
- [Interface](#)
- [Virtual Interface](#)
- [Neighbor](#)
- [RRD Route](#)
- [Aggregation](#)
- [AsExtAggregation](#)

Basic Settings

Figure 5-114. OSPF Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the OSPF BASIC SETTINGS page (Figure 5-114). The parameters for this page are shown in Table 5-95.

Table 5-95. OSPF Basic Settings Page Parameters

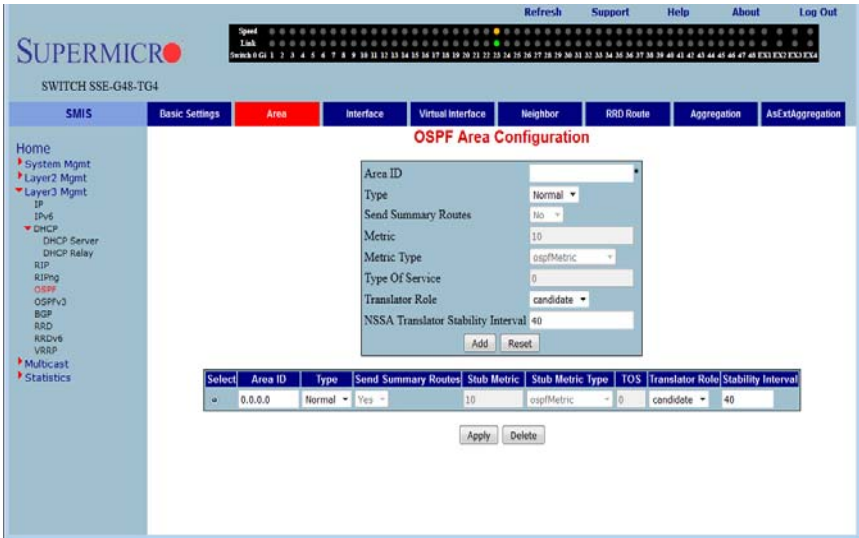
Parameter	Description
OSPF Status	This parameter specifies the global status of the protocol in the switch.
Router ID	This parameter specifies the router identifier.
Autonomous System Border Router	This parameter indicates the flag to denote whether or not the router is to be configured as an Autonomous System Border Router.
RFC 1583 Compatibility	This parameter specifies the compatibility to RFC 1583 for choosing the route among multiple AS for the same destination.
NSSA ASBR-Default-Route Translator	This parameter allows you to either <i>Enable</i> or <i>Disable</i> the NSSA ASBR-Default-Route Translator.
ABR-type	This parameter allows you to choose to configure ABR-type as <i>Standard</i> , CISCO or IBM
NSSA ASBR-Default-Route Translator	This parameter allows you to either <i>Enable</i> or <i>Disable</i> the NSSA ASBR-Default-Route Translator.
ABR-type	This parameter allows you to configure ABR-type as <i>Standard</i> , CISCO or IBM

Table 5-95. OSPF Basic Settings Page Parameters (Continued)

Parameter	Description
Default External Route	This parameter allows you to <i>Enable</i> or <i>Disable</i> the Default External Route.
Default External Route Metric	This parameter specifies the External Route Metric in range 0 to 16777215. The default value is 10 .
Default External Route Metric Type	This parameter allows you to choose to configure the default route metric type as “1” or “2”.
External Link State Database Limit	This parameter specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link state database.

Area

Figure 5-115. OSPF Area Configuration Page



Clicking the AREA tab brings up the OSPF AREA CONFIGURATION page (Figure 5-115). The parameters for this page are shown in Table 5-96.

Table 5-96. OSPF Area Configuration Page Parameters

Parameter	Description
Area ID	This parameter specifies the identifier for the area.
Type	This parameter allows you to configure the area type, as a <i>Stub</i> area, a <i>Normal</i> area or <i>NSSA</i> .

Table 5-96. OSPF Area Configuration Page Parameters (Continued)

Parameter	Description
Send Summary Router	This field is used to control the import of summary LSAs to stub areas. This does not have any impact for other areas.
Metric	This parameter specifies the metric/cost associated with the routes. The allowed value ranges between 0 to 16777215. The default value is 10.

Interface

Figure 5-116. OSPF Interface Configuration Page

The screenshot shows the 'OSPF Interface Configuration' page in the SUPERMICRO web management utility. The page is titled 'OSPF Interface Configuration' and is part of the 'Interface' tab. The configuration form includes the following fields and values:

- Interface: vlan1
- Area ID: 0.0.0.0
- Priority: 1
- Authentication Type: None
- MD5 Key ID: (empty)
- Authentication Key: (empty)
- Metric: 10
- Passive: No
- Demand Circuit: No
- If Type: broadcast
- Transit Delay: 1
- Retransmit Interval: 5
- Hello Interval: 10
- Dead Interval: 40

At the bottom of the page, there is a table with the following columns: Select, IP Address, Area ID, Priority, Designated Router, Authen Type, MD5 Key id, Authen Key, Metric, Passive, Demand Circuit, If Type, Transit Delay, Retransmit Delay, Hello Interval, and Router Dead Interval.

Clicking the INTERFACE tab brings up the OSPF INTERFACE CONFIGURATION page (Figure 5-116). The parameters for this page are shown in Table 5-97.

Table 5-97. OSPF Interface Configuration Page Parameters

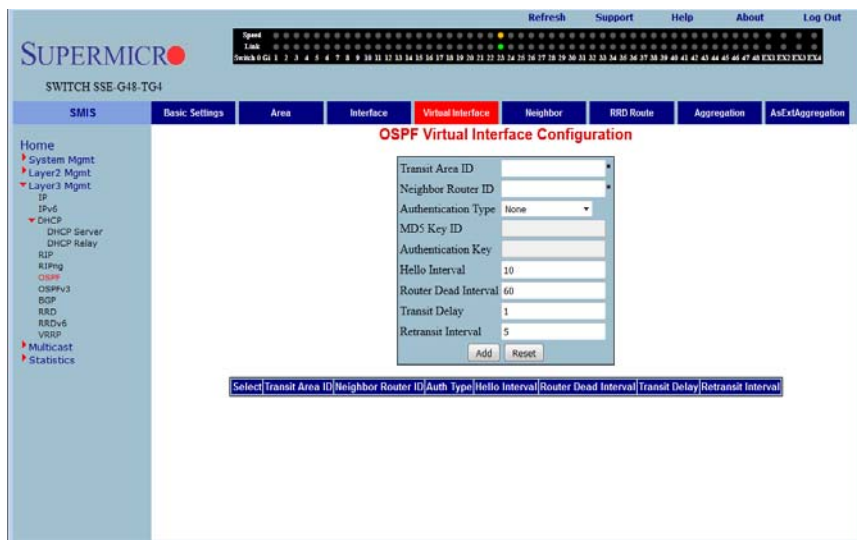
Parameter	Description
Interface	This parameter specifies the interface index of the port.
Area ID	This parameter indicates the 32-bit integer uniquely identifying the area to which the interface connects.
Priority	This parameter specifies the priority of this interface, which is used in the DR election algorithm. The allowed value ranges between 0 and 255. The default value is 1.
Authentication Type	This parameter allows you to choose <i>MD5</i> , <i>Simple Password</i> or <i>None</i> as the authentication type.

Table 5-97. OSPF Interface Configuration Page Parameters (Continued)

Parameter	Description
MD5 Key ID	This parameter specifies the secret key used to create the message digest appended to the OSPF packet, if the authentication type is <i>MD5</i> .
Authentication Key	This parameter specifies the key required for authentication, if authentication is enabled on this interface.
IP Address	This parameter specifies the IP Address of the OSPF interface.
Designated Router	This read-only field specifies the IP Address of the Designated Router.
Metric	Specifies the metric assigned to this interface. The allowed value ranges between 0 to 16777215. The default value is 10.
Passive	This parameter allows you to choose <i>Enable</i> or <i>Disable</i> . The passive-interface command disables OSPF hellos from being sent out, thus disabling the interface from forming adjacencies on that interface.
Demand Circuit	A demand circuit is a point-to-point connection between two neighboring interfaces configured for the OSPF. This parameter allows you to <i>Enable</i> or <i>Disable</i> the demand circuit.
If Type	Specifies the type of OSPF interface (<i>Broadcast</i> , <i>NBMA</i> , <i>Point-to-point</i> , or <i>Point-to-multipoint</i>).
Transit Delay	This parameter indicates the estimated number of seconds to transmit a link state update packet over the interface. The allowed value ranges between 0 to 3600. The default value is 1 second.
Retransmit Interval	This parameter indicates the number of seconds between the link-state advertisement retransmissions, for adjacencies belonging to the interface. The allowed value ranges between 0 to 3600. The default value is 5.
Hello Interval	This parameter indicates the length of time, in seconds, between the Hello packets that the router sends on the interface. The allowed value ranges between 1 to 65535. The default value is 10.
Dead Interval	This parameter specifies the number of seconds for which the router waits for hello packet from the neighbor before declaring this neighbor down. The allowed value ranges between 0 to 2147483647. The default value is 40.

Virtual Interface

Figure 5-117. OSPF Virtual Interface Configuration Page



Clicking the VIRTUAL INTERFACE tab brings up the OSPF VIRTUAL INTERFACE CONFIGURATION page (Figure 5-117). The parameters for this page are shown in Table 5-98.

Table 5-98. OSPF Virtual Interface Configuration Page Parameters

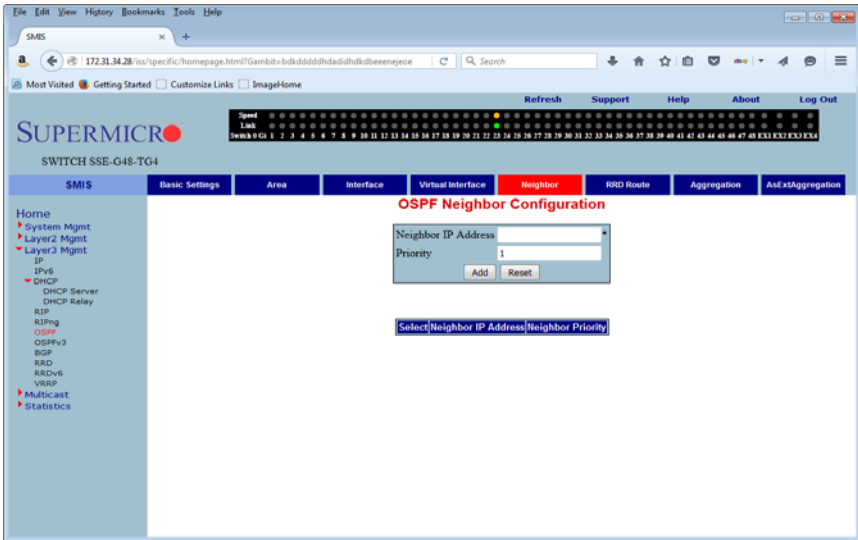
Parameter	Description
Transit Area ID	This parameter specifies the transit area that the virtual link traverses.
Neighbor Router ID	This parameter specifies the router ID of the virtual neighbor.
Authentication Type	This parameter allows you to choose <i>MD5</i> , <i>Simple Password</i> or <i>None</i> as the authentication type.
MD5 Key ID	This parameter specifies the secret key used to create the message digest appended to the OSPF packet if the authentication type is <i>MD5</i> .
Authentication Key	This parameter specifies the key required for authentication, if authentication is enabled on this interface.
Hello Interval	This parameter indicates the length of time, in seconds, between the Hello packets that the router sends on the interface. The allowed value ranges between 1 and 65535. The default value is 10.
Route Dead Interval	This parameter specifies the number of seconds for which the router waits for hello packet from the neighbor before declaring this neighbor down. The allowed value ranges between 0 and 2147483647. The default value is 60.

Table 5-98. OSPF Virtual Interface Configuration Page Parameters (Continued)

Parameter	Description
Transit Delay	This parameter indicates the estimated number of seconds to transmit a link state update packet over the interface. The allowed value ranges between 0 and 3600. The default value is 1 second.
Retransmit Interval	This parameter indicates the number of seconds between the link-state advertisement retransmissions, for adjacencies belonging to the interface. . The allowed value ranges between 0 and 3600. The default value is 5.

Neighbor

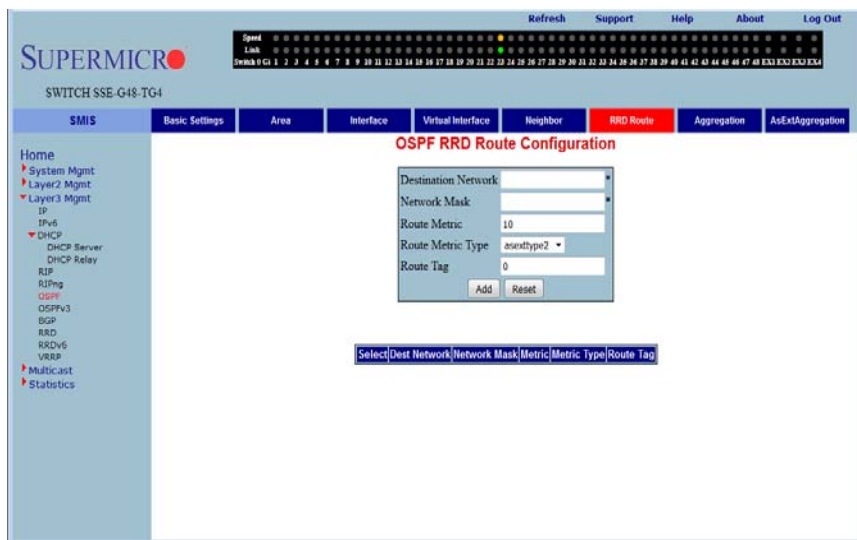
Figure 5-118. OSPF Neighbor Configuration Page



Clicking the NEIGHBOR tab brings up the OSPF NEIGHBOR CONFIGURATION page (Figure 5-118), which allows you to configure OSPF neighbors. The parameters for this page are shown in Table 5-99.

Table 5-99. OSPF Neighbor Configuration Page Parameters

Parameter	Description
Neighbor IP Address	This parameter specifies the neighbor router ID.
Priority	This parameter specifies a number value for the router priority.

RRD Route**Figure 5-119. OSPF RRD Route Configuration Page**

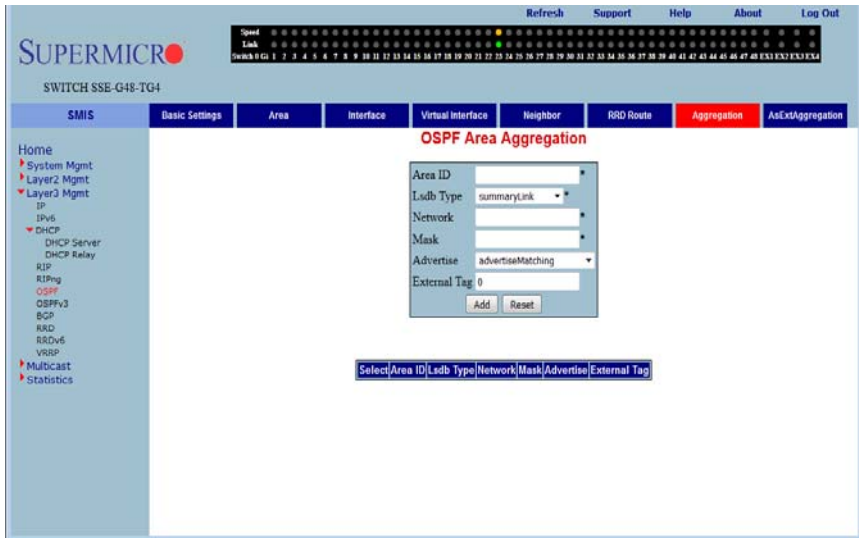
Clicking the RRD ROUTE tab brings up the OSPF RRD ROUTE CONFIGURATION page (Figure 5-119), which displays the various parameters for RRD Route configuration. The parameters for this page are shown in Table 5-100.

Table 5-100. OSPF RRD Route Configuration Page Parameters

Parameter	Description
Destination Network	This parameter specifies the DESTINATION NETWORK.
Network Mask	This parameter specifies the NETWORK MASK.
Route Metric	This parameter specifies the ROUTE METRIC.
Route Metric Type	This parameter specifies the ROUTE METRIC TYPE.
Route Tag	This parameter specifies the ROUTE TAG.

Aggregation

Figure 5-120. OSPF Area Aggregation Page



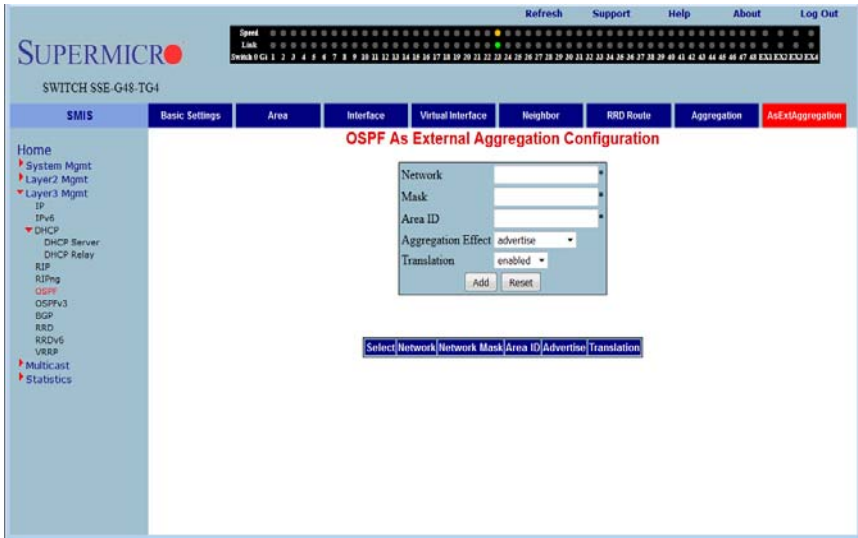
Clicking the AGGREGATION tab brings up the OSPF AREA AGGREGATION page (Figure 5-120). The parameters for this page are shown in Table 5-101.

Table 5-101. OSPF Area Aggregation Page Parameters

Parameter	Description
Area ID	This parameter specifies the area associated with the OSPF address range. It is specified as an IP address.
Lsdb Type	This parameter specifies the link state data base type as a <i>Summary Link</i> or as a <i>NSSA External Link</i> .
Network	This parameter specifies the network address.
Mask	This parameter specifies the network mask.
Advertise	This parameter specifies the advertise option as <i>Advertise Matching</i> or <i>Do Not Advertise Matching</i> .
External Tag	This parameter is not used by the OSPF protocol itself. It may be used to communicate information between AS boundary routers. The precise nature of this information is outside the scope of OSPF.

AsExtAggregation

Figure 5-121. OSPF As External Aggregation Configuration Page



Clicking the ASEXTAGGREGATION tab brings up the OSPF AS EXTERNAL AGGREGATION CONFIGURATION page (Figure 5-121), which allows you to configure OSPF external aggregation parameters. The parameters for this page are shown in Table 5-102.

Table 5-102. OSPF As External Aggregation Configuration Page Parameters

Parameter	Description
Network	This parameter specifies the external network address.
Mask	This parameter specifies the network mask.
Area ID	This parameter specifies the Area identifier.

Table 5-102. OSPF As External Aggregation Configuration Page Parameters

Parameter	Description
Aggregation Effect	<p>This parameter specifies the Aggregation option as one of the following:</p> <ul style="list-style-type: none"> • Advertise – When set to <i>advertise</i> and associated Area ID is 0.0.0.0, then the aggregated Type-5 are generated. Otherwise if the associated Area ID is x.x.x.x (other than 0.0.0.0), then the aggregated Type-7 is generated in NSSA x.x.x.x for the specified range. • Do Not Advertise – When set to <i>doNotAdvertise (2)</i> and associated Area ID is 0.0.0.0, then the Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if the associated Area ID is x.x.x.x (other than 0.0.0.0), then the Type-7 are not generated in NSSA x.x.x.x for the specified range. • Allow All – When set to <i>allowAll</i> and associated Area ID is 0.0.0.0, then the aggregated Type-5 are generated for the specified range. In addition aggregated Type-7 are generated in all attached NSSA for the specified range. • Deny All – When set to <i>denyAll</i> neither Type-5 nor Type-7 will be generated for the specified range.
Translation	This parameter enables or disables the translation.
Advertise	This parameter displays the aggregation status of OSPF.

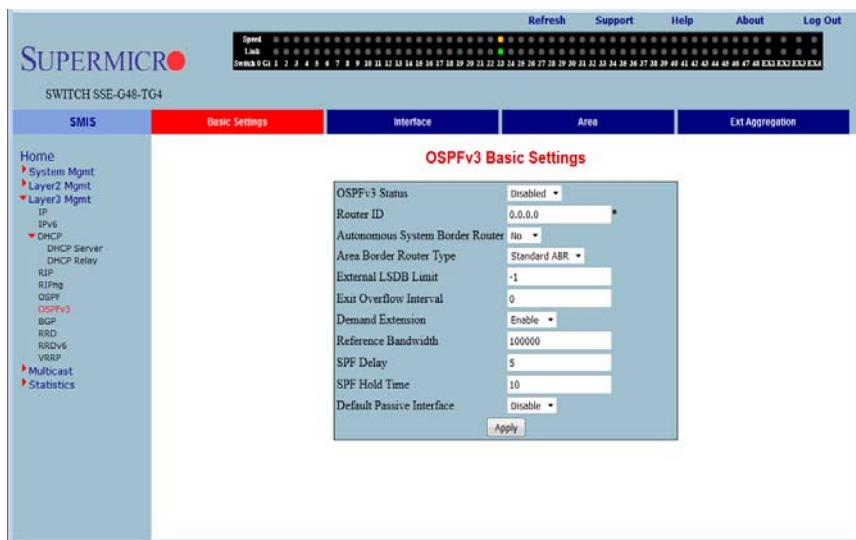
OSPF V3

The OSPFv3 link allows you to configure the OSPFv3 protocol through the following pages:

- [Basic Settings](#)
- [Interface](#)
- [Area](#)
- [Ext Aggregation](#)

Basic Settings

Figure 5-122. OSPFv3 Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the OSPFv3 BASIC SETTINGS page (Figure 5-122). The parameters for this page are shown in Table 5-103.

Table 5-103. OSPFv3 Basic Settings Page Parameters

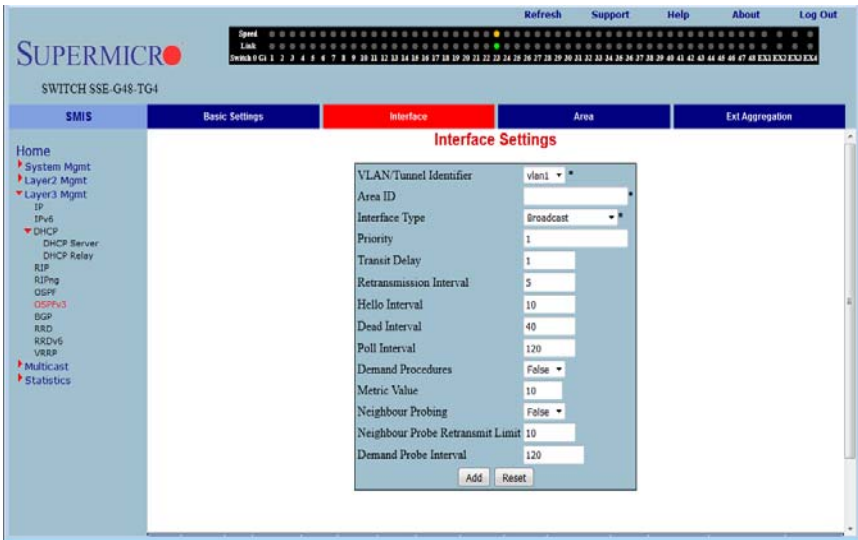
Parameter	Description
OSPFv3 Status	This parameter enables or disables OSPFv3 administratively.
Router ID	This parameter uniquely identifies the router in the Autonomous System.
Autonomous System Border Router Status	This parameter specifies the router as Autonomous System border router.
Area Border Router	This parameter specifies the router as an area border router.
External LSDB Limit	This parameter specifies maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	This parameter specifies the time interval in seconds a router will attempt to leave Overflow State. The allowed value ranges between 1 and 65535.
Demand Extension	This parameter indicates the router's support for demand routing.
Reference Bandwidth	This parameter specifies Reference bandwidth in kilobits/seconds for calculating default interface metrics. The allowed value ranges between 1 and 65535.
SPF Delay	This parameter indicates the delay in routing calculation after a topology change. The allowed value ranges between 1 and 65535. The default value is 5.

Table 5-103. OSPFv3 Basic Settings Page Parameters (Continued)

Parameter	Description
SPF Hold Time	This parameter specifies the minimum time between two consecutive SPF calculations. The allowed value ranges between 1 and 65535. The default value is 10.
Default Passive Interface	This parameter specifies whether all the OSPFv3 interfaces created after this setting are passive or not.
Trace Level	This parameter defines the level of trace required for OSPFv3.

Interface

Figure 5-123. Interface Settings Page



Clicking the INTERFACE tab brings up the INTERFACE SETTINGS page (Figure 5-123). The parameters for this page are shown in Table 5-104.

Table 5-104. Interface Settings Page Parameters

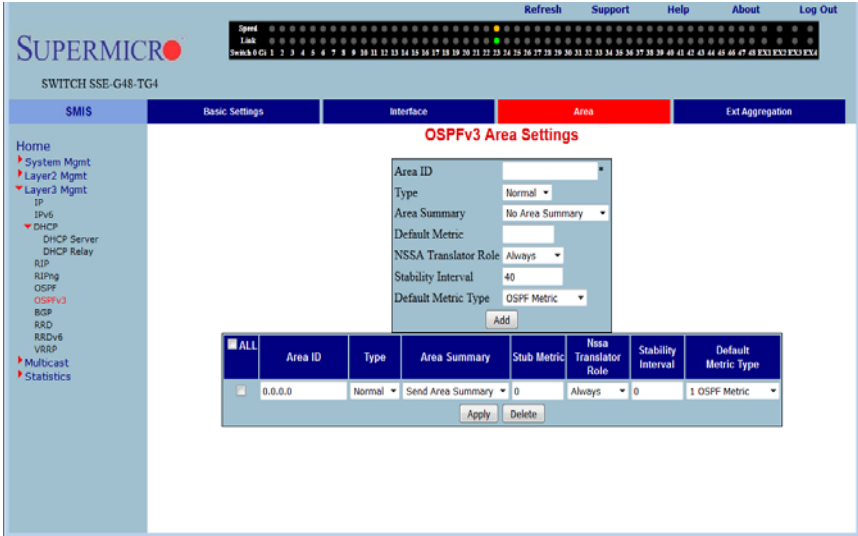
Parameter	Description
VLAN/Tunnel Identifier	This parameter specifies the IPv6 interface over which OSPFv3 is enabled.
Area ID	This parameter specifies the area ID associated with the IPv6 interface.
Interface Type	This parameter specifies the type of OSPFv3 interface (broadcast, nbma, pointToPoint and pointToMultipoint).
Priority	This parameter specifies the priority of the interface. The allowed value ranges between 0 and 255. The default value is 1.

Table 5-104. Interface Settings Page Parameters (Continued)

Parameter	Description
Transit Delay	This parameter indicates the estimated number of seconds to transmit a link state update packet over the interface. The allowed value ranges between 0 and 3600. The default value is 1.
Retransmission Interval	This parameter indicates the number of seconds between the link-state advertisement retransmissions, for adjacencies belonging to the interface. The allowed value ranges between 0 and 3600. The default value is 5.
Hello Interval	This parameter indicates the length of time, in seconds, between the Hello packets that the router sends on the interface. The allowed value ranges between 1 and 65535. The default value is 10.
Dead Interval	This parameter specifies the number of seconds for which the router waits for hello packet from the neighbor before declaring this neighbor down. The allowed value ranges between 0 and 2147483647. The default value is 40.
Poll Interval	This parameter denotes the larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
Demand Procedures	This parameter indicates whether Demand OSPFv3 procedures must be performed on this interface.
Metric Value	This parameter specifies the metric assigned to this interface. The allowed value ranges between 0 and 16777215. The default value is 10.
Neighbour Probing	This parameter enables or disables neighbor probing to determine whether the neighbor is active or inactive.
Neighbour Probe Retransmit Limit	This parameter indicates the number of consecutive LSA retransmissions before the neighbor is deemed inactive and the neighbor adjacency is brought down. The default value is 10.
Demand Probe Interval	This parameter defines how often the neighbor is probed. The default value is 120.

Area

Figure 5-124. OSPFv3 Area Settings Page



Clicking the AREA tab brings up the OSPFv3 AREA SETTINGS page (Figure 5-124). The parameters for this page are shown in Table 5-105.

Table 5-105. OSPFv3 Area Settings Page Parameters

Parameter	Description
Area ID	This parameter uniquely identifies an area.
Type	This parameter indicates whether an area is a <i>Stub</i> area, <i>NSSA</i> , or <i>Standard</i> (normal) area.
Area Summary	This parameter controls the import of Inter-Area LSAs into stub areas. This can be <i>noAreaSummary</i> or <i>sendAreaSummary</i> .
Stub Metric	This parameter indicates the metric value advertised for the default route into <i>Stub</i> area and <i>NSSA</i> .
NSSA Translator Role	This parameter specifies the NSSA Border router's ability to perform NSSA translation of type-7 LSAs into type-5 LSAs.
NSSA Stability Interval	This parameter specifies the number of seconds after an elected translator determines its services are no longer required, in which it must continue to perform its translation duties.
Stub Metric Type	This parameter specifies the type of metric (<i>OSPFv3 Metric</i> , <i>External Type 1</i> , <i>External Type 2</i>) advertised as a default route.

Ext Aggregation

Figure 5-125. OSPF AS External Aggregation Configuration Page

The screenshot shows the SUPERMICR web management utility interface. At the top, there is a status bar with 'Open' and 'Link' indicators, and navigation links for 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. Below this is the device name 'SWITCH SSE-G48-TG4'. The main navigation menu on the left includes 'Home', 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'IP', 'IPv6', 'DHCP', 'DHCP Server', 'DHCP Relay', 'RIP', 'RIPng', 'OSPF', 'OSPFv3', 'BGP', 'RBD', 'RRDv6', 'VRRP', 'Multicast', and 'Statistics'. The 'OSPFv3' option is highlighted in red. The main content area is titled 'OSPF As External Aggregation Configuration' and contains a form with the following fields: 'Summary Prefix' (text input), 'Prefix Length' (text input), 'Area ID' (text input), 'Aggregation Effect' (dropdown menu set to 'advertise'), and 'Translation' (dropdown menu set to 'enabled'). There are 'Add' and 'Reset' buttons at the bottom of the form. A status bar at the bottom of the form reads 'Select|Prefix|Prefix Length|Area ID|advertise|Translation'.

Clicking the EXT AGGREGATION tab brings up the OSPF AS EXTERNAL AGGREGATION CONFIGURATION page (Figure 5-125), which allows you to configure OSPF external aggregation parameters. The parameters for this page are shown in Table 5-106.

Table 5-106. OSPF AS External Aggregation Configuration Page Parameters

Parameter	Description
Summary Prefix	This parameter specifies the summary prefix for external aggregation.
Prefix Length	This parameter specifies the length of the prefix. The allowed value ranges between 1 to 128.
Area ID	This parameter specifies the Area identifier.

Table 5-106. OSPF AS External Aggregation Configuration Page Parameters

Parameter	Description
Aggregation Effect	<p>This parameter specifies the Aggregation option as one of the following:</p> <ul style="list-style-type: none"> • Advertise – When set to <i>advertise</i> and the associated Area ID is 0.0.0.0, then aggregated Type-5 are generated. Otherwise if associated Area ID is x.x.x.x (other than 0.0.0.0), then aggregated Type-7 is generated in NSSA x.x.x.x for the specified range. • Do Not Advertise – When set to <i>doNotAdvertise (2)</i> and the associated Area ID is 0.0.0.0, then Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While associated Area ID is x.x.x.x (other than 0.0.0.0), then Type-7 are not generated in NSSA x.x.x.x for the specified range. • Allow All – When set to <i>allowAll</i> and associated Area ID is 0.0.0.0, then aggregated Type-5 are generated for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified range. • Deny All – When set to <i>denyAll</i> neither Type-5 nor Type-7 will be generated for the specified range.
Translation	This parameter enables or disables the translation.
Advertise	This parameter displays the aggregation status of OSPF V3.

BGP

The BGP link allows you to configure the BGP protocol. Following are the configuration parameters available to manage BGP through this interface:

- [Basics](#)
- [Neighbors](#)
- [Multi-Exit Disc](#)
- [Local Pref](#)
- [Filters](#)
- [Route Aggr](#)
- [Advanced](#)
- [Community](#)

Basics

Figure 5-126. BGP Basic Settings Page

Refresh Support Help About Log Out

Speed
Link
Switch 0 Gi 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 E33 E33 E33 E33

SUPERMICR
SWITCH SSE-G48-TG4

SMIS Basics Neighbors Multi-Exit Disc Local Pref Filters Route Aggr Advanced Community

Home
System Mgmt
Layer2 Mgmt
Layer3 Mgmt
IP
IPv6
DHCP
DHCP Server
DHCP Relay
RIP
RIPng
OSPF
OSPFv3
BGP
RBD
RRDv6
VRRP
Multicast
Statistics

BGP Basic Settings

Status Disabled
AS Number 0
Router ID 0.0.0.0
Synchronization Disabled
Overlap Router Policy Both
Default Local Preference 100
Advertisement of Non - BGP Routes ExternalAndInternal
Always Compare MED Disabled
Apply

Note : To enable BGP Functionality, Route Redistribution should be enabled.

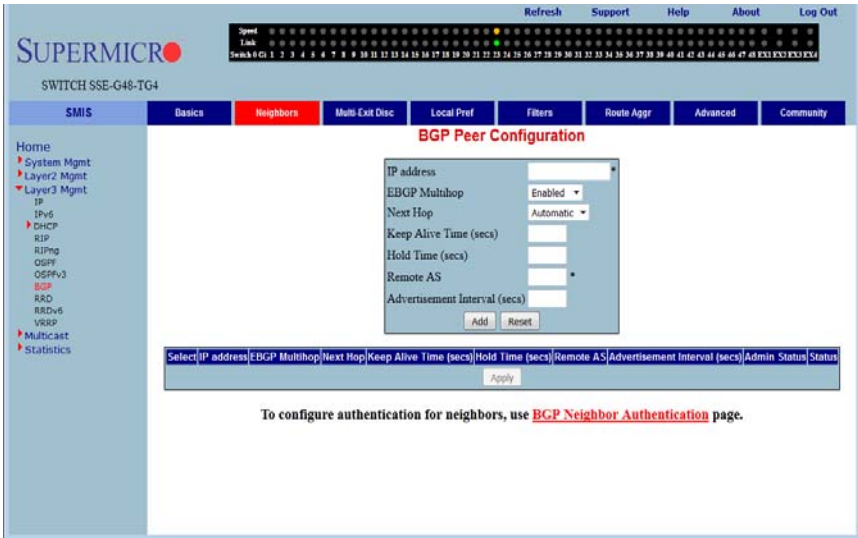
Clicking the BASICS tab brings up the BGP BASIC SETTINGS page (Figure 5-126). The parameters for this page are shown in Table 5-107.

Table 5-107. BGP Basic Settings Page Parameters

Parameter	Description
Status	This parameter specifies the BGP administration status. Using this, the protocol can be enabled/disabled in the switch.
AS Number	This parameter specifies the autonomous system to which the switch is connected, which is a read-only field. The allowed value ranges between 1 to 65535. The default value is 0.
Synchronization	The synchronization between IGP and BGP can be ensured by enabling this field.
Router ID	This parameter specifies the router address.
Overlap Router Policy	This parameter represents the policy for handling overlapping routes. When an overlapping route is received, depending upon the configured policy, either the less-specific routes or most-specific routes or both are installed in the RIB tree.
Default Local Preference	This parameter sets a preference value for the autonomous system path.
Advertisement of Non-BGP Routes	You can choose to advertise even the external non-BGP routes by enabling this feature.
Always Compare MED	By enabling this feature, you can choose to always compare the MED values of paths from different neighbors for the same prefix, for choosing the best path.

Neighbors

Figure 5-127. BGP Peer Configuration Page



Clicking the NEIGHBORS tab brings up the BGP PEER CONFIGURATION page (Figure 5-127), which allows you to configure BGP Neighbors. The parameters for this page are shown in Table 5-108.

Table 5-108. BGP Peer Configuration Page Parameters

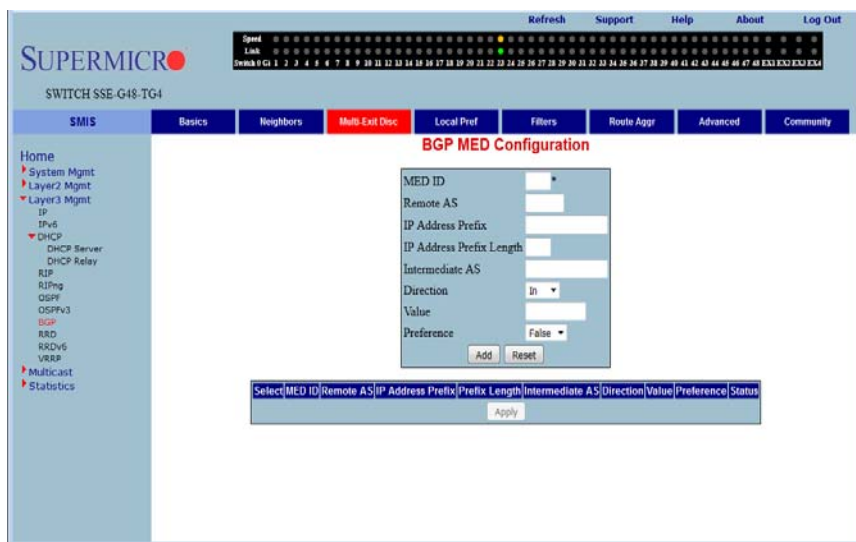
Parameter	Description
IP Address	This parameter specifies the IP address of the BGP neighbor.
EBGP MultiHop	By enabling this feature, BGP connections can be established between peers, which are not directly connected.
Next Hop	Using this parameter, next Hop can be set as <i>Self</i> or <i>Automatic</i> . By setting this field to <i>Self</i> , you can make the switch the next hop for all the routes that it distributes to its peers.
Keep Alive Time (Seconds)	This parameter specifies the maximum time interval between successive updates between any two BGP peers. The allowed value ranges from 0 to 21845.
Hold Time (Seconds)	This parameter specifies the Hold time. This is the timer interval that a BGP will wait, before it decides that a connection to the peer is torn down. The allowed value ranges from 3 to 65535.
Remote AS	This parameter represents the remote autonomous system number. The allowed value ranges from 0 to 65535.
Advertisement Interval (seconds)	This parameter specifies the interval in seconds for the Minimum Route advertisement interval timer. The allowed value ranges from 1 to 65535.

Table 5-108. BGP Peer Configuration Page Parameters (Continued)

Parameter	Description
Admin Status	This parameter displays the admin status of the entry.
Status	This parameter specifies the status of the entry.

Multi-Exit Disc

Figure 5-128. BGP MED Configuration Page



Clicking the MULTI-EXIT DISC tab brings up the BGP MED CONFIGURATION page (Figure 5-128), which allows you to configure the MED value for routes learnt from BGP peers. The parameters for this page are shown in Table 5-109.

Table 5-109. BGP MED Configuration Page Parameters

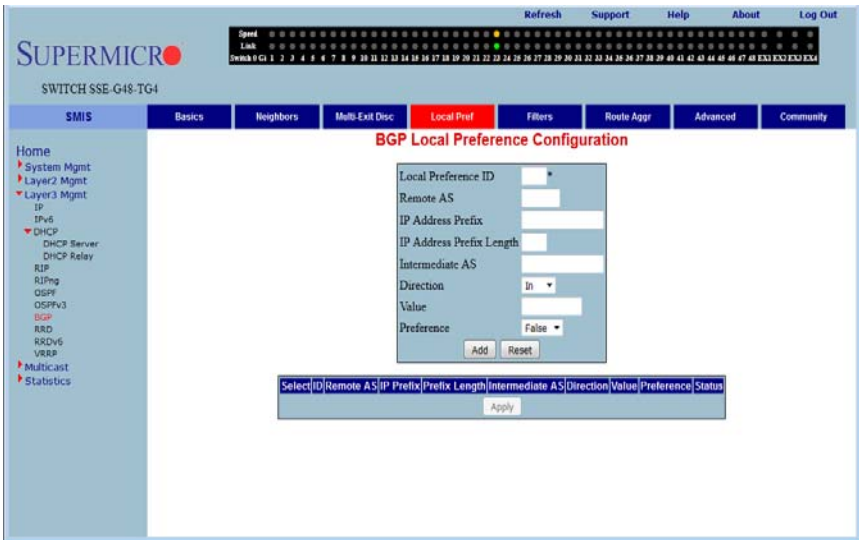
Parameter	Description
MED ID	This parameter specifies the index for this table. The allowed value ranges between 1 and 10.
Remote AS	This parameter specifies the AS number from which the route update is received. The allowed value ranges between 0 and 65535.
IP Address Prefix	This parameter specifies the IP address prefix for which the update is received.
IP Address Prefix Length	This parameter is used to calculate the subnet. The allowed value ranges between 0 and 32.
Intermediate AS	This parameter represents the intermediate AS between the BGP peers.

Table 5-109. BGP MED Configuration Page Parameters (Continued)

Parameter	Description
Direction	This parameter can be set for the incoming or the outgoing packets using <i>In</i> and <i>Out</i> values.
Value	This parameter specifies the MED value to be associated with this path learned. The allowed value ranges between 0 and 32.
Preference	This parameter is used to enable/disable filtering.
Status	This parameter indicates the status of the entry.

Local Pref

Figure 5-129. BGP Local Preference Configuration Page



Clicking the LOCAL PREF tab brings up the BGP LOCAL PREFERENCE CONFIGURATION page (Figure 5-129), which allows you to configure the Local Preference value for routes. The parameters for this page are shown in Table 5-110.

Table 5-110. BGP Local Preference Configuration Page Parameters

Parameter	Description
Local Preference ID	This parameter specifies the Local Preference ID, which is the index for this table. The allowed value ranges between 1 and 10.
Remote AS	This parameter specifies the AS number from which the route update is received. The allowed value ranges between 0 and 65535.
IP Address Prefix	This parameter specifies the IP Address prefix for which the update is received.

Table 5-110. BGP Local Preference Configuration Page Parameters (Continued)

Parameter	Description
IP Address Prefix Length	This parameter is used to calculate the subnet. The allowed value ranges between 0 and 32.
Intermediate AS	This parameter represents the intermediate AS between the BGP peers.
Direction	This parameter can be set for the incoming or the outgoing packets using <i>In</i> and <i>Out</i> values.
Value	This parameter specifies the Local preference value to be associated with this learnt path. The allowed value ranges between 0 and 2147483647.
Preference	This parameter is used to enable/disable filtering.
Status	This parameter specifies the status of the entry.

Filters

Figure 5-130. BGP Filter Configuration Page

The screenshot shows the SUPERMICRO web-based management utility interface. The main navigation bar includes tabs for SMIS, Basics, Neighbors, Multi-Exit Disc, Local Pref, **Filters**, Route Aggr, Advanced, and Community. The left sidebar contains a tree view for system management, including System Mgmt, Layer2 Mgmt, Layer3 Mgmt, IP, IPv6, DHCP, DHCP Relay, RIP, OSPF, OSPFv3, BGP, RRD, RRDv6, VRRP, Multicast, and Statistics. The 'Filters' tab is selected, displaying the 'BGP Filter Configuration' page. The configuration form includes the following fields and controls:

- Filter ID:
- Remote AS:
- IP Address:
- IP Address Prefix Length:
- Intermediate AS:
- Direction:
- Action:
- Buttons: Add, Reset

Below the form is a table with the following columns: Select, Filter ID, Remote AS, IP Address, Prefix Length, Intermediate AS, Direction, Action, Status. An Apply button is located below the table.

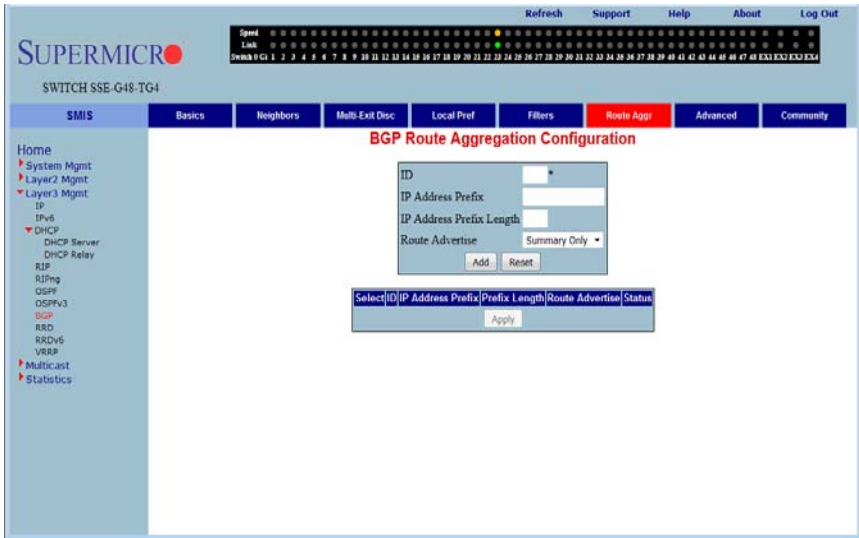
Clicking the FILTERS tab brings up the BGP FILTER CONFIGURATION page (Figure 5-130), which is used to set the filters on the routes being learnt. The parameters for this page are shown in Table 5-111.

Table 5-111. BGP Filter Configuration Page Parameters

Parameter	Description
Filter ID	This parameter specifies the filter index. The allowed value ranges between 1 and 10.
Remote AS	This parameter specifies the remote AS associated with the BGP peer from which the router is being distributed. The allowed value ranges between 0 and 65535.
IP Address	This parameter specifies the IP address for which the route is being learned.
IP Address Prefix Length	This parameter specifies the prefix length to calculate the Subnet. The allowed value ranges between 0 and 32.
Intermediate AS	This parameter represents the intermediate AS between the BGP peers.
Direction	This parameter indicates the direction of the packet.
Action	With this parameter you can choose either to <i>Allow</i> (not to filter) or <i>Deny</i> (Filter) for the above configuration set.
Status	This parameter specifies the status of the entry.

Route Aggr

Figure 5-131. BGP Route Aggregation Configuration Page



Clicking the ROUTE AGGR tab brings up the BGP ROUTE AGGREGATION CONFIGURATION page (Figure 5-131), which is used to aggregate and configure the routes advertised by BGP. The parameters for this page are shown in Table 5-112.

Table 5-112. BGP Route Aggregation Configuration Page Parameters

Parameter	Description
ID	This parameter specifies the index to this table. The allowed value ranges between 1 and 10.
IP Address Prefix	This parameter specifies the IP address prefix that needs to be aggregated.
IP Address Prefix Length	This parameter, in combination with the IP Prefix, decides the aggregated route to be distributed by this switch. The allowed value ranges between 0 and 32.
Route Advertise	With this parameter you can either choose to advertise only the aggregated routes by setting <i>Summary only</i> , or choose to advertise all routes by setting <i>All</i> .
Status	This parameter specifies the status of the entry.

Advanced

Figure 5-132. Advanced BGP Configuration Page

The screenshot shows the SUPERMICRO web management utility interface. The top navigation bar includes 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. The main navigation tabs are 'SMIS', 'Basics', 'Neighbors', 'Multi-Exit Desc', 'Local Pref', 'Filters', 'Route Aggr', 'Advanced' (highlighted in red), and 'Community'. The left sidebar shows a tree view of configuration options under 'Layer3 Mgmt', including 'BGP'. The main content area displays the 'Advanced BGP Configuration' page with the following parameters:

Client to Client Reflection	Enabled
Dampening Half Life Time	900
Dampening Reuse Value	500
Dampening Suppress Value	3500
Dampening Max Suppress Time	3600
Dampening Decay Granularity	1
Dampening Reuse Granularity	15
Dampening Reuse Array Size	1024
Confederation Identifier	0
Best Path MED Confed	Disabled
Confederation Peers	Add: <input type="text"/> Remove: <input type="text"/>

An 'Apply' button is located at the bottom of the configuration area.

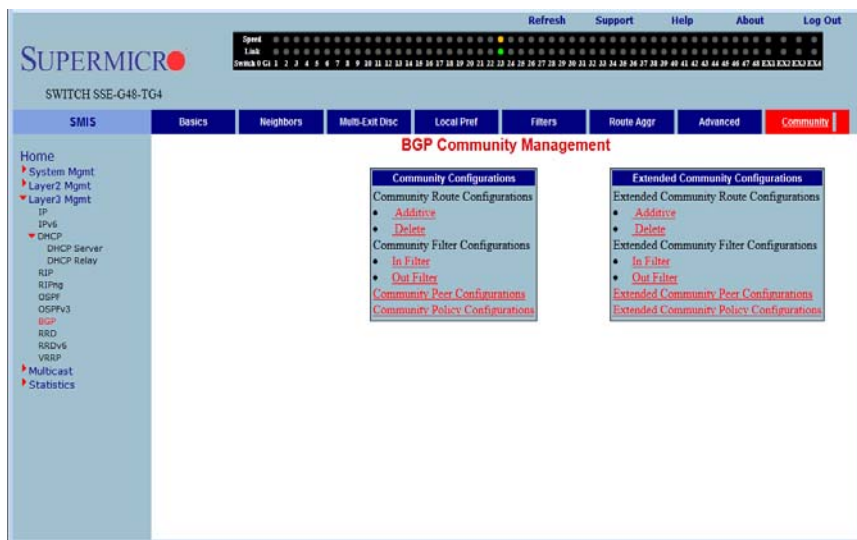
Clicking the ADVANCED tab brings up the ADVANCED BGP CONFIGURATION page (Figure 5-132), which configures dampening and confederation parameters. The parameters for this page are shown in Table 5-113.

Table 5-113. Advanced BGP Configuration Page Parameters

Parameter	Description
Client to Client Reflection	<p>This parameter configures the Route Reflector to support route reflection to client peers.</p> <p>By default, the Route Reflector will reflect routes learnt from a client peer to all other client peers. If required, the administrator can disable this feature by disabling client-to-client reflection.</p> <p>If disabled, then the Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector.</p>
Dampening Half Life Time	This parameter specifies the time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased by half after the half-life time. The possible values are between 600 and 2700. The default value is 900.
Dampening Reuse Value	If the penalty associated with a suppressed route falls below this value, the route is re-used. The possible values are between 15 and 10800. The default value is 500.
Dampening Suppress Value	A route is suppressed when the penalty associated with the route exceeds this value. The possible values are between 2000 and 3999. The default value is 3500.
Dampening Max Suppress Time	This parameter specifies the maximum time (in seconds) a route can be suppressed. The possible values are between 1800 and 10800. The default value is 3600.
Dampening Decay Granularity	This parameter specifies the time granularity in seconds used to perform all decay computations. The possible values are between 1 and 10800. The default value is 1.
Dampening Reuse Granularity	This parameter specifies the time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment. The possible values are between 15 and 10800. The default value is 15.
Dampening Reuse Array Size	This parameter specifies the size of the reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists, when suppressed for a long time. The possible values are between 256 and 65535. The default value is 1024.
Confederation Identifier	This parameter specifies the BGP confederation identifier. The possible values are between 1 to 65535. Configuring 0 removes the existing configuration.
Best Path MED Confed	This parameter enables or disables MED comparison among paths learnt from confed peers.
Confederation Peers	This parameter configures the ASs that belongs to the confederation.

Community

Figure 5-133. BGP Community Management Page



Clicking the COMMUNITY tab brings up the BGP COMMUNITY MANAGEMENT page (Figure 5-133), which configures BGP community and extended community parameters. The parameters for this page are shown in Table 5-114.

Table 5-114. BGP Community Management Page Parameters

Parameter	Description
Community Route Configurations	This parameter configures an entry in the Additive or Delete Community table.
Community Filter Configurations	This parameter configures the permit or deny function for the community attribute while receiving or advertising.
Community Peer Configurations	This parameter enables or disables advertisement of community attributes to the peer.
Community Policy Configurations	This parameter configures the community attribute advertisement policy for a specific destination.
Extended Community Route Configurations	This parameter configures an entry in the Additive or Delete Extended Community table.
Extended Community Filter Configurations	This parameter configures the permit or deny function for the Extended Community attribute while receiving or advertising.
Extended Community Peer Configurations	This parameter enables or disables advertisement of the Extended Community attributes to the peer.
Extended Community Policy Configurations	This parameter configures the Extended Community attribute advertisement policy for the specific destination.

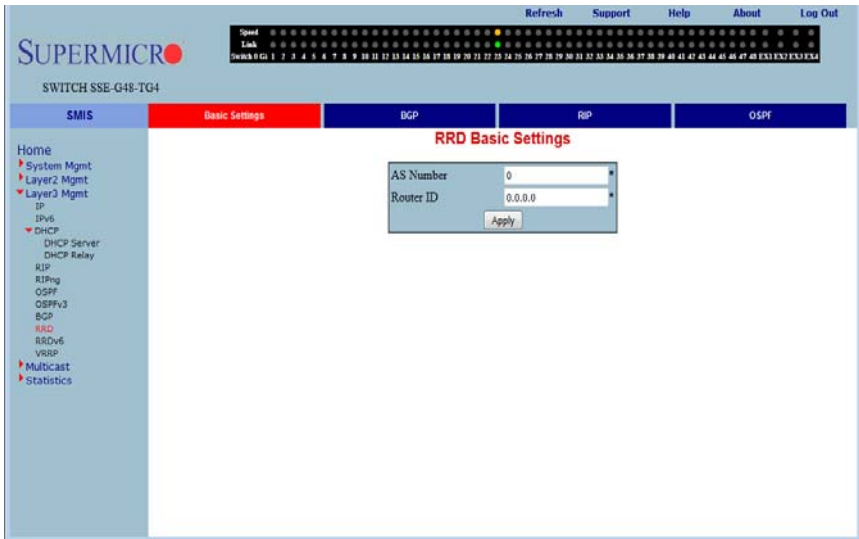
RRD

The RRD link allows you to manage the Route Redistribution with the help of the following pages:

- [Basic Settings](#)
- [BGP](#)
- [RIP](#)
- [OSPF](#)

Basic Settings

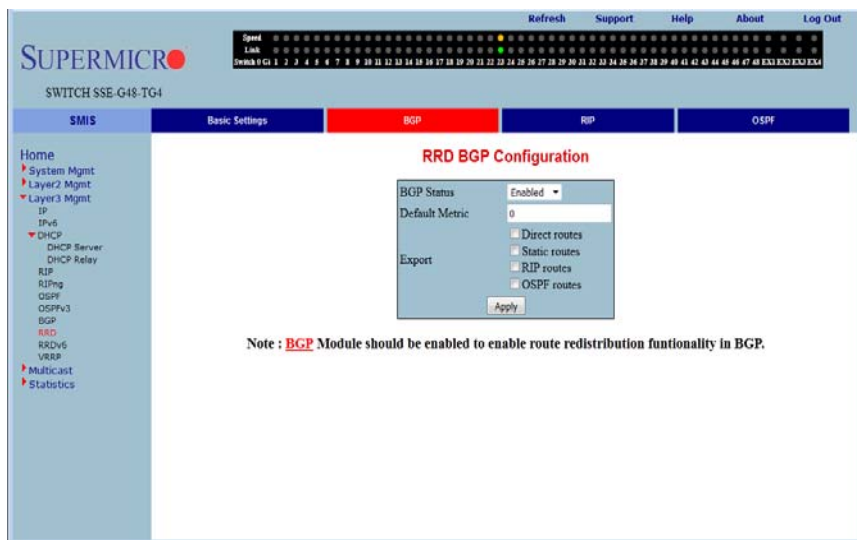
Figure 5-134. RRD Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the RRD BASIC SETTINGS page (Figure 5-134). The parameters for this page are shown in Table 5-115.

Table 5-115. RRD Basic Settings Page Parameters

Parameter	Description
AS Number	This parameter is used to configure the Router AS number to which this switch belongs.
Router ID	This parameter represents the Router ID of the switch.

BGP**Figure 5-135. RRD BGP Configuration Page**

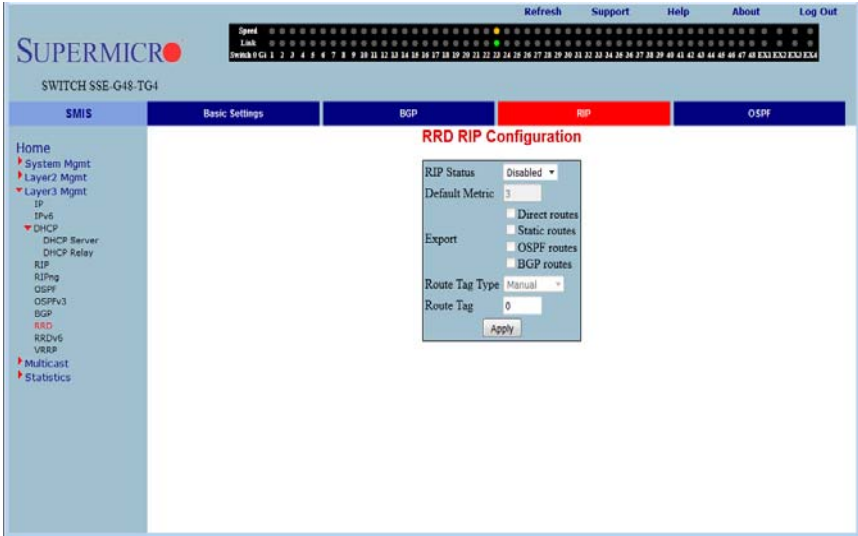
Clicking the BGP tab brings up the RRD BGP CONFIGURATION page (Figure 5-135), which allows you to re-distribute the routes that are learnt through other routing protocols to BGP. The parameters for this page are shown in Table 5-116.

Table 5-116. RRD BGP Configuration Page Parameters

Parameter	Description
BGP Status	This parameter enables or disables redistribution for BGP.
Default Metric	This parameter specifies the metric for the routes that are being re-distributed. The possible values are between 0 and 2147483647. The default value is 0.
Import	With this parameter you can choose to import <i>Direct routes</i> , <i>Static routes</i> , <i>RIP routes</i> and/or <i>OSPF routes</i> to BGP.

RIP

Figure 5-136. RRD RIP Configuration Page



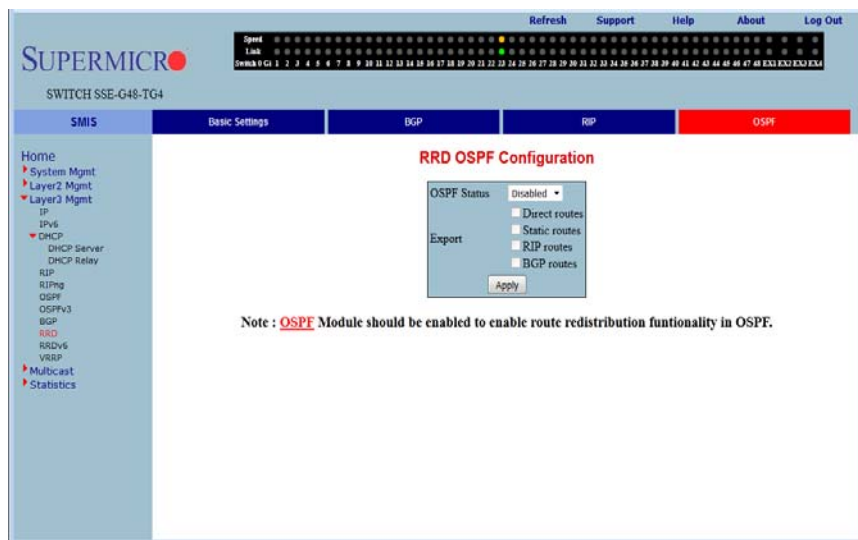
Clicking the RIP tab brings up the RRD RIP CONFIGURATION page (Figure 5-136), which allows you to re-distribute the routes that are learnt through other routing protocols to RIP. The parameters for this page are shown in Table 5-117.

Table 5-117. RRD RIP Configuration Page Parameters

Parameter	Description
RIP Status	This parameter enables or disables redistribution for RIP.
Default Metric	This parameter specifies the metric for the routes that are being re-distributed. The default value is 3.
Import	You can use this parameter to choose to import <i>Direct routes</i> , <i>Static routes</i> , <i>OSPF routes</i> and <i>BGP routes</i> to RIP.
Route Tag Type	This parameter describes whether a tag is <i>manually</i> configured or <i>automatically</i> generated.
Route Tag	This parameter indicates the route tag in case you configure a manual option for the tag type. The possible values are between 0 to 65535. The default value is 0.

OSPF

Figure 5-137. RRD OSPF Configuration Page



Clicking the OSPF tab brings up the RRD OSPF CONFIGURATION page (Figure 5-137), which allows you to e-distribute the routes that are learned through other routing protocols to OSPF. The parameters for this page are shown in Table 5-118.

Table 5-118. RRD OSPF Configuration Page Parameters

Parameter	Description
OSPF Status	This parameter enables or disables redistribution for OSPF.
Import	With this parameter you can choose to import <i>Direct routes</i> , <i>Static routes</i> , <i>RIP routes</i> and <i>BGP routes</i> to OSPF.

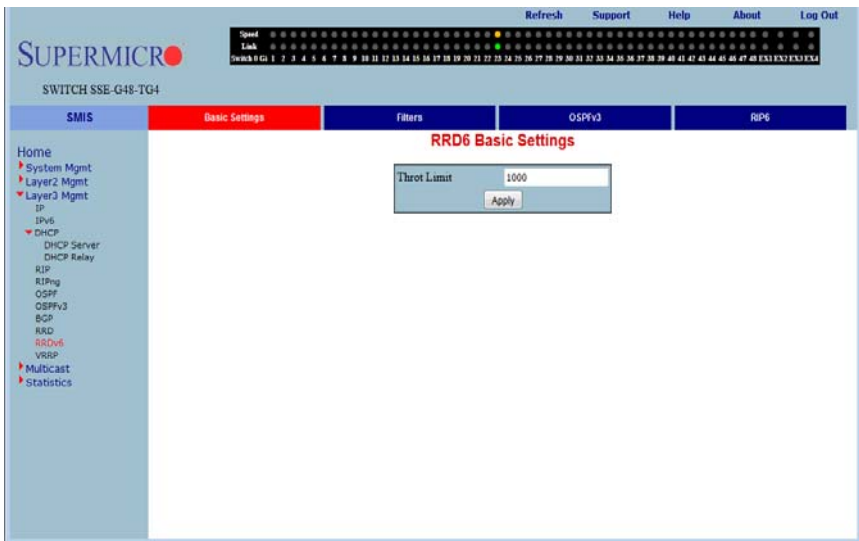
RRD6

The RRD6 link allows you to perform RRD6 related configuration through the following pages.

- [Basic Settings](#)
- [Filters](#)
- [OSPFv3](#)
- [RIP6](#)

Basic Settings

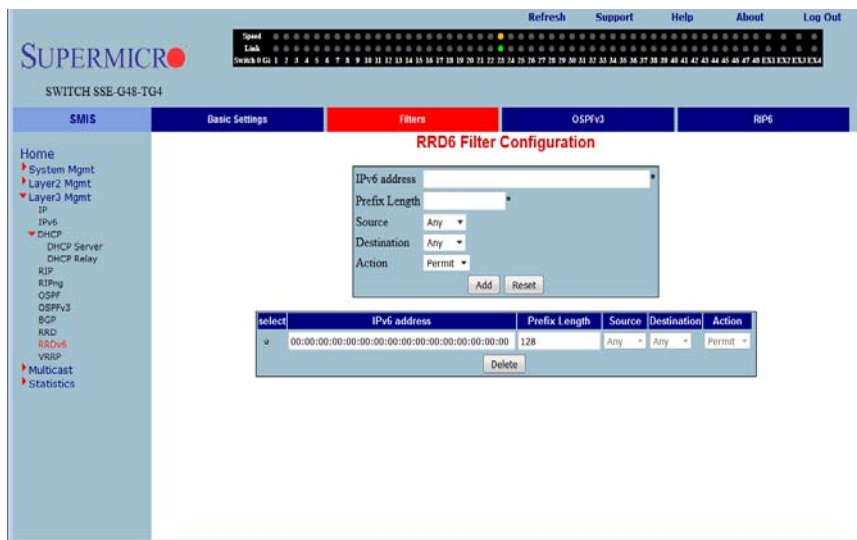
Figure 5-138. RRD6 Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the RRD6 BASIC SETTINGS page (Figure 5-138), which has the single parameter option of changing the THROT LIMIT for RRD6. The THROT LIMIT values are between 1 and 4294967295. The default value is 1000.

Filters

Figure 5-139. RRD6 Filter Configuration Page



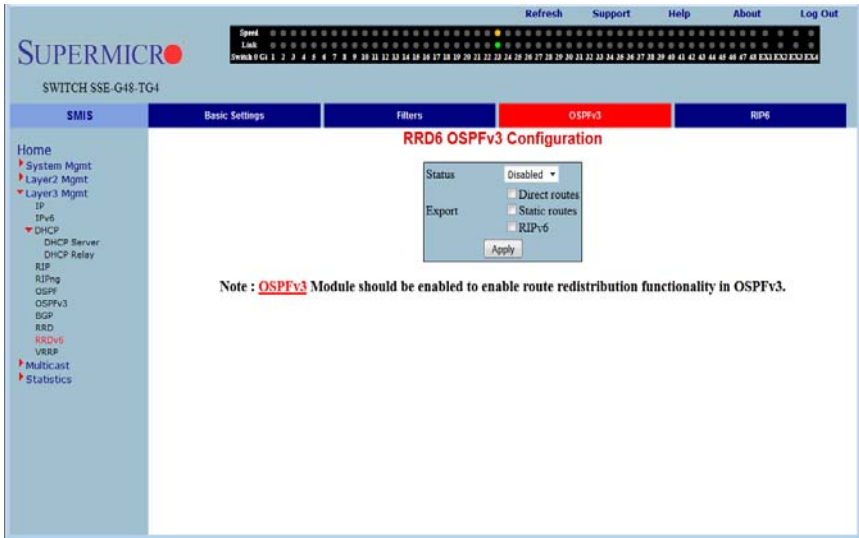
Clicking the FILTERS tab brings up the RRD6 FILTER CONFIGURATION page (Figure 5-139). The parameters for this page are shown in Table 5-119.

Table 5-119. RRD6 Filter Configuration Page Parameters

Parameter	Description
IPv6 address	This parameter specifies the IPv6 Address.
Prefix Length	This parameter indicates the length of the prefix (in bits) associated with this entry's IPv6 address.
Source	This parameter denotes the address of the Source.
Destination	This parameter specifies the address of the Destination.
Action	With this parameter you can either choose to <i>Permit</i> (not to filter) or <i>Deny</i> (Filter) for the above configuration set.

OSPFv3

Figure 5-140. RRD6 OSPFv3 Configuration Page



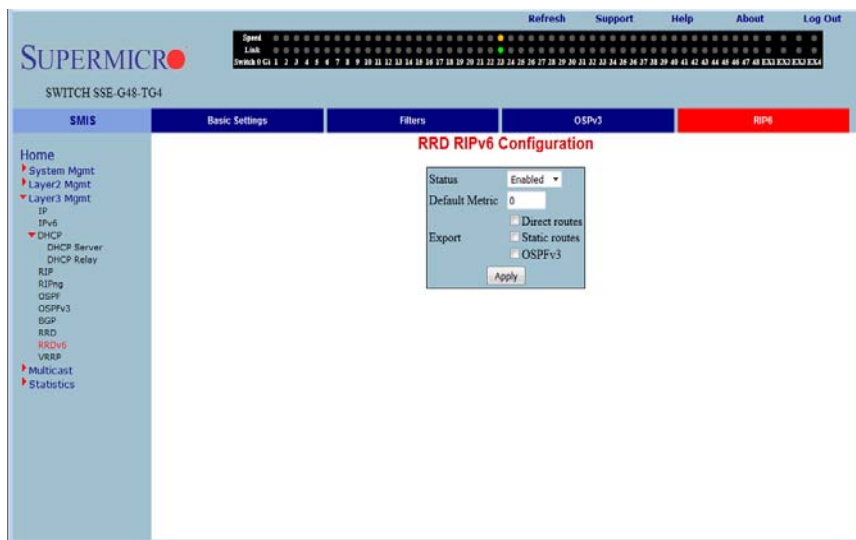
Clicking the OSPFv3 tab brings up the RRD6 OSPFv3 CONFIGURATION page (Figure 5-140). The parameters for this page are shown in Table 5-120.

Table 5-120. RRD6 OSPFv3 Configuration Page Parameters

Parameter	Description
Status	This parameter enables or disables redistribution for OSPFv3.
Export	With this parameter you can choose to export <i>Direct Routes</i> , <i>Static Routes</i> or <i>RIPv6 Routes</i> .

RIP6

Figure 5-141. RRD RIPv6 Configuration Page



Clicking the RP6 tab brings up the RRD RIPv6 CONFIGURATION page (Figure 5-141). The parameters for this page are shown in Table 5-121.

Table 5-121. RRD RIPv6 Configuration Page Parameters

Parameter	Description
Status	This parameter enables or disables redistribution for RIP6.
Default Metric	This parameter specifies the metric for the routes that are being re-distributed. The allowed value ranges from 0 and 16. The default value is 0.
Export	With this parameter you can choose to export <i>Direct Routes</i> , <i>Static Routes</i> or <i>OSPFv3 Routes</i> .

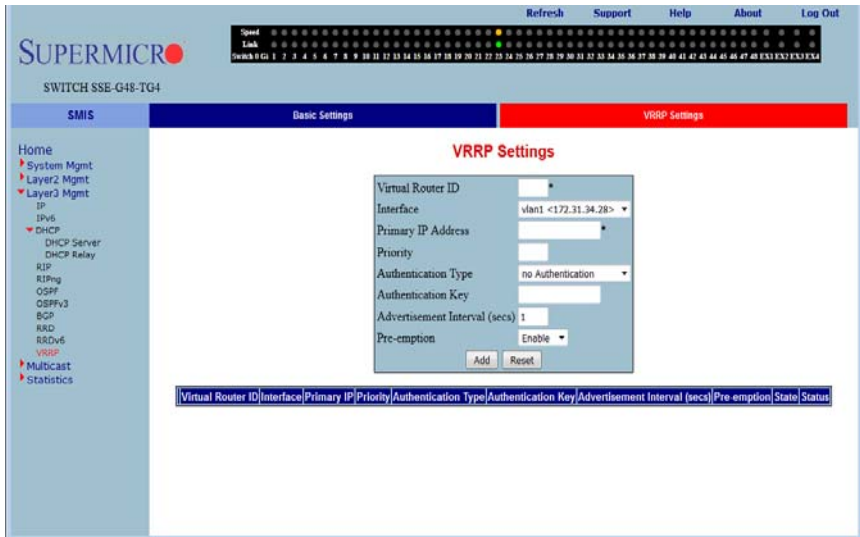
VRRP

The VRRP link allows you to configure VRRP through the following two pages:

- [Basic Settings](#)
- [VRRP Settings](#)

Basic Settings

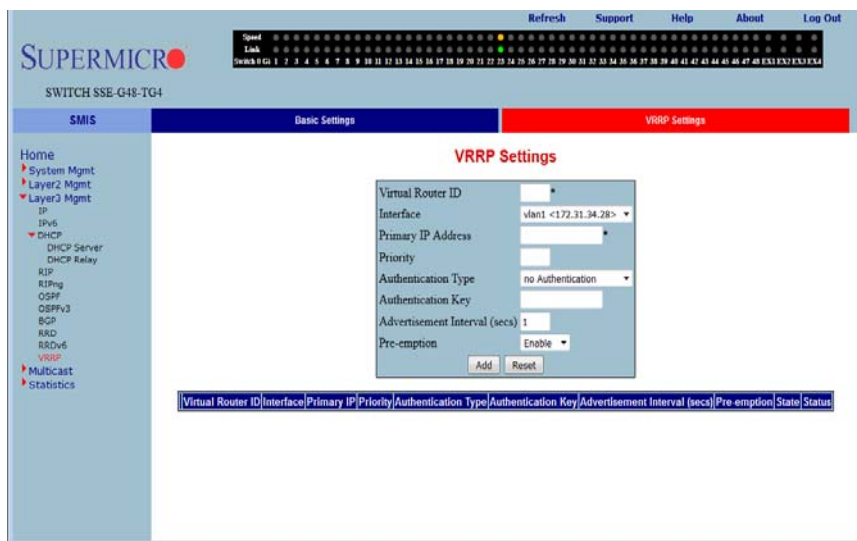
Figure 5-142. VRRP Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the VRRP BASIC SETTINGS page (Figure 5-142), whose single parameter allows you to specify the status of VRRP in the switch.

VRRP Settings

Figure 5-143. VRRP Settings Page



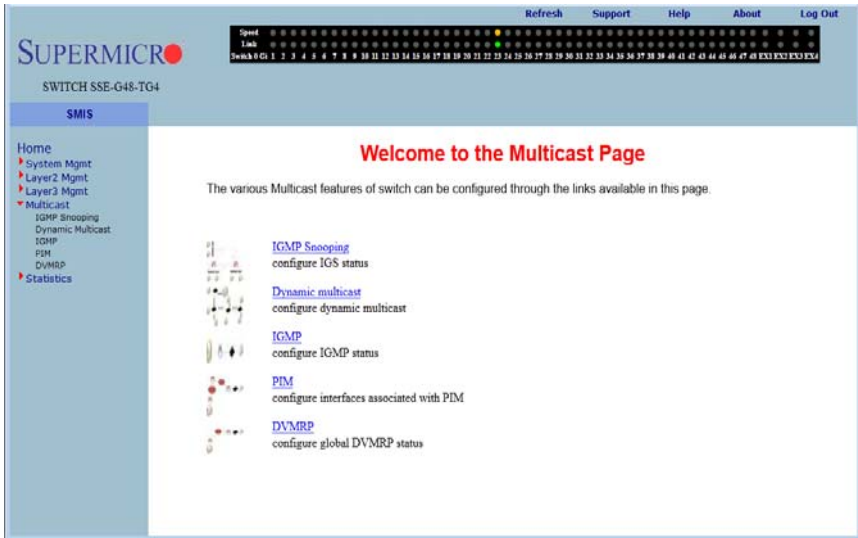
Clicking the VRRP SETTINGS link brings up the VRRP SETTINGS page (Figure 5-143). The parameters for this page are shown in Table 5-122.

Table 5-122. VRRP Settings Page Parameters

Parameter	Description
Virtual Router ID	This parameter indicates the Virtual ID associated with each Virtual Router. The allowed value ranges between 1 and 255.
Interface	This parameter represents the interface on which the Virtual Router must be configured.
Primary IP Address	This parameter specifies the PRIMARY IP ADDRESS for the Virtual Router.
Priority	This parameter indicates the PRIORITY for the Virtual Router. The configurable priority value ranges from 1 to 254.
Authentication Type	This parameter indicates the AUTHENTICATION TYPE for the Virtual Router.
Authentication Key	This parameter indicates the AUTHENTICATION KEY for the Virtual Router.
Advertisement Interval (Seconds)	This parameter specifies the time Interval in seconds for sending the advertisement packets.
Preempt Mode	This parameter enables or disables the PREEMPT MODE.
State	This parameter indicates the current state of the Virtual Router.
Status	This parameter specifies the Admin Status of the Virtual Router.

5-7 Multicast

Figure 5-144. Multicast Home Page



MULTICAST HOME page (Figure 5-144) has the following links to multicast features in the switch:

- [IGMP Snooping](#)
- [Dynamic Multicast](#)
- [IGMP](#)
- [PIM](#)
- [DVMRP](#)

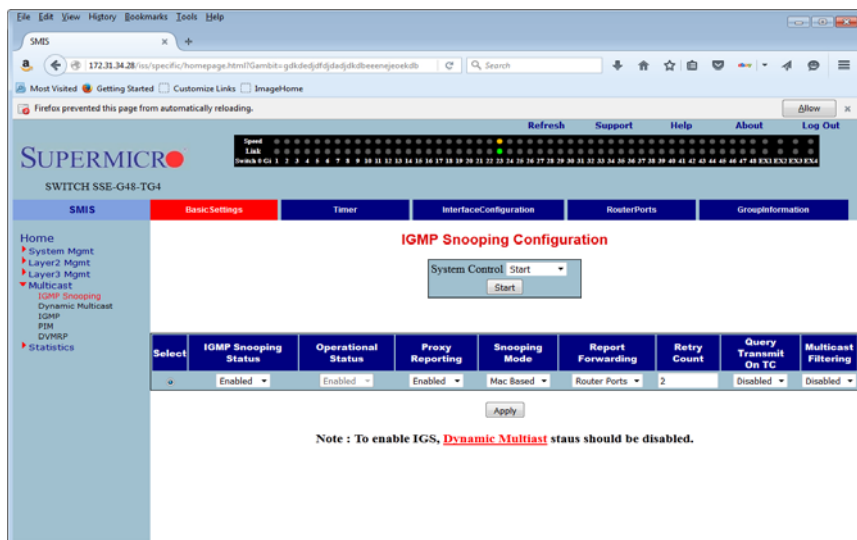
IGMP Snooping

The IGMP Snooping link allows you to configure IGMP snooping through the following pages:

- [Basic Settings](#)
- [Timer](#)
- [Interface Configuration](#)
- [Router Ports](#)
- [Group Information](#)

Basic Settings

Figure 5-145. IGMP Snooping Configuration Page



Clicking the BASIC SETTINGS tab brings up the IGMP SNOOPING CONFIGURATION page (Figure 5-145), which allows you to configure IGMP snooping parameters. The parameters for this page are shown in Table 5-123.

Table 5-123. IGMP Snooping Configuration Page Parameters

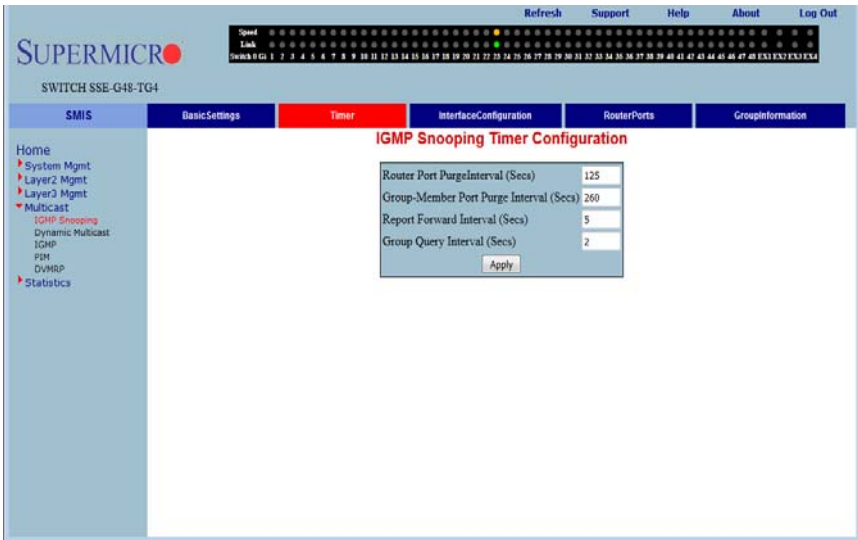
Parameter	Description
System Control	This parameter <i>Starts</i> or <i>Shutdowns</i> IGS in the switch.
IGMP Snooping Status	This parameter enables or disables IGMP snooping globally in the switch. To enable IGS, GMRP status must be <i>Disabled</i> .
Operational Status	This parameter enables or disables IGMP snooping operationally in the switch. To enable IGS, GMRP status must be <i>Disabled</i> .
Proxy Reporting	This parameter indicates whether the proxy reporting in the IGMP snooping switch is to be enabled or disabled.
Snooping Mode	This parameter specifies the IGMP snooping multicast forwarding mode, which can be configured using the Destination IP Address or the Destination MAC Address.
Report Forwarding	This parameter specifies whether the IGMP reports are forwarded on all ports or only on router ports.
Retry Count	This parameter specifies the maximum number of group specific queries sent on a port on the reception of an IGMPv2 leave message. The allowed ranges from 1 to 5. The default value is 2.

Table 5-123. IGMP Snooping Configuration Page Parameters (Continued)

Parameter	Description
Query Transmit On TC	This parameter allows you to enable or disable query transmit when topology changes.
Multicast Filtering	This parameter allows you to enable or disable the multicast filtering.

Timer

Figure 5-146. IGMP Snooping Timer Configuration Page



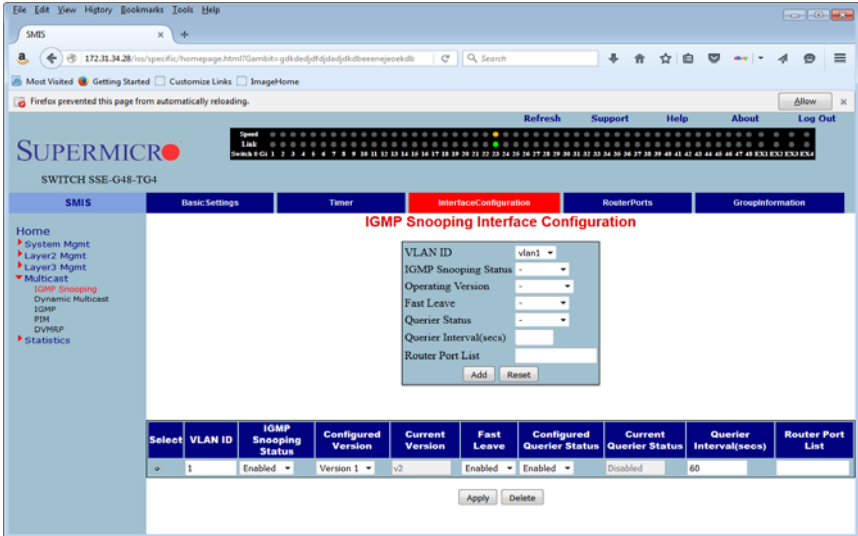
Clicking the **TIMER** tab brings up the **IGMP SNOOPING TIMER CONFIGURATION** page (Figure 5-146), which configures IGMP snooping timers. The parameters for this page are shown in Table 5-124.

Table 5-124. IGMP Snooping Timer Configuration Page Parameters

Parameter	Description
Router Port PurgeInterval (Secs)	This parameter specifies the interval for which the learnt router port will be purged. The default value is 125-seconds .
Group-Member Port Purge Interval (Secs)	This parameter specifies the interval after which a port gets deleted, if IGMP reports are not received on a port. The default value is 260-seconds .
Report Forward Interval (Secs)	This parameter specifies the interval within which the next report messages for the same multicast group will not be forwarded. The default value is 5-seconds .
Group Query Interval (Secs)	This parameter specifies the interval within which the switch sends a group specific query on a port when an IGMPv2 leave message is received. The default value is 2-seconds .

Interface Configuration

Figure 5-147. IGMP Snooping Interface Configuration Page



Clicking the INTERFACE CONFIGURATION tab brings up the IGMP SNOOPING INTERFACE CONFIGURATION page (Figure 5-147), which configures IGMP snooping interface specific parameters. The parameters for this page are shown in Table 5-125.

Table 5-125. IGMP Snooping Interface Configuration Page Parameters

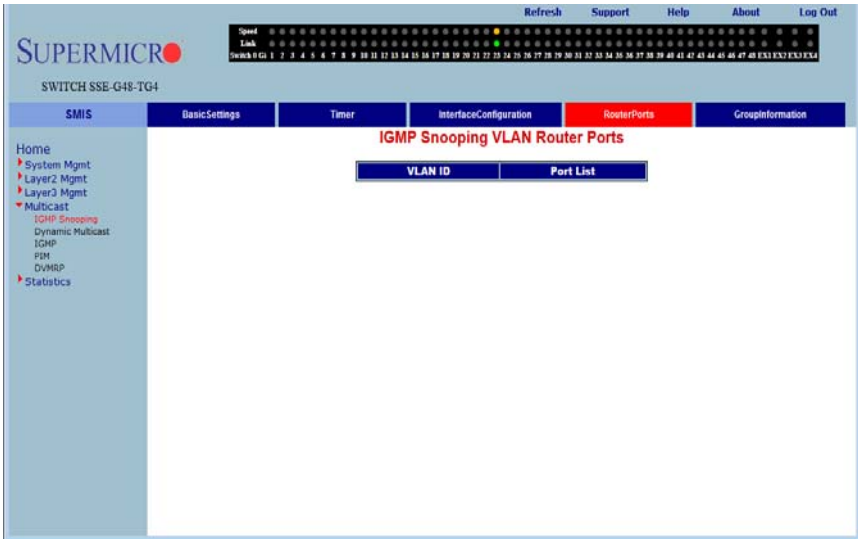
Parameter	Description
VLAN ID	This parameter specifies the VLAN ID for which the configuration is to be performed.
IGMP Snooping Status	This parameter specifies the status of IGMP snooping in the Switch, which can be enabled or disabled for a specific VLAN.
Operating Version	This parameter specifies the operating version of the IGMP snooping switch for a specific VLAN. Options are <i>version 1</i> or <i>version 2</i> or <i>version 3</i> .
Fast Leave	This parameter indicates whether the fast leave processing for a specific VLAN, is to be enabled or disabled.
Querier Status	This parameter specifies whether the IGMP snooping switch is enabled or disabled as a querier for a specific VLAN. The value ranges between 60 and 600.
Querier Interval (secs)	This parameter specifies the time period for which general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN.
Router Port List	This parameter specifies the router port list for a specific VLAN.
Current Version	This parameter specifies the working IGMP Version on the given VLAN.

Table 5-125. IGMP Snooping Interface Configuration Page Parameters (Continued)

Parameter	Description
Configured Version	This displays the configured IGMP operating Version on the given VLAN.
Current Querier Status	This parameter specifies the current status of the Querier.
Configured Querier Status	This displays the configured Querier status, which can be enabled or disabled.

Router Ports

Figure 5-148. IGMP Snooping VLAN Router Ports Page



Clicking the ROUTE PORTS tab brings up the IGMP SNOOPING VLAN ROUTER PORTS page (Figure 5-148). The parameters for this page are shown in Table 5-126.

Table 5-126. IGMP Snooping VLAN Router Ports Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN ID.
Port List	This parameter specifies the ports on which routers are connected for a specific VLAN.

Group Information

Figure 5-149. MAC Based Multicast Forwarding Table Page

The screenshot shows the SUPERMICR web interface for a SWITCH SSE-G48-TG4. The 'GROUP INFORMATION' tab is selected. The main content area displays the 'MAC Based Multicast Forwarding Table' with the following data:

VLAN ID	Group MAC Address	Port List
1	01:00:5e:7f:ff:fa	Gi0/23

Clicking the GROUP INFORMATION tab brings up the MAC BASED MULTICAST FORWARDING TABLE page (Figure 5-149), which displays either the IP Based or the MAC Based Multicast Forwarding Table depending upon the configuration of the forwarding mode. The parameters for this page are shown in Table 5-127.

Table 5-127. MAC Based Multicast Forwarding Table Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN ID pertaining to the MAC based multicast forwarding entry.
Group MAC Address	This parameter specifies the Group MAC Multicast address that is learnt.
Port List	This parameter specifies the learnt ports.

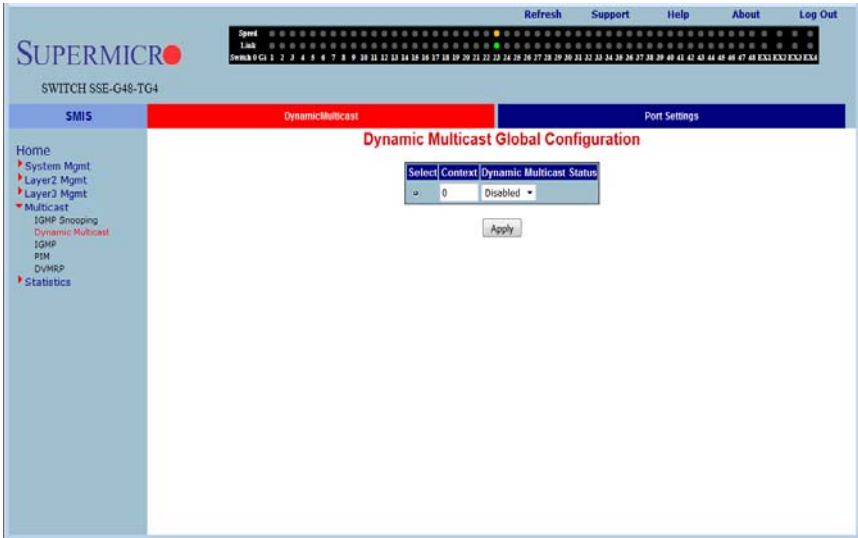
Dynamic Multicast

The Dynamic Multicast link allows you to configure Dynamic Multicast through the following pages:

- [Dynamic Multicast](#)
- [Port Settings](#)

Dynamic Multicast

Figure 5-150. Dynamic Multicast Global Configuration Page



Clicking the DYNAMIC MULTICAST tab brings up the DYNAMIC MULTICAST GLOBAL CONFIGURATION page (Figure 5-150), which allows you to enable or disable the dynamic multicast feature. The parameters for this page are shown in Table 5-128.

Table 5-128. Dynamic Multicast Global Configuration Page Parameters

Parameter	Description
Context	Displays the context identifier, which is a read only field.
Dynamic Multicast Status	Enable or disable dynamic multicast.

Port Settings

Figure 5-151. Dynamic Multicast Port Configuration Page

The screenshot shows the 'Dynamic Multicast Port Configuration' page for a SUPERMICR switch. The page title is 'Dynamic Multicast Port Configuration' and the selected port is 'Gi0/1-Ex0/3'. The table below shows the configuration for each port:

Select	Port	Dynamic Multicast Status	Restricted Group Registration
<input type="radio"/>	Gi0/1	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/2	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/3	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/4	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/5	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/6	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/7	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/8	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/9	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/10	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/11	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/12	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/13	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/14	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/15	Enabled ▾	Disabled ▾
<input type="radio"/>	Gi0/16	Enabled ▾	Disabled ▾
<input type="radio"/>	Ex0/1	Enabled ▾	Disabled ▾
<input type="radio"/>	Ex0/2	Enabled ▾	Disabled ▾
<input type="radio"/>	Ex0/3	Enabled ▾	Disabled ▾

An 'Apply' button is located below the table.

Clicking the PORT SETTINGS tab brings up the DYNAMIC MULTICAST PORT CONFIGURATION page (Figure 5-151), which configures dynamic multicast at the port level. The parameters for this page are shown in Table 5-129.

Table 5-129. Dynamic Multicast Port Configuration Page Parameters

Parameter	Description
Port	This parameter specifies the Port index.
Dynamic Multicast Status	This parameter enables or disables dynamic multicast on this port.
Restricted Group Registration	This parameter enables or disables RESTRICTED GROUP REGISTRATION on this port.

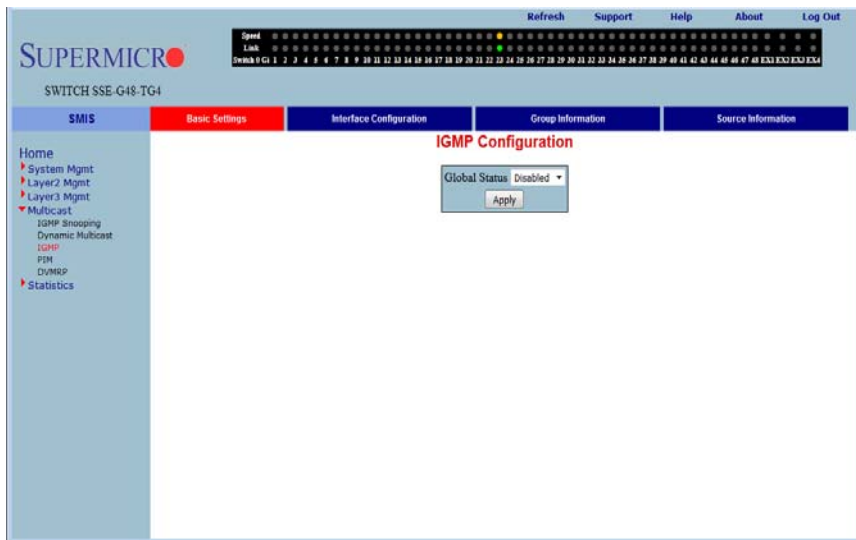
IGMP

The IGMP page allows you to configure the IGMP protocol. The IGMP protocol in the switch can be configured through the following pages:

- [Basic Settings](#)
- [Interface Configuration](#)
- [Group Information](#)
- [Source Information](#)

Basic Settings

Figure 5-152. IGMP Configuration Page



Clicking the BASIC SETTINGS tab brings up the IGMP CONFIGURATION page (Figure 5-152), whose single parameter allows you to enable or disable IGMP in the switch.

Interface Configuration

Figure 5-153. IGMP Interface Configuration Page

The screenshot shows the SUPERMICR web management utility interface. At the top, there is a navigation bar with 'Refresh', 'Support', 'Help', 'About', and 'Log Out' buttons. Below the navigation bar, the device name 'SWITCH SSE-G48-TG4' is displayed. The main content area is titled 'IGMP Interface Configuration' and is for interface 'vlan1'. The configuration parameters are as follows:

Parameter	Value
Interface	vlan1
IGMP Status	Disabled
Operating Version	Version 2
Fast Leave	Disabled
Query Interval (Secs)	125
Query Response Time (1/10 Secs)	100
Robustness Value	2
Last Memb Query Int (1/10 Secs)	10

Below the configuration form is a table with columns: Select, Interface, IGMP Status, Operating Version, Fast Leave, Query Interval, Query Resp Time, Robust Value, and Last Memb Query Int. The table contains one row for 'vlan1' with the corresponding values. There are 'Apply' and 'Delete' buttons below the table.

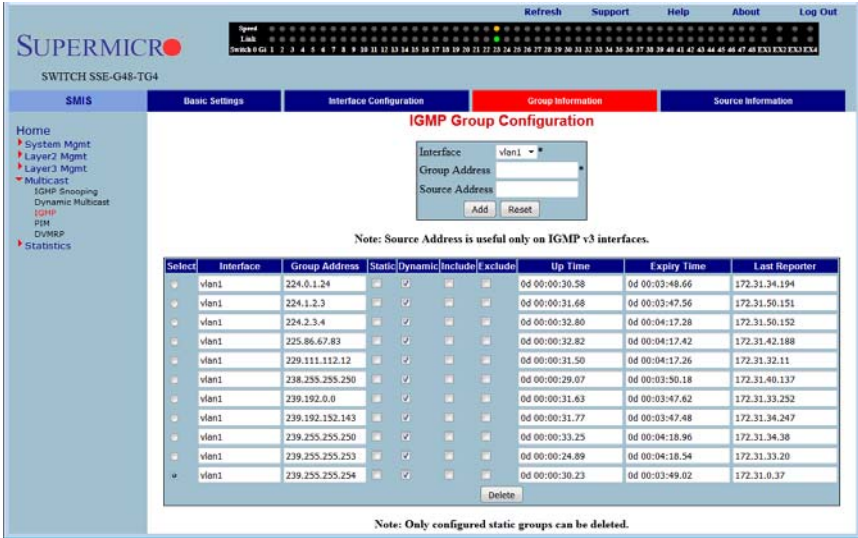
Clicking the INTERFACE CONFIGURATION tab brings up the IGMP INTERFACE CONFIGURATION page (Figure 5-153). The parameters for this page are shown in Table 5-130.

Table 5-130. IGMP Interface Configuration Page Parameters

Parameter	Description
Interface	This parameter specifies the interface index.
IGMP Status	This parameter specifies the IGMP Status.
Operating Version	With this parameter you can choose to run either in <i>IGMP Version 1</i> , <i>IGMP Version 2</i> or <i>IGMP Version 3</i> . This can be configured for every interface.
Fast Leave	This parameter indicates whether the fast leave processing for a specific interface, is to be enabled or disabled.
Query Interval	This parameter indicates the interval between two successive IGMP queries. The value ranges between 1 and 65535. The default value is 125.
Query Response Time	This parameter specifies the response time for IGMP queries. The value ranges between 1 and 255. The default value is 100.
Robustness Value	This parameter specifies the ROBUSTNESS VALUE on this interface. The value ranges between 1 and 255. The default value is 2.
Last Memb Query Int	This parameter specifies the IGMP last member query interval for the interface. The value ranges from 1 to 255. The default value is 10.

Group Information

Figure 5-154. IGMP Group Configuration Page



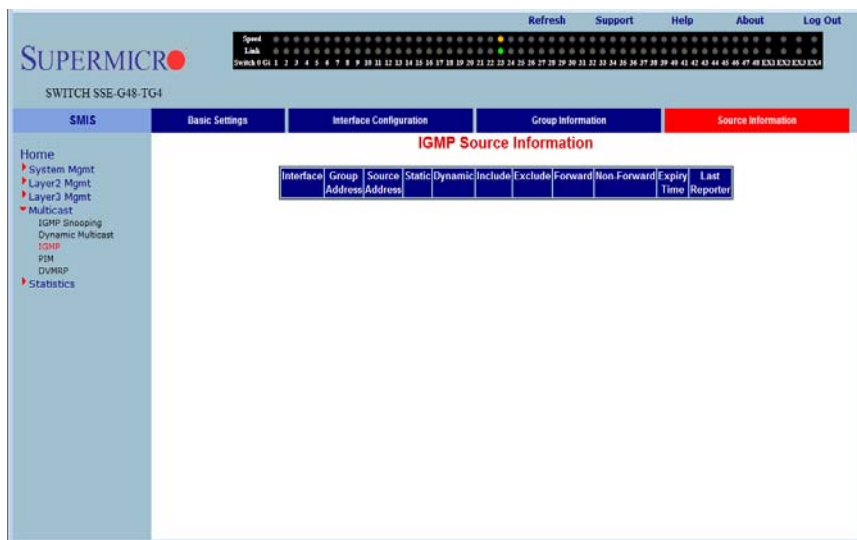
Clicking the GROUP INFORMATION tab brings up the IGMP GROUP CONFIGURATION page (Figure 5-154). The parameters for this page are shown in Table 5-131.

Table 5-131. IGMP Group Configuration Page Parameters

Parameter	Description
Interface	This parameter specifies the interface index.
Group Address	This parameter specifies the IP multicast group address.
Source Address	This parameter represents the IP Source address. NOTE: Source configuration is allowed only when the operating version is v3 on this interface.
Static and Dynamic	This parameter displays the type of member.
Include and Exclude	This parameter displays the filter mode.
Up Time	This parameter displays Up time in seconds.
Expiry Time	This parameter displays Expiry time in seconds.
Last Reporter	This parameter displays the IP address for IGMP group.

Source Information

Figure 5-155. IGMP Source Information Page



Clicking the SOURCE INFORMATION tab brings up the IGMP SOURCE INFORMATION page (Figure 5-155). The parameters for this page are shown in Table 5-132.

Table 5-132. IGMP Source Information Page Parameters

Parameter	Description
Group Address	This parameter specifies the IP multicast group address.
Interface	This parameter specifies the interface index.
Source Address	This parameter represents the IP Source address.
Static and Dynamic	This parameter displays the type of member.
Include and Exclude	This parameter displays the filter mode.
Forward and Non-forward	This parameter displays the member list.
Expiry Time	This parameter displays Expiry time in seconds.
Last Reporter	This parameter displays the IP address for IGMP group.

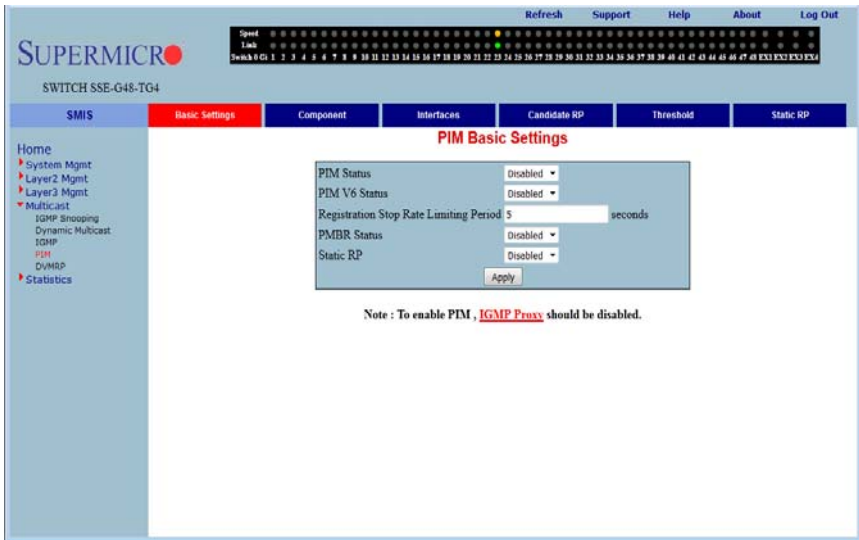
PIM

The PIM link allows you to perform PIM related configuration through the following pages:

- [Basic Settings](#)
- [Component](#)
- [Interfaces](#)
- [Candidate RPs](#)
- [Threshold](#)
- [Static RP](#)

Basic Settings

Figure 5-156. PIM Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the PIM BASIC SETTINGS page (Figure 5-156), which specifies the PIM status in the switch. The parameters for this page are shown in Table 5-133.

Table 5-133. PIM Basic Settings Page Parameters

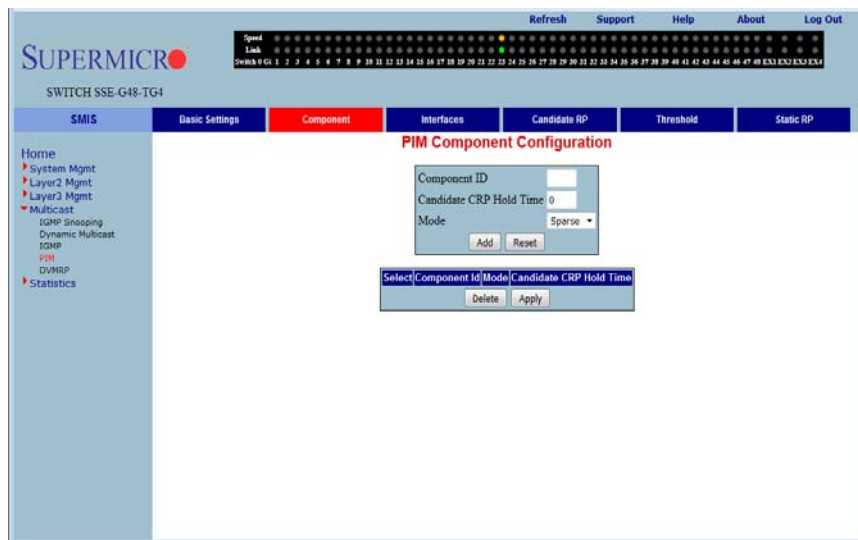
Parameter	Description
PIM Status	This parameter allows you to enable or disable the PIM status in the switch.
PIM V6 Status	This parameter allows you to enable or disable the PIM V6 status in the switch.

Table 5-133. PIM Basic Settings Page Parameters (Continued)

Parameter	Description
Registration Stop Rate Limiting Period	This parameter specifies the registration stop rate limiting period in seconds. It should be between 0 and 2147483647. The default value is 5 seconds.
PMBR Status	This parameter allows you to enable or disable the PMBR status in the switch.
Static RP	This parameter allows you to enable or disable the Static RP in the switch.

Component

Figure 5-157. PIM Component Configuration Page



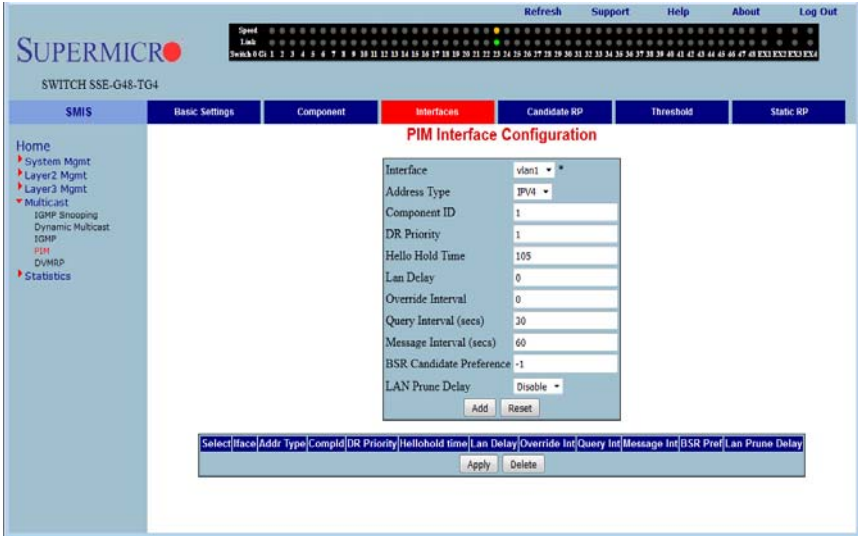
Clicking the COMPONENT tab brings up the PIM COMPONENT CONFIGURATION page (Figure 5-157). The parameters for this page are shown in Table 5-134.

Table 5-134. PIM Component Configuration Page Parameters

Parameter	Description
Component ID	This parameter specifies a number uniquely identifying the component. The allowed value ranges between 1 and 255. The default value is 1.
Candidate CRP Hold Time	This parameter specifies the hold time of the component when it is a candidate RP in the local domain.
Mode	This parameter specifies the mode of the component. It can be <i>Sparse</i> or <i>Dense</i> .

Interfaces

Figure 5-158. PIM Interface Configuration Page



Clicking the INTERFACES tab brings up the PIM INTERFACE CONFIGURATION page (Figure 5-158). The parameters for this page are shown in Table 5-135.

Table 5-135. PIM Interface Configuration Page Parameters

Parameter	Description
Interface	This parameter specifies the interface index.
Address Type	Specifies the address type, which can be IPv4 or IPv6.
Component ID	This parameter specifies a number uniquely identifying the component. The allowed range is 1 to 255. The default value is 1.
DR Priority	This parameter specifies the designated Router (DR) priority value for the PIM component. The DR priority value can be any number from 1 to 65535. The default value is 1.
Hello Hold Time (Seconds)	This parameter specifies the time interval between two successive Hello messages being sent by PIM on this interface.
LAN Delay	This parameter configures LAN delay time for PIM messages. The allowed range is 0 to 65535. The default value is 0 seconds.
Override Interval	This parameter configures override interval for PIM messages. The allowed range is 0 to 65535. The default value is 0 seconds.
Query Interval	This parameter configures the time interval between two successive queries being sent by PIM on this interface. The allowed range is 1 to 255. The default value is 30 seconds.

Table 5-135. PIM Interface Configuration Page Parameters (Continued)

Parameter	Description
Message Interval	This parameter configures the time interval between two successive messages being sent by PIM on this interface. The allowed ranges are 1 to 255. The default value is 60 seconds.
CBSR Preference	This parameter indicates the preference value for the local interface as a candidate bootstrap router. The allowed value ranges between -1 and 255. The default value is -1.
LAN Prune Delay	This parameter specifies the prune delay, which can be enabled or disabled.
Join Prune Interval (Seconds)	This parameter specifies the time interval between two successive Join/Prune messages being sent by PIM on this interface.
CBSR Preference	This parameter indicates the preference value for the local interface as a candidate bootstrap router.
Row Status	This parameter indicates the operational status of the entry.

Candidate RPs

Figure 5-159. Candidate RP Configuration Page

The screenshot displays the 'Candidate RP Configuration' page. At the top, there is a navigation bar with 'SMIS' and tabs for 'Basic Settings', 'Component', 'Interfaces', 'Candidate RP' (highlighted), 'Threshold', and 'Static RP'. The left sidebar contains a tree view with 'Home' expanded to show 'System Mgmt', 'Layer2 Mgmt', 'Layer3 Mgmt', 'Multicast', 'IGMP Snooping', 'Dynamic Multicast', 'IGMP', 'PIM', 'DVMRP', and 'Statistics'. The main content area is titled 'Candidate RP Configuration' and features a form with the following fields: 'Component Id' (text input), 'Address Type' (dropdown menu set to 'IPv4'), 'Group Address' (text input), 'Group Mask' (text input), and 'RP Address' (text input). Below the form are 'Add' and 'Reset' buttons. A status bar at the bottom of the form indicates the selection criteria: 'Select Component Id|Address|Group Address|Group Mask|RP Address'.

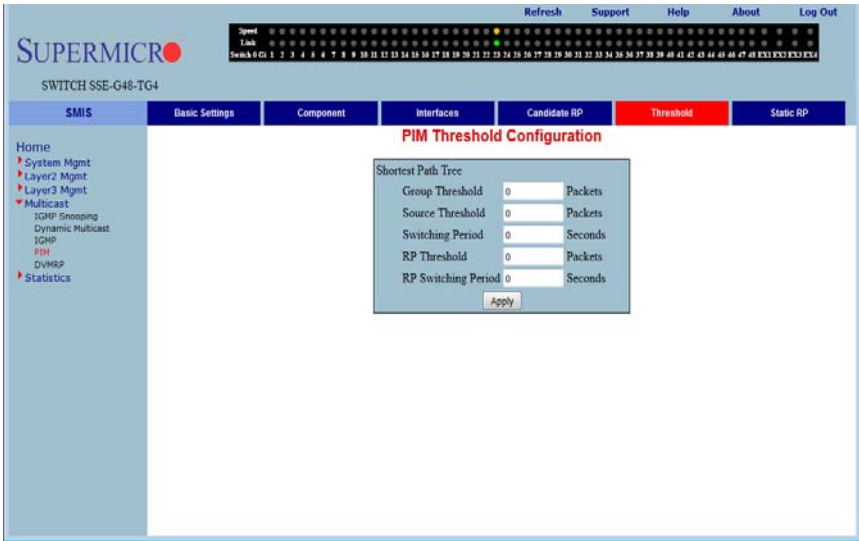
Clicking the CANDIDATE RPs tab brings up the CANDIDATE RP CONFIGURATION page (Figure 5-159). The parameters for this page are shown in Table 5-136.

Table 5-136. Candidate RP Configuration Page Parameters

Parameter	Description
Component ID	This parameter specifies a number uniquely identifying the component.
Group Address	This parameter represents the multicast group, for which the switch advertises itself as the candidate RP. This can be IPV4 or IPV6.
Group Mask	This parameter specifies the subnet mask, which when combined with the group address gives the group prefix.
RP Address	This parameter represents the IP address of the Candidate-RP.

Threshold

Figure 5-160. PIM Threshold Configuration Page



Clicking the THRESHOLD tab brings up the PIM THRESHOLD CONFIGURATION page (Figure 5-160). The parameters for this page are shown in Table 5-137.

Table 5-137. PIM Threshold Configuration Page Parameters

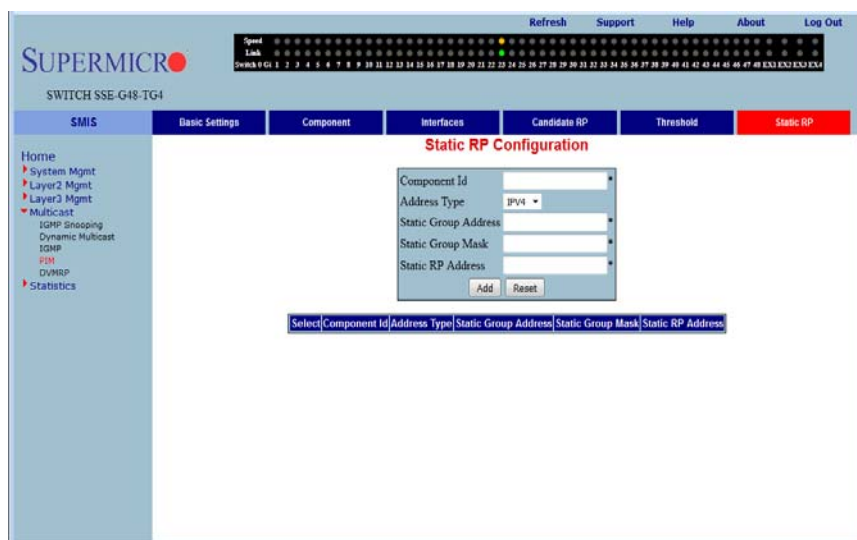
Parameter	Description
Group Threshold	This parameter is a bits-per-second (BPS) value that when it exceeds a certain value, initiates source specific counters for a particular group.
Source Threshold	This parameter is a bits-per-second (BPS) value that when exceeds a certain value, initiates switching to shortest path tree.
Switching Period	This parameter specifies the time interval that the data rate is monitored for, initiating the counters or for switching to SPT.

Table 5-137. PIM Threshold Configuration Page Parameters (Continued)

Parameter	Description
RP Threshold	When the number of registered packets received exceeds this threshold value, RP initiates switching to SPT.
RP Switching Period	This parameter specifies the time interval for which the registered packets are monitored to initiate switching to SPT.

Static RP

Figure 5-161. Static RP Configuration Page



Clicking the STATIC RP tab brings up the STATIC RP CONFIGURATION page (Figure 5-161), which configure static PIM RPs (Rendezvous Points). The parameters for this page are shown in Table 5-138.

Table 5-138. Static RP Configuration Page Parameters

Parameter	Description
Component ID	This parameter specifies a number uniquely identifying the component.
Address Type	This parameter chooses the IPv4 or IPv6 address type.
Static Group Address	This parameter represents the multicast group, for which the switch advertises itself as the candidate RP.
Static Group Mask	This parameter specifies the subnet mask, which when combined with the group address gives the group prefix.
Static RP Address	This parameter represents the IP address of the candidate RP.

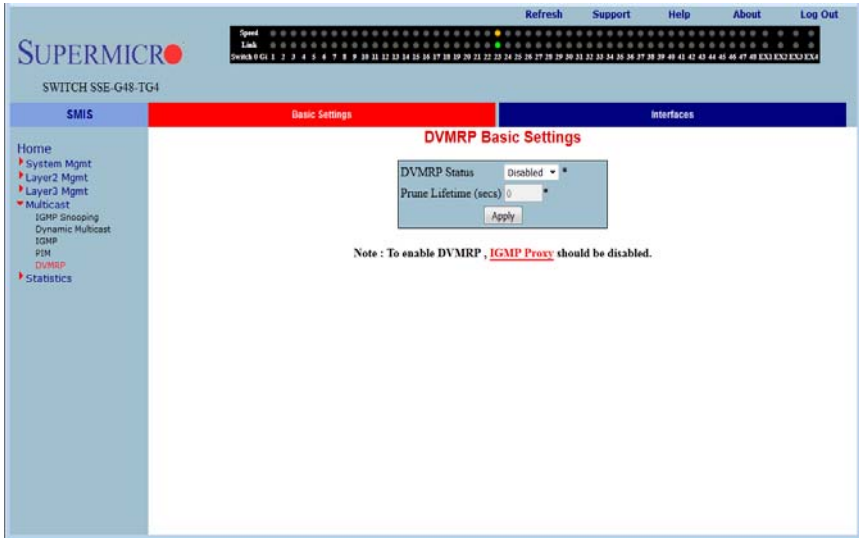
DVMRP

The DVMRP page allows you to configure the DVMRP protocol using the following pages:

- [Basic Settings](#)
- [Interfaces](#)

Basic Settings

Figure 5-162. DVMRP Basic Settings Page



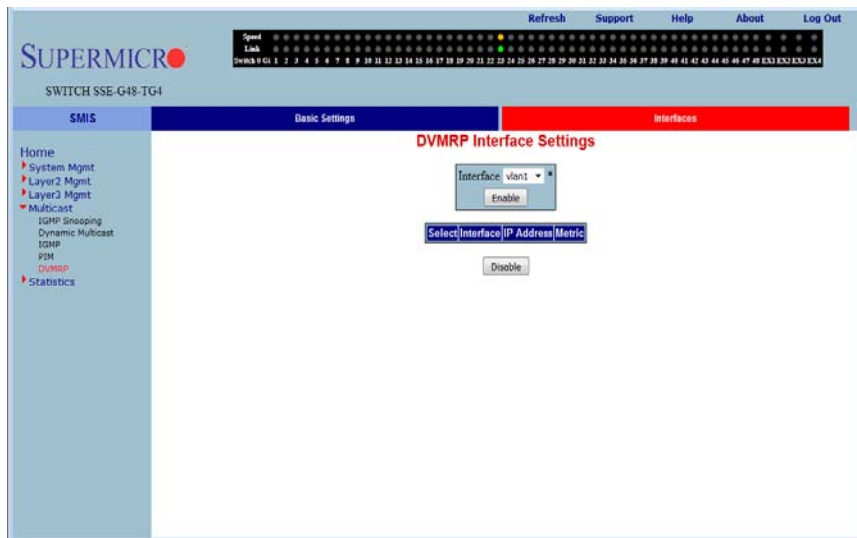
Clicking the BASIC SETTINGS tab brings up the DVMRP BASIC SETTINGS page (Figure 5-162). The parameters for this page are shown in Table 5-139.

Table 5-139. DVMRP Basic Settings Page Parameters

Parameter	Description
DVMRP Status	DVMRP can be enabled or disabled in the switch using this field.
Prune Lifetime (Seconds)	This parameter represents the Prune Life Time Configuration value. The allowed value ranges between 1 and 7200. The default value is 50.

Interfaces

Figure 5-163. DVMRP Interface Settings Page



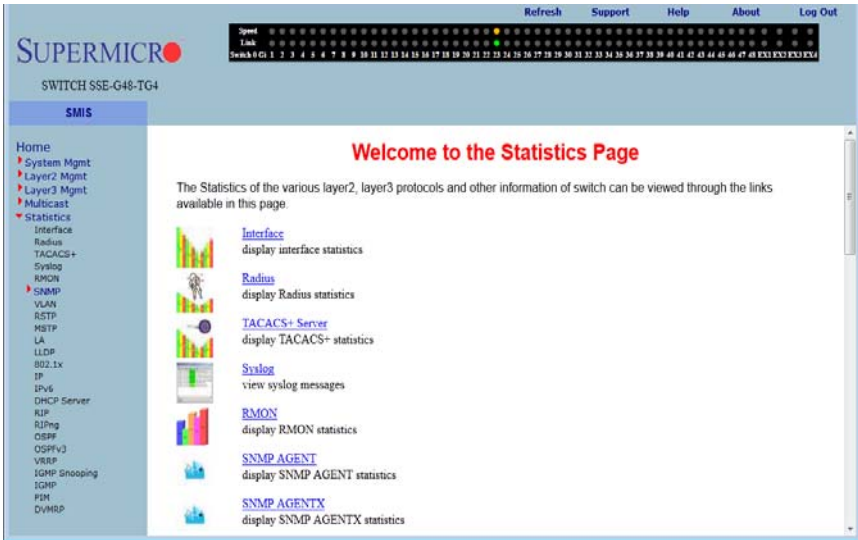
Clicking the INTERFACES tab brings up the DVMRP INTERFACE SETTINGS page (Figure 5-163), which displays the various parameters. The parameters for this page are shown in Table 5-140.

Table 5-140. DVMRP Interface Settings Page Parameters

Parameter	Description
Interface	This parameter specifies the Port interface.
IP Address	This parameter specifies the IP Address of the interface, which is a read-only field.
Metric	This parameter specifies the distance metric for this interface, which is used to calculate distance vectors.

5-8 Statistics

Figure 5-164. Statistics Home Page



The STATISTICS HOME page (Figure 5-164) contains links to all statistical information for all switch features and includes the following statistics pages:

- [Interface](#)
- [Radius](#)
- [TACACS+ Statistics](#)
- [RMON Ethernet Statistics](#)
- [SNMP Statistics](#)
- [VLAN](#)
- [RSTP Statistics](#)
- [MSTP Statistics](#)
- [Link Aggregation \(LA\)](#)
- [802.1X](#)
- [IP](#)
- [IPv6](#)
- [RIP](#)
- [RIP6](#)
- [OSPF](#)
- [OSPFv3](#)
- [VRRP](#)
- [IGMP Snooping](#)

- IGMP
- PIM
- DVMRP

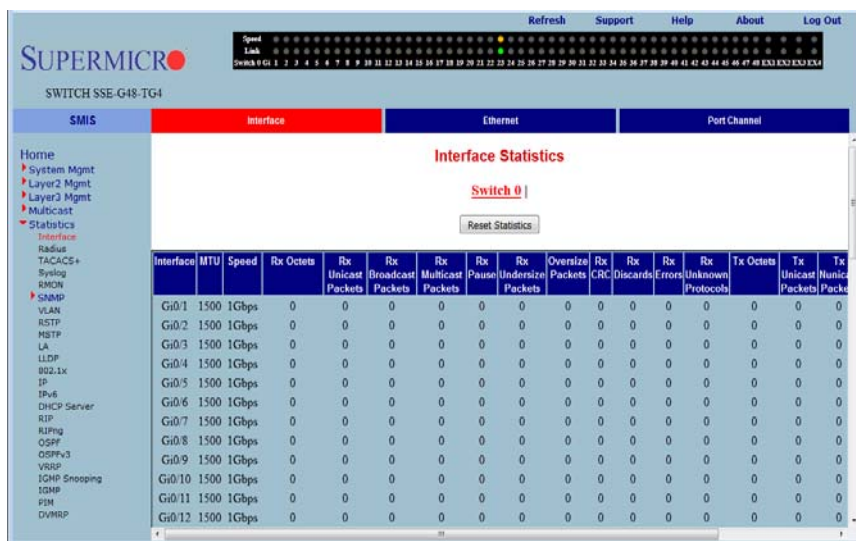
Interface

The Interface link allows you to configure the following pages:

- [Interface](#)
- [Ethernet](#)
- [Port Channel](#)

Interface

Figure 5-165. Interface Statistics Page



Clicking the INTERFACE tab brings up the INTERFACE STATISTICS page (Figure 5-165). The parameters for this page are shown in Table 5-141.

Table 5-141. Interface Statistics Page Parameters

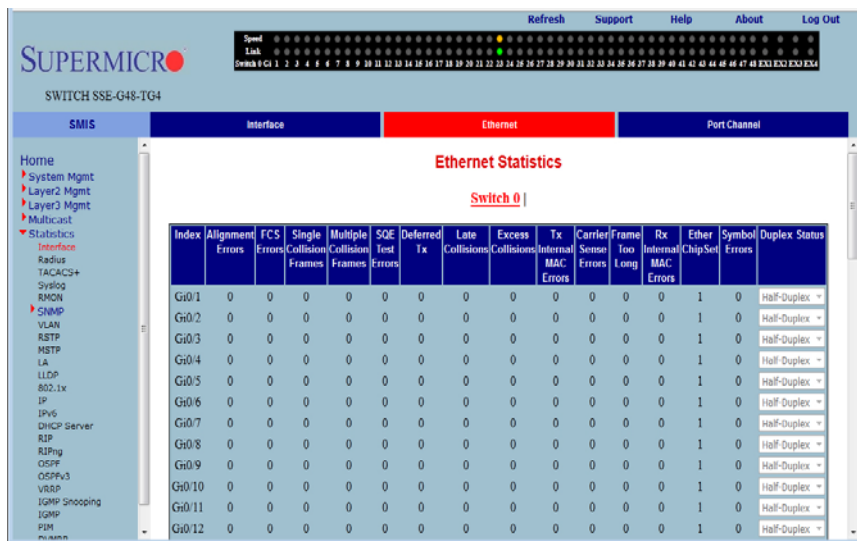
Parameter	Description
Interface	This parameter specifies the Port Interface.
MTU	This parameter specifies the Max Transfer Unit bytes.
Speed (Bits Per Second)	This parameter specifies the port speed in bits per second.

Table 5-141. Interface Statistics Page Parameters (Continued)

Parameter	Description
Received Octets	This parameter specifies the number of bytes received.
Received Unicast Packets	This parameter specifies the number of unicast packets received.
Received Broadcast Packets	This parameter specifies the number of broadcast packets received.
Received Multicast Packets	This parameter specifies the number of multicast packets received.
Received Pause	This parameter specifies the number of pause packets received.
Received Undersize Packets	This parameter specifies the number of packets received with size lesser than minimum accepted Ethernet frame size.
Oversize Packets	This parameter specifies the number of packets received with size greater than maximum accepted frame size of this interface.
Received CRC	This parameter specifies the number of packets received with CRC errors.
Received Discards	This parameter specifies the number of packets discarded due to errors.
Received Errors	This parameter specifies the number of packets received with errors.
Received Unknown Protocols	This parameter specifies the number of packets received with unknown protocol.
Received Nunicast Packets	This parameter specifies the number of non-unicast packets received.
Received Discards	This parameter specifies the number of packets discarded due to errors.
Received Errors	This parameter specifies the number of packets received with errors.
Received Unknown Protocols	This parameter specifies the number of packets received with an unknown protocol.
Transmitted Octets	This parameter specifies the number of bytes transmitted.
Transmitted Unicast Packets	This parameter specifies the number of unicast packets transmitted.
Transmitted Nunicast Packets	This parameter specifies the number of non-unicast packets transmitted.
Transmitted Pause	This parameter specifies the number of pause packets transmitted.
Transmitted Discards	This parameter specifies the number of packets discarded due to transmit errors.
Transmitted Errors	This parameter specifies the number of transmit errors.
Reset Statistics	This button used to reset the received and transmitted packet counter values to 0 .

Ethernet

Figure 5-166. Ethernet Statistics Page



Clicking the ETHERNET tab brings up the ETHERNET STATISTICS page (Figure 5-166). The parameters for this page are shown in Table 5-142.

Table 5-142. Ethernet Statistics Page Parameters

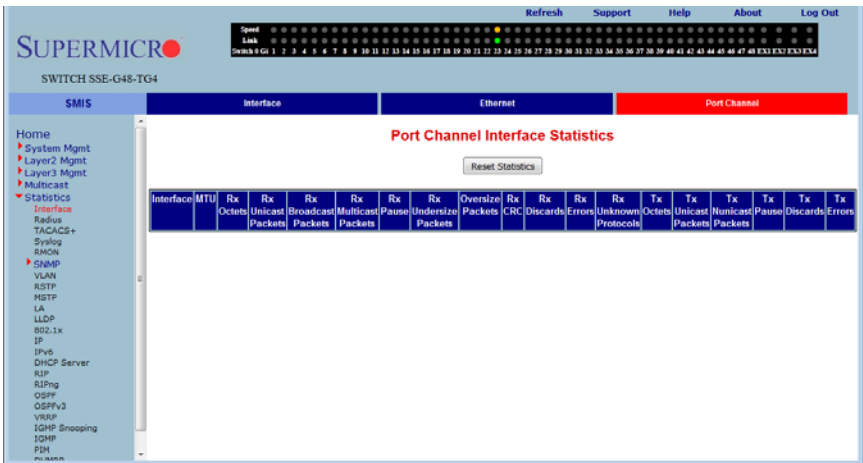
Parameter	Description
Index	This parameter specifies the port index.
Alignment Errors	This parameter specifies the number of alignment errors. Alignment errors generally indicate improper byte-alignment for Ethernet packets.
FCS Errors	This parameter specifies the number of packets received with checksum errors.
Single Collision Frames	This parameter specifies the number of frames received with a collision.
Multiple Collision Frames	This parameter specifies the number of frames received with multiple collisions.
SQE Test Errors	This parameter specifies the number of Signal Quality Errors that have occurred.
Deferred Transmissions	This parameter specifies the number of frames deferred for transmissions due to network sense.
Late Collisions	This parameter specifies the number of frames faced late collisions. A collision is considered late if the jam occurs after 512 bit-times, or 64 bytes.
Excess Collisions	This parameter specifies the number of excess collisions detected. Excessive Collisions describe the situation where a station has tried 16 times to transmit without success and discards the frame. This means that there is excessive traffic on the network and this must be reduced.

Table 5-142. Ethernet Statistics Page Parameters (Continued)

Parameter	Description
Transmitted Internal MAC Errors	This parameter specifies the number of MAC transmit errors.
Carrier Sense Errors	This parameter specifies the number of carrier sense errors.
Frame Too Long	This parameter specifies the number of too long frames received for transmission.
Received Internal MAC Errors	This parameter specifies the number of MAC received errors.
Ether ChipSet	This parameter specifies the number of ethernet chip set value.
Symbol Errors	This parameter specifies the number of symbol errors.
Duplex Status	This parameter specifies the current status of duplex.

Port Channel

Figure 5-167. Port Channel Interface Statistics Page



Clicking the PORT CHANNEL link brings up the PORT CHANNEL INTERFACE STATISTICS page (Figure 5-167), which displays the port statistics. The parameters for this page are shown in Table 5-144.

Table 5-143. Port Channel Interface Statistics Page Parameters

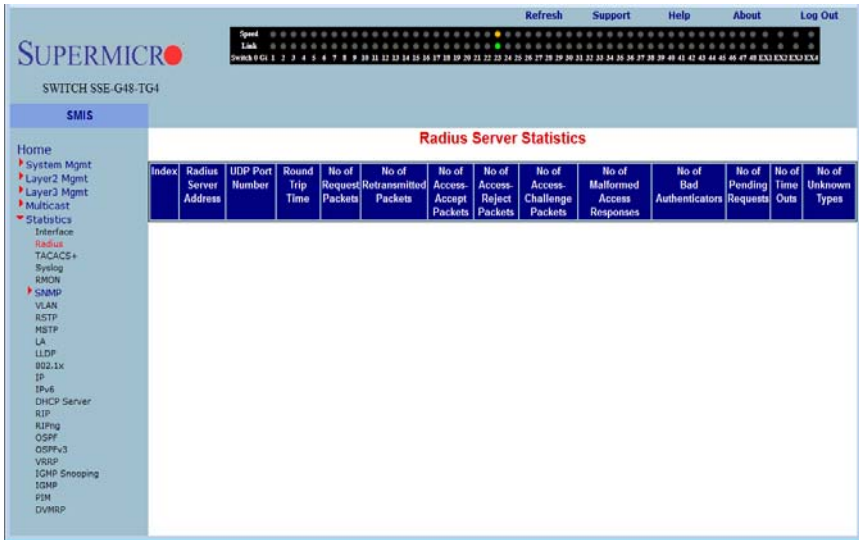
Parameter	Description
Interface	This parameter specifies the Port interface.
MTU	This parameter specifies the Max Transfer Unit bytes.
Received Octets	This parameter specifies the number of bytes received.

Table 5-143. Port Channel Interface Statistics Page Parameters (Continued)

Parameter	Description
Received Unicast Packets	This parameter specifies the number of unicast packets received.
Received Broadcast Packets	This parameter specifies the number of broadcast packets received.
Received Multicast Packets	This parameter specifies the number of multicast packets received.
Received Pause	This parameter specifies the number of pause packets received.
Received Undersize Packets	This parameter specifies the number of packets received with size lesser than minimum accepted Ethernet frame size.
Oversize Packets	This parameter specifies the number of packets received with size greater than maximum accepted Ethernet frame size.
Received CRC	This parameter specifies the number of packets received with CRC errors.
Received Discards	This parameter specifies the number of packets discarded due to errors.
Received Errors	This parameter specifies the number of packets received with errors.
Received Unknown Protocols	This parameter specifies the number of packets received with unknown protocol.
Transmitted Octets	This parameter specifies the number of bytes transmitted.
Transmitted Unicast Packets	This parameter specifies the number of unicast packets transmitted.
Transmitted Nunicast Packets	This parameter specifies the number of non-unicast packets transmitted.
Transmitted Pause	This parameter specifies the number of pause packets transmitted.
Transmitted Discards	This parameter specifies the number of packets discarded due to transmit errors.
Transmitted Errors	This parameter specifies the number of transmit errors.
Reset Statistics	This button is used to reset the received and transmitted packet counter values to 0 .

Radius

Figure 5-168. Radius Server Statistics Page



Clicking the RADIUS link brings up the RADIUS SERVER STATISTICS page (Figure 5-168). The parameters for this page are shown in Table 5-144.

Table 5-144. Radius Server Statistics Page Parameters

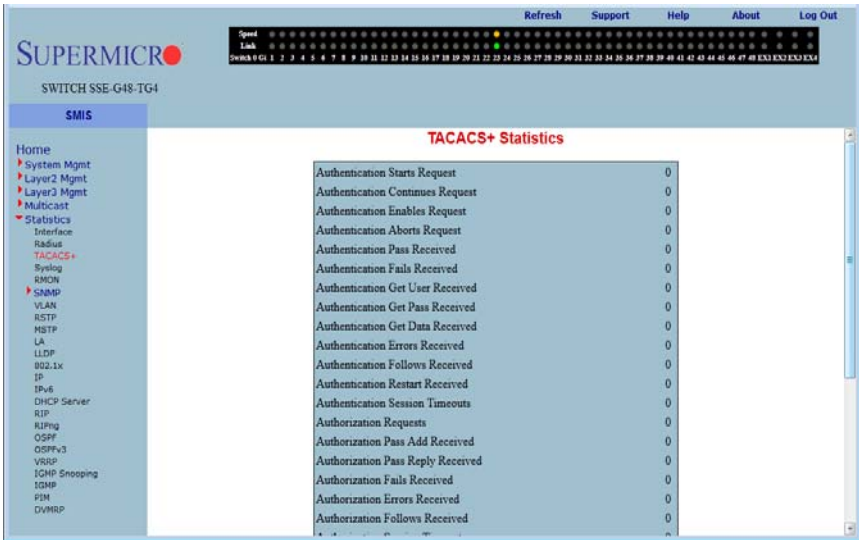
Parameter	Description
Index	This parameter specifies the port index.
Radius Server Address	This parameter specifies the RADIUS SERVER ADDRESS.
UDP Port Number	This parameter specifies the UDP PORT NUMBER.
Round Trip Time	This parameter displays the ROUND TRIP TIME in seconds.
No of Request Packets	This parameter specifies the number of request packets transmitted.
No of Retransmitted Packets	This parameter specifies the number of packets retransmitted.
No of Access-Accept Packets	This parameter specifies the number of accept packets.
No of Access-Reject Packets	This parameter specifies the number of reject packets.
No of Access-Challenge Packets	This parameter specifies the number of challenge packets.

Table 5-144. Radius Server Statistics Page Parameters (Continued)

Parameter	Description
No of Malformed Access Responses	This parameter specifies the number of invalid access responses received.
No of Bad Authenticators	This parameter specifies the number of failed authentications.
No of Pending Requests	This parameter specifies the number of currently pending requests.
No of Time Outs	This parameter specifies the number of time outs that have happened.
No of Unknown Types	This parameter specifies the number of unknown types that have been received.

TACACS+ Statistics

Figure 5-169. TACACS+ Statistics Page



Clicking the TACACS+ link brings up the TACACS+ STATISTICS page (Figure 5-169). The parameters for this page are shown in Table 5-145.

Table 5-145. TACACS+ Statistics Page Parameters

Parameter	Description
Authentication Starts Request	This parameter specifies the number of authentication starts requested.
Authentication Continues Request	This parameter specifies the number of authentication continues requested.
Authentication Enables Request	This parameter specifies the number of authentication enables requested.
Authentication Aborts Request	This parameter specifies the number of authentication aborts requested.
Authentication Pass Received	This parameter specifies the number of authentication passes received.
Authentication Fails Received	This parameter specifies the number of authentication fails received.
Authentication Get User Received	This parameter specifies the number of authentication get users received.
Authentication Get Pass Received	This parameter specifies the number of authentication get passes received.

Table 5-145. TACACS+ Statistics Page Parameters (Continued)

Parameter	Description
Authentication Get Data Received	This parameter specifies the number of authentication get datas received.
Authentication Errors Received	This parameter specifies the number of authentication errors received.
Authentication Follows Received	This parameter specifies the number of authentication follows received.
Authentication Restart Received	This parameter specifies the number of authentication restarts received.
Authentication Session Timeouts	This parameter specifies the number of authentication session timeouts received.
Authorization Requests	This parameter specifies the number of authentication requests received.
Authorization Pass Add Received	This parameter specifies the number of authentication pass adds received.
Authorization Pass Reply Received	This parameter specifies the number of authentication pass replies received.
Authorization Fails Received	This parameter specifies the number of authentication fails received.
Authorization Errors Received	This parameter specifies the number of authentication errors received.
Authorization Follows Received	This parameter specifies the number of authentication follows received.
Authorization Session Timeouts	This parameter specifies the number of authentication session timeouts.
Accounting Start Requests	This parameter specifies the number of accounting start requests.
Accounting WD Requests	This parameter specifies the number of accounting WD requests.
Accounting Stop Requests	This parameter specifies the number of accounting stop requests.
Accounting Success Received	This parameter specifies the number of accounting successes received.
Accounting Errors Received	This parameter specifies the number of accounting errors received.
Accounting Follows Received	This parameter specifies the number of accounting follows received.
Accounting Session Timeouts	This parameter specifies the number of accounting sessions received.
Malformed Packets Received	This parameter specifies the number of malformed packets received.
Socket Failures	This parameter specifies the number of socket failures.
Connection Failures	This parameter specifies the number of connection failures.

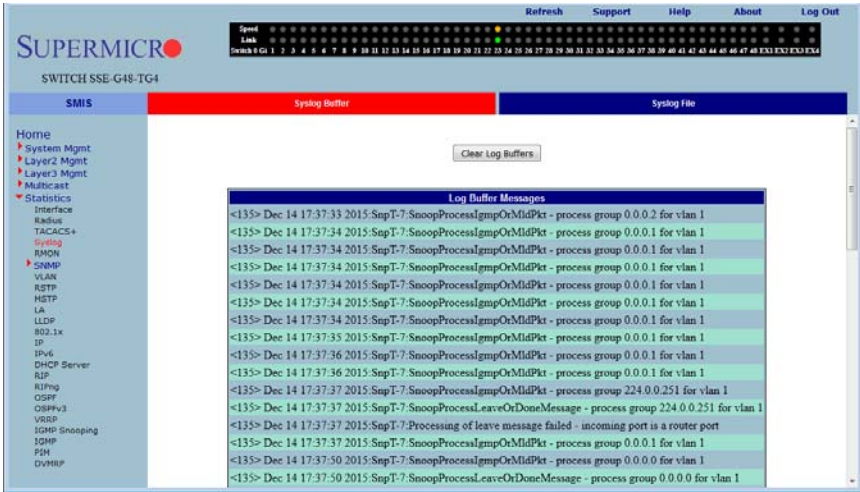
Syslog

The Syslog link allows you to configure the following pages:

- Syslog Buffer
- Syslog File

Syslog Buffer

Figure 5-170. Syslog Buffer Page

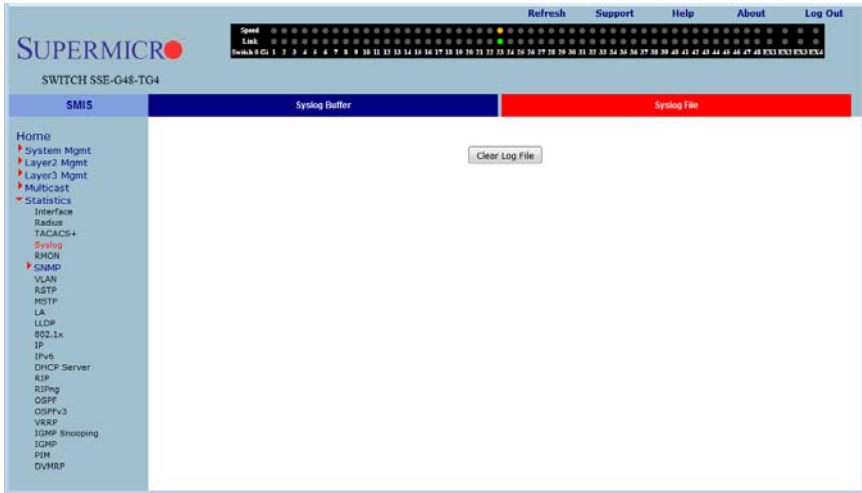


Clicking the SYSLOG BUFFER link brings up the SYSLOG BUFFER page (Figure 5-170), which displays syslog messages from syslog buffers in memory.

The CLEAR LOG BUFFERS button helps you to clear all messages in the syslog buffer memory.

Syslog File

Figure 5-171. Syslog File Page

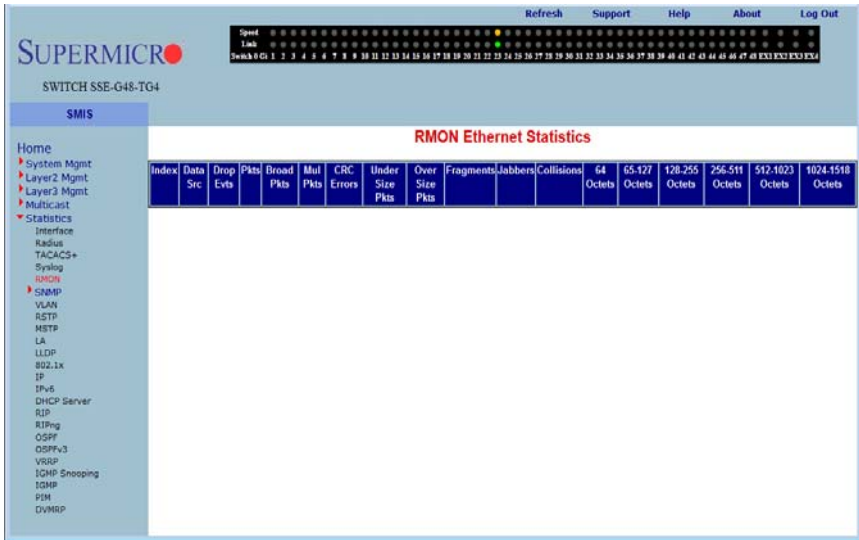


Clicking the SYSLOG FILE link brings up the SYSLOG FILE page (Figure 5-171), which displays syslog file in flash memory..

The CLEAR LOG FILE button helps you to remove all messages in the current syslog file.

RMON Ethernet Statistics

Figure 5-172. RMON Ethernet Statistics Page



Clicking the RMON link brings up the RMON ETHERNET STATISTICS page (Figure 5-172), which displays RMON Ethernet statistics information. The parameters for this page are shown in Table 5-146.

Table 5-146. RMON Ethernet Statistics Page Parameters

Parameter	Description
Index	This parameter specifies the index.
Port	This parameter specifies the port.
Octets	This parameter specifies the number of octets received.
Packets	This parameter specifies the number of packets received.
Broadcast Packets	This parameter specifies the number of broadcast packets received.
Multicast Packets	This parameter specifies the number of multicast packets received.
CRC Errors	This parameter specifies the number of packets received with crc errors.
Under Size Packets	This parameter specifies the number of under size packets received.
Over Size Packets	This parameter specifies the number of over size packets received.
Fragments	This parameter specifies the number of fragments received.
Jabbers	This parameter specifies the number of jabbers.
Collisions	This parameter specifies the number of collisions.

Table 5-146. RMON Ethernet Statistics Page Parameters (Continued)

Parameter	Description
64 Octets	This parameter specifies the number of Ethernet packets received with a size less than 64 bytes.
65-127 Octets	This parameter specifies the number of Ethernet packets received with a size between 65 and 127 bytes.
128-255 Octets	This parameter specifies the number of Ethernet packets received with a size between 128 and 255 bytes.
256-511 Octets	This parameter specifies the number of Ethernet packets received with a size between 256 and 511 bytes.
512-1023 Octets	This parameter specifies the number of Ethernet packets received with a size between 512 and 1023 bytes.
1024-1518 Octets	This parameter specifies the number of Ethernet packets received with a size between 1024 and 1518 bytes.

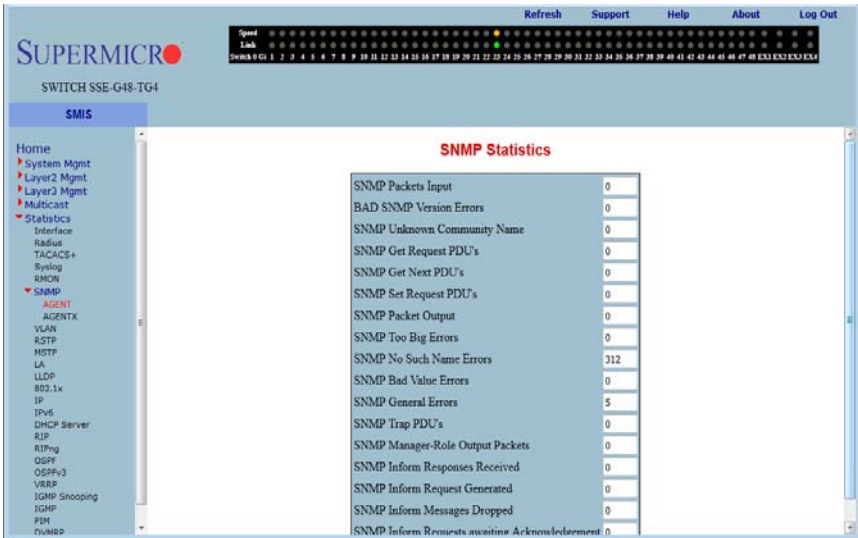
SNMP Statistics

The SNMP Statistics link allows you to configure SNMP Statistics through the following pages:

- [Agent](#)
- [AgentX](#)

Agent

Figure 5-173. SNMP Statistics Page



Clicking the AGENT link brings up the SNMP STATISTICS page (Figure 5-173), which displays SNMP statistics. The parameters for this page are shown in Table 5-147.

Table 5-147. SNMP Statistics Page Parameters

Parameter	Description
SNMP Packets Input	This parameter specifies the number of SNMP packets input.
BAD SNMP Version Errors	This parameter specifies the number of BAD SNMP version errors.
SNMP Unknown Community Name	This parameter specifies the number of SNMP unknown community names.
SNMP Get Request PDU's	This parameter specifies the number of SNMP Get Request PDU's.
SNMP Get Next PDU's	This parameter specifies the number of SNMP Get Next PDU's.

Table 5-147. SNMP Statistics Page Parameters (Continued)

Parameter	Description
SNMP Set Request PDU's	This parameter specifies the number of SNMP Set Request PDU's.
SNMP Packet Output	This parameter specifies the number of SNMP packets output.
SNMP Too Big Errors	This parameter specifies the number of SNMP Too Big errors,
SNMP No Such Name Errors	This parameter specifies the number of SNMP No Such Name errors,
SNMP Bad Value Errors	This parameter specifies the number of SNMP Bad Value errors.
SNMP General Errors	This parameter specifies the number of SNMP General errors.
SNMP Trap PDU's	This parameter specifies the number of SNMP Trap PDU's.
SNMP Manager-Role Output Packets	This parameter specifies the number of SNMP Manager-Role Output packets.
SNMP Inform Responses Received	This parameter specifies the number of SNMP Inform responses received.
SNMP Inform Request Generated	This parameter specifies the number of SNMP Inform requests generated.
SNMP Inform Messages Dropped	This parameter specifies the number of SNMP Inform messages dropped.
SNMP Inform Requests awaiting Acknowledgement	This parameter specifies the number of SNMP Inform requests awaiting acknowledgement.

AgentX

Figure 5-174. SNMP Agentx Subagent Settings page

The screenshot shows the SUPERMICR web management utility interface. The top navigation bar includes links for Refresh, Support, Help, About, and Log Out. The main content area is titled "Agentx Subagent Statistics" and displays the following data:

Tx Statistics	
Transmitted Packets	0
Open PDU	0
IndexAlloc PDU	0
Register PDU	0
Add Agent Caps PDU	0
Notify PDU	0
Ping PDU	0
Remove Agent Caps PDU	0
IndexDeAlloc PDU	0
UnRegister PDU	0
Close PDU	0
Response PDU	0
Rx Statistics	
Received Packets	0
Get Request PDU	0

The left sidebar shows the navigation menu with "AGENT" and "AGENTX" selected. The page title is "SWITCH SSE-G48-TG4".

Clicking the [AGENTX](#) link brings up the [SNMP AGENTX SUBAGENT SETTINGS](#) page which displays Agentx Subagent information. The parameters for this page are shown in [Table 5-148](#).

Table 5-148. Agentx Subagent Statistics Page Parameters

Parameter	Description
Transmit Statistics	
Transmitted Packets	This parameter specifies the number of packets transmitted.
Open PDU	This parameter specifies the number of open PDUs transmitted.
IndexAlloc PDU	This parameter specifies the number of IndexAlloc PDUs transmitted.
Register PDU	This parameter specifies the number of register PDUs transmitted.
Add Agent Caps PDU	This parameter specifies the number of add agent caps PDUs transmitted.
Notify PDU	This parameter specifies the number of notify PDUs transmitted.
Ping PDU	This parameter specifies the number of ping PDUs transmitted.
Remove Agent Caps PDU	This parameter specifies the number of remove agent caps PDUs transmitted.
IndexDeAlloc PDU	This parameter specifies the number of IndexDeAlloc PDUs transmitted.
UnRegister PDU	This parameter specifies the number of unregister PDUs transmitted.
Close PDU	This parameter specifies the number of close PDUs transmitted.
Response PDU	This parameter specifies the number of response PDUs transmitted.
Receive Statistics	
Received Packets	This parameter specifies the number of packets received.
Get Request PDU	This parameter specifies the number of get request PDUs received.
Get Next PDU	This parameter specifies the number of get next PDUs received.
Get Bulk PDU	This parameter specifies the number of get bulk PDUs received.
TestSet PDU	This parameter specifies the number of test set PDUs received.
Commit PDU	This parameter specifies the number of commit PDUs received.
Cleanup PDU	This parameter specifies the number of cleanup PDUs received.
Undo PDU	This parameter specifies the number of undo PDUs received.
Dropped Packets	This parameter specifies the number of dropped packets.
Parse Drop Errors	This parameter specifies the number of received PDUs dropped due to parse errors.
Open Fail Errors	This parameter specifies the number of open fail PDUs received.
Close PDU	This parameter specifies the number of close PDUs received.
Response PDU	This parameter specifies the number of response PDUs received.

VLAN

The VLAN link allows you to view VLAN statistics through the following pages:

- [Current DB](#)
- [Multicast Table](#)
- [Capabilities](#)
- [MAC Address Table](#)

Current DB

Figure 5-175. VLAN Current Database Page

The screenshot shows the SUPERMICR web interface for a SWITCH SSE-G48-TG4. The 'CurrentDB' tab is selected, displaying the 'VLAN Current Database' page. A table lists the following entry:

VLAN ID	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	1	Gr0/1-48, Ex0/1-4	Gr0/1-48, Ex0/1-4	Permanent

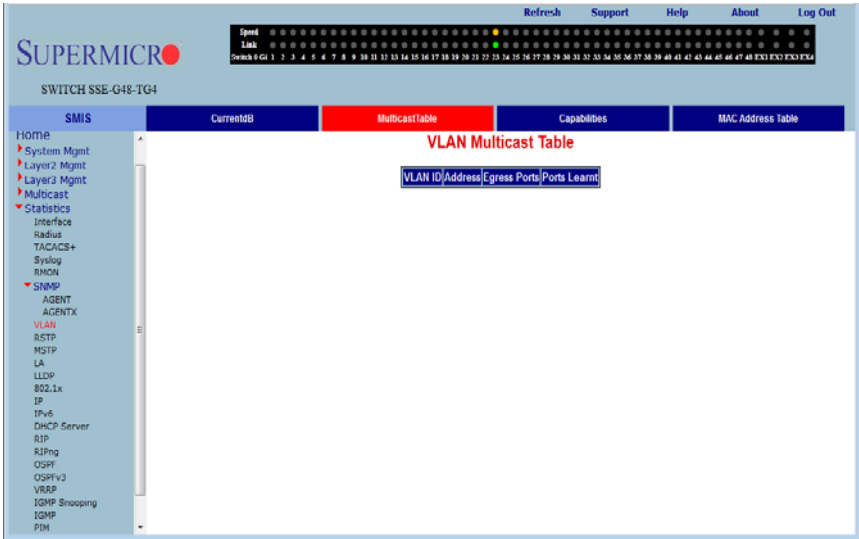
Clicking the CURRENT DB tab brings up the VLAN CURRENT DATABASE page (Figure 5-175), which displays VLAN database entries. The parameters for this page are shown in Table 5-149.

Table 5-149. VLAN Current Database Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
VLAN FDB ID	This parameter specifies the VLAN filter database identifier.
Member Ports	This parameter specifies the index of member ports.
Untagged Ports	This parameter specifies the index of untagged member ports.
Status	This parameter specifies the VLAN status.

Multicast Table

Figure 5-176. VLAN Multicast Table Page



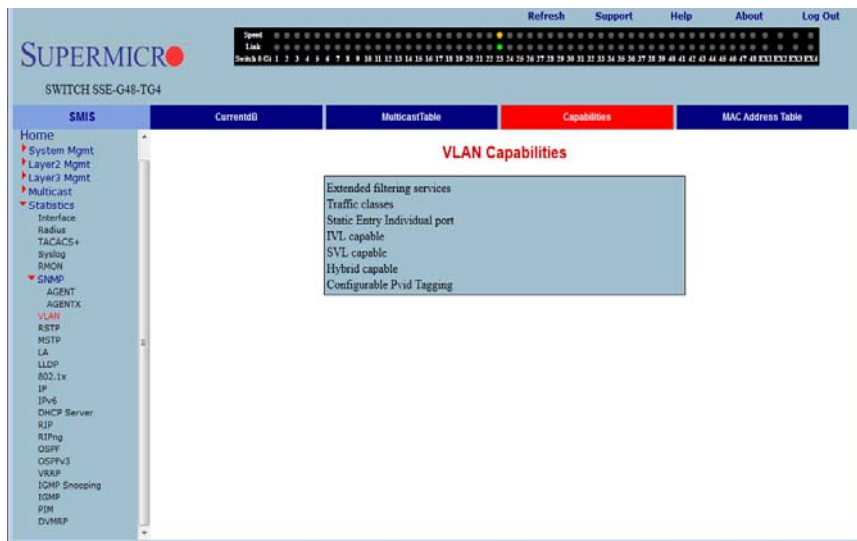
Clicking the MULTICAST TABLE tab brings up the VLAN MULTICAST TABLE page (Figure 5-176), which displays multicast VLAN information. The parameters for this page are shown in Table 5-150.

Table 5-150. VLAN Multicast Table Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
Address	This parameter specifies the VLAN address.
Egress Ports	This parameter specifies the indexes of egress ports.
Ports Learnt	This parameter specifies the indexes of ports on this VLAN that are learned.

Capabilities

Figure 5-177. VLAN Capabilities Page



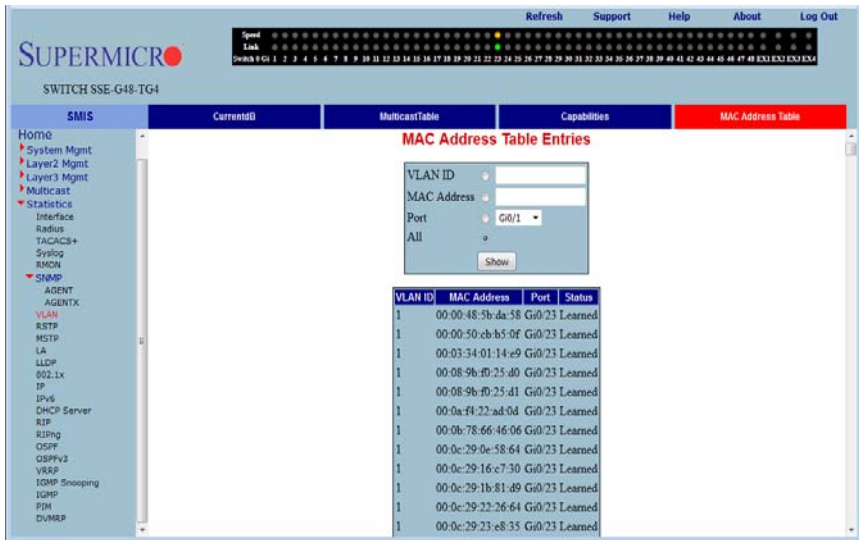
Clicking the CAPABILITIES tab brings up the VLAN CAPABILITIES page (Figure 5-177), which displays the VLAN capabilities of the switch. The parameters for this page are shown in Table 5-151.

Table 5-151. VLAN Capabilities Page Parameters

Parameter	Description
Extended Filtering Services	This parameter specifies the number of extended filtering services.
Traffic Classes	This parameter specifies the number of traffic classes
Static Entry Individual port	This parameter specifies the number of Static Entry Individual ports.
IVL capable	This parameter specifies the number of IVL capables.
SVL capable	This parameter specifies the number of SVL capables.
Hybrid capable	This parameter specifies the number of Hybrid capables.
Configurable PVID Tagging	This parameter specifies the number of Configurable PVID taggings.

MAC Address Table

Figure 5-178. MAC Address Table Entries Page



Clicking the MAC ADDRESS TABLE tab brings up the MAC ADDRESS TABLE ENTRIES page (Figure 5-178), which displays VLAN filter database entries. The parameters for this page are shown in Table 5-152.

Table 5-152. MAC Address Table Entries Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
MAC Address	This parameter specifies the MAC address learned.
Port	This parameter specifies the Index of port where this entry is learned.
Status	This parameter specifies the Status of this entry.
All	Use this parameter to get a display of the VLAN ID, MAC address and Port details.

RSTP Statistics

The RSTP STATISTICS link allows you to view RSTP statistics through the following pages:

- [Information](#)
- [Port Statistics](#)

Information

Figure 5-179. RSTP Information Page

The screenshot shows the SUPERMICR web interface for a SWITCH SSE-G48-TG4. The main content area is titled 'RSTP Information' and contains a table with the following columns: Context Id, Protocol Specification, Time Since Topology Change, Designated Root, Root Brg Priority, Root Cost, Root Port, Max Age, Hello Time, Hold Time, and Forward Delay. The left sidebar shows a navigation menu with 'RSTP' selected under the 'Statistics' section.

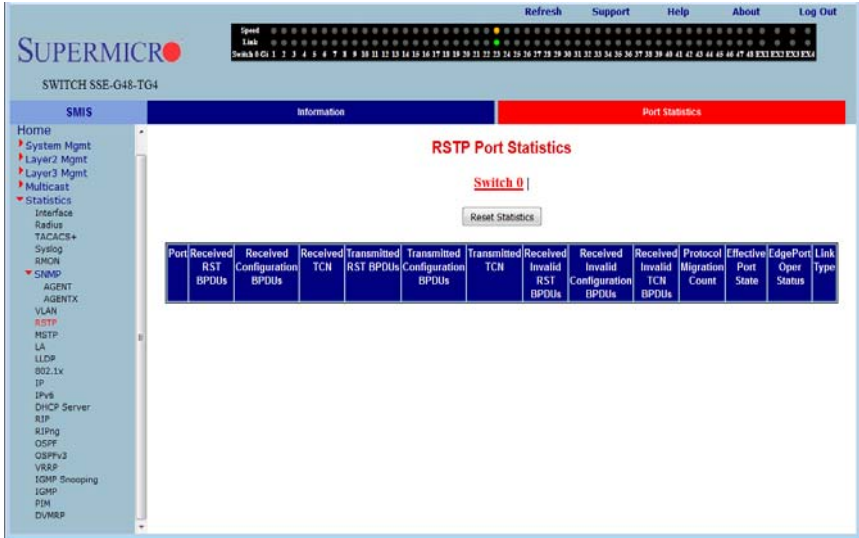
Clicking the INFORMATION tab brings up the RSTP INFORMATION page (Figure 5-179), which displays RSTP statistics. The parameters for this page are shown in Table 5-153.

Table 5-153. RSTP Information Page Parameters

Parameter	Description
Context ID	This parameter specifies the Context identifier.
Protocol Specification	This parameter specifies the Protocol Specification.
Time Since Topology Change	This parameter specifies the number of seconds since topology changed.
Designated Root	This parameter specifies the designated root bridge address.
Root Brg Priority	This parameter specifies the priority of root bridge.
Root Cost	This parameter specifies the cost to root.
Root Port	This parameter specifies the index of the root port.
Max Age	This parameter specifies the max age in seconds.
Hello Time	This parameter specifies the Hello time in seconds.
Hold Time	This parameter specifies the hold time in seconds.
Forward Delay	This parameter specifies the forward delay in seconds.

Port Statistics

Figure 5-180. RSTP Port Statistics Page



Clicking the PORT STATISTICS tab brings up the RSTP PORT STATISTICS page (Figure 5-180), which displays RSTP port level statistics. The parameters for this page are shown in Table 5-154.

Table 5-154. RSTP Port Statistics Page Parameters

Parameter	Description
Port	This parameter specifies the port index.
Received RST BPDUs	This parameter specifies the number of RSTP BPDUs received.
Received Configuration BPDUs	This parameter specifies the number of config BPDUs received.
Received TCN	This parameter specifies the number of topology changed notifications received.
Transmitted RST BPDUs	This parameter specifies the number of RSTP BPDUs transmitted.
Transmitted Configuration BPDUs	This parameter specifies the number of config BPDUs transmitted.
Transmitted TCN	This parameter specifies the number of topology change notifications transmitted.
Received Invalid RST BPDUs	This parameter specifies the number of invalid RSTP BPDUs received.

Table 5-154. RSTP Port Statistics Page Parameters (Continued)

Parameter	Description
Received Invalid Configuration BPDUs	This parameter specifies the number of invalid configuration BPDUs received.
Received Invalid TCN BPDUs	This parameter specifies the number of invalid topology change BPDUs received.
Protocol Migration Count	This parameter specifies the number of times protocol migration happened.
Effective Port State	This parameter specifies the effective port state.
EdgePort Oper Status	This parameter specifies the operational status of edge port.
Link Type	This parameter specifies the broadcast or point-to-point.
Reset Statistics Button	This button is used to set all field values to 0.

MSTP Statistics

The MSTP Statistics link allows you to view MSTP statistics through the following pages:

- [MSTP Information](#)
- [CIST Port Statistics](#)
- [MSTI Port Statistics](#)

MSTP Information

Figure 5-181. MSTP Information Page

The screenshot shows the SUPERMICR web management utility interface. At the top, there are navigation links: Refresh, Support, Help, About, and Log Out. Below the navigation is a status bar with a speed indicator and a search bar. The main content area is titled "MSTP Information" and contains a table with the following data:

Context Id	Bridge Address	CIST Root	Regional Root	CIST Root Cost	Reg Root Cost	Root Port	Hold Time	Max Age	Forward Delay	CIST Time Since Topology Change	Topology Changes	
0	00-30-48-e0-29-84	80-00-00-12-34-56	78-00-80-00-00-30-48	e0-29-84-2000	40000	0	23	1	20	15	25710348	1

The left sidebar shows a navigation menu with options like Home, System Mgmt, Layer2 Mgmt, Layer3 Mgmt, Multicast, and Statistics. The Statistics menu is expanded, showing options like Interface, Radius, TACACS+, Syslog, RMON, and SNMP.

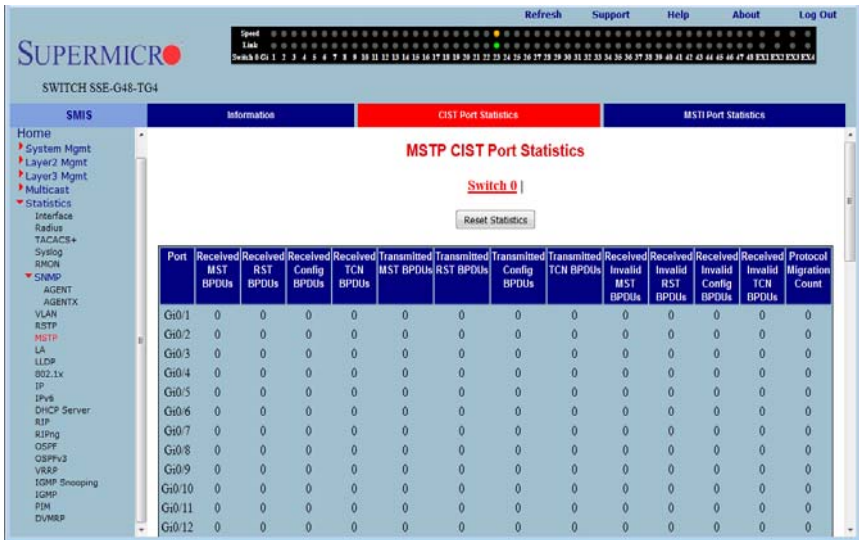
Clicking the INFORMATION tab brings up the MSTP INFORMATION page (Figure 5-135), which displays MSTP statistics. The parameters for this page are shown in Table 5-12.

Table 5-155. MSTP Information Page Parameters

Parameter	Description
Context ID	This parameter specifies the Context identifier.
Bridge Address	This parameter specifies the Bridge Address.
CIST Root	This parameter specifies the CIST root.
Regional Root	This parameter specifies the Regional root.
CIST Root Cost	This parameter specifies the CIST root cost.
Regional Root Cost	This parameter specifies the Regional root cost.
Root Port	This parameter specifies the index of the root port.
Hold Time	This parameter specifies the hold time in seconds.
Max Age	This parameter specifies the maximum age in seconds.
Forward Delay	This parameter specifies the forward delay in seconds.
CIST Time Since Topology Change	This parameter specifies the number of seconds since topology last changed.
Topology Changes	This parameter specifies the number of topology changes.

CIST Port Statistics

Figure 5-182. MSTP CIST Port Statistics Page



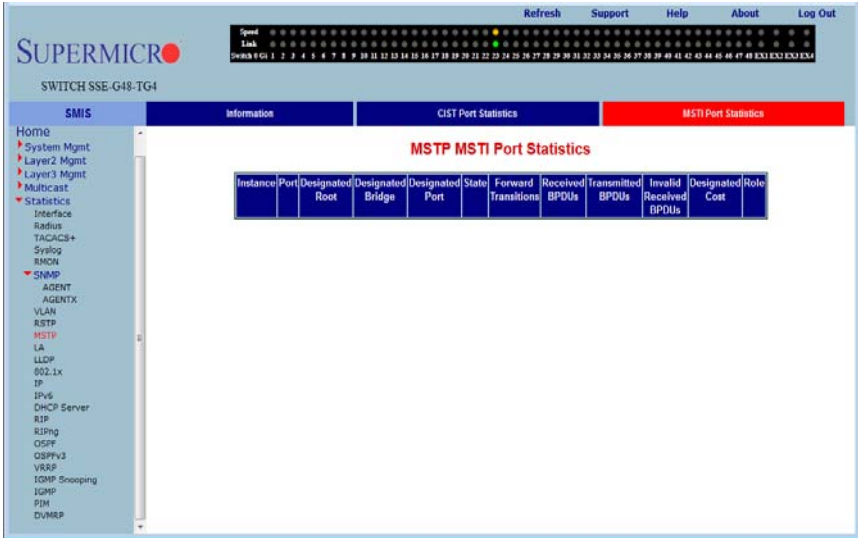
Clicking the CIST PORT STATISTICS tab brings up the MSTP CIST PORT STATISTICS page (Figure 5-182), which displays STP CIST port level statistics. The parameters for this page are shown in Table 5-156.

Table 5-156. MSTP CIST Port Statistics Page Parameters

Parameter	Description
Received MST BPDUs	This parameter specifies the number of MSTP BPDUs received.
Received RST BPDUs	This parameter specifies the number of RSTP BPDUs received.
Received Config BPDUs	This parameter specifies the number of config BPDUs received.
Received TCN BPDUs	This parameter specifies the number of topology change notification BPDUs received.
Transmitted MST BPDUs	This parameter specifies the number of MSTP BPDUs transmitted.
Transmitted RST BPDUs	This parameter specifies the number of RSTP BPDUs transmitted.
Transmitted Config BPDUs	This parameter specifies the number of config BPDUs transmitted.
Transmitted TCN BPDUs	This parameter specifies the number of topology change notification BPDUs transmitted.
Received Invalid MST BPDUs	This parameter specifies the number of invalid MSTP BPDUs received.
Received Invalid RST BPDUs	This parameter specifies the number of invalid RSTP BPDUs received.
Received Invalid Config BPDUs	This parameter specifies the number of invalid config BPDUs received.
Received Invalid TCN BPDUs	This parameter specifies the number of invalid TCN BPDUs received.
Protocol Migration Count	This parameter specifies the number of times protocol migration happened.
Reset Statistics Button	This button is used to set all field values to 0.

MSTI Port Statistics

Figure 5-183. MSTP MSTI Port Statistics Page



Clicking the MSTI PORT STATISTICS tab brings up the MSTP MSTI PORT STATISTICS page (Figure 5-183), which displays MSTP MSTI port level statistics. The parameters for this page are shown in Table 5-157.

Table 5-157. MSTP MSTI Port Statistics Page Parameters

Parameter	Description
Instance	This parameter specifies the MSTP instance Identifier.
Port	This parameter specifies the port index.
Designated Root	This parameter specifies the designated root bridge address.
Designated Bridge	This parameter specifies the designated Bridge address.
Designated Port	This parameter specifies the index of designated port for this MSTP instance.
State	This parameter specifies the current state.
Forward Transitions	This parameter specifies the number of Forward Transitions.
Received BPDUs	This parameter specifies the number of BPDUs received.
Transmitted BPDUs	This parameter specifies the number of BPDUs transmitted.
Invalid Received BPDUs	This parameter specifies the number of invalid BPDUs received.
Designated Cost	This parameter specifies the designated cost.
Role	This parameter specifies the current role.

Link Aggregation (LA)

The Link Aggregation link allows you to view Link Aggregation (LA) statistics through the following pages:

- [Port LACP Stats](#)
- [Neighbor Stats](#)

Port LACP Stats

Figure 5-184. LA Port Statistics Page

The screenshot shows the SUPERMICRO web management utility interface. The main content area is titled "LA Port Statistics" for "Switch 0". It contains a table with the following data:

Port	Received PDUs	Received Marker PDUs	Received Marker Response	Received Unknown PDUs	Received Illegal PDUs	Transmitted PDUs	Transmitted Marker PDUs	Transmitted Marker Response
Gi0/1	0	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0	0
Gi0/8	0	0	0	0	0	0	0	0
Gi0/9	0	0	0	0	0	0	0	0
Gi0/10	0	0	0	0	0	0	0	0
Gi0/11	0	0	0	0	0	0	0	0
Gi0/12	0	0	0	0	0	0	0	0
Gi0/13	0	0	0	0	0	0	0	0
Gi0/14	0	0	0	0	0	0	0	0
Gi0/15	0	0	0	0	0	0	0	0

Clicking the PORT LACP STATS tab brings up the LA PORT STATISTICS page (Figure 5-184), which displays LACP port level statistics. The parameters for this page are shown in Table 5-158.

Table 5-158. LA Port Statistics Page Parameters

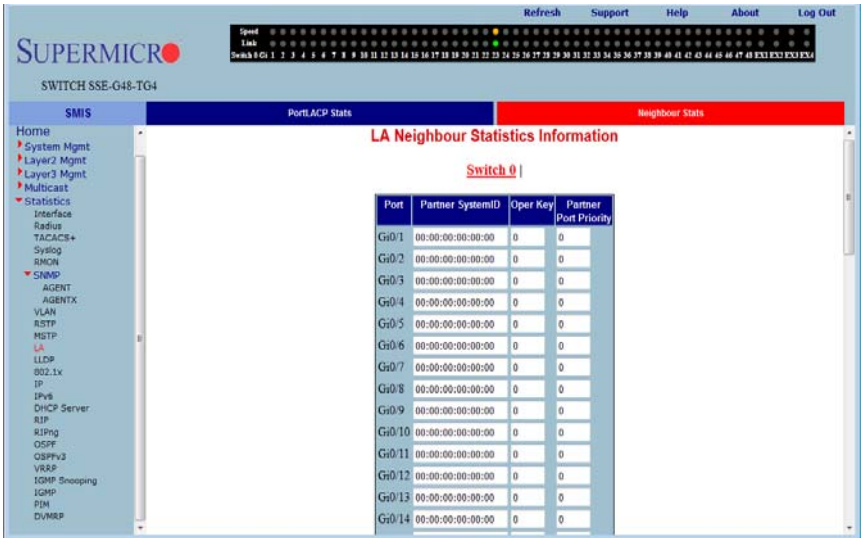
Parameter	Description
Port	This parameter specifies the port index.
Received PDUs	This parameter specifies the number of LACP PDUs received.
Received Marker PDUs	This parameter specifies the number of Marker PDUs received.
Received Marker Response	This parameter specifies the number of Marker response PDUs received.
Received Unknown PDUs	This parameter specifies the number of unknown PDUs received.

Table 5-158. LA Port Statistics Page Parameters (Continued)

Parameter	Description
Received Illegal PDUs	This parameter specifies the number of invalid PDUs received.
Transmitted PDUs	This parameter specifies the number of LACP PDUs transmitted.
Transmitted Marker PDUs	This parameter specifies the number of Marker PDUs transmitted.
Transmitted Marker Response	This parameter specifies the number of Marker response PDUs transmitted.

Neighbor Stats

Figure 5-185. LA Neighbor Statistics Information Page



Clicking the NEIGHBOR STATS tab brings up the LA NEIGHBOR STATISTICS INFORMATION page (Figure 5-185), which displays LACP neighbor statistics. The parameters for this page are shown in Table 5-159.

Table 5-159. LA Neighbor Statistics Information Page Parameters

Parameter	Description
Port Index	This parameter specifies the port index.
Partner SystemID	This parameter specifies the Partner SystemID.
Oper Key	This parameter specifies the Oper Key.
Partner Port Priority	This parameter specifies the Partner Port Priority.

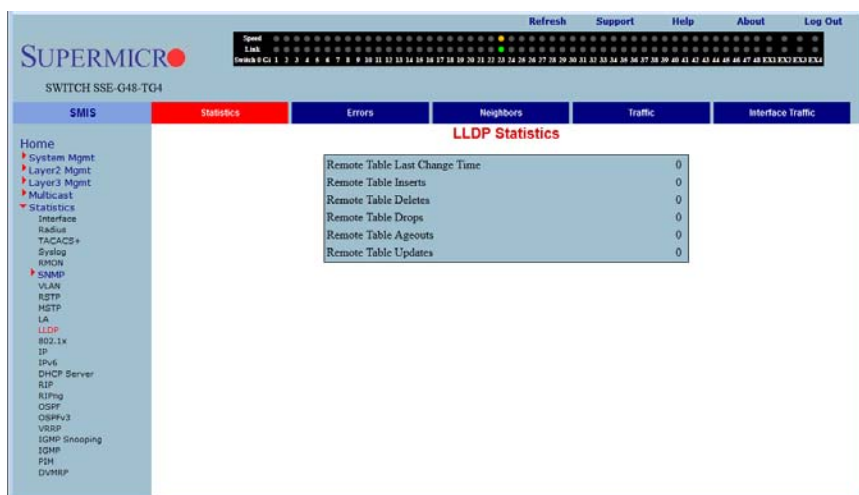
LLDP

The LLDP link allows you to view LLDP statistics through the following pages:

- [Statistics](#)
- [Errors](#)
- [Neighbors](#)
- [Traffic](#)
- [Interface Traffic](#)

Statistics

Figure 5-186. LLDP Statistics Page



Clicking the STATISTICS link brings up the LLDP STATISTICS page (Figure 5-186), which displays LLDP statistics information. The parameters for this page are shown in Table 5-160.

Table 5-160. LLDP Statistics Page Parameters

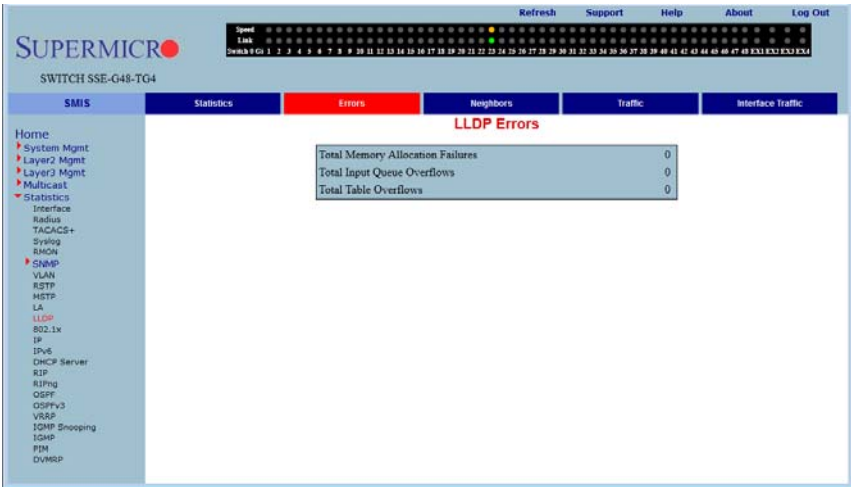
Parameter	Description
Remote Table Last Change Time	This parameter specifies the time since the last time remote LLDP information table got changed.
Remote Table Inserts	This parameter specifies the number of inserts happened on remote information table.
Remote Table Deletes	This parameter specifies the number of deletes happened on remote information table.
Remote Table Drops	This parameter specifies the number of drops happened on remote information table.

Table 5-160. LLDP Statistics Page Parameters (Continued)

Parameter	Description
Remote Table Ageouts	This parameter specifies the number of ageouts happened on remote information table.
Remote Table Updates	This parameter specifies the number of times remote information table got updated.

Errors

Figure 5-187. LLDP Errors Page



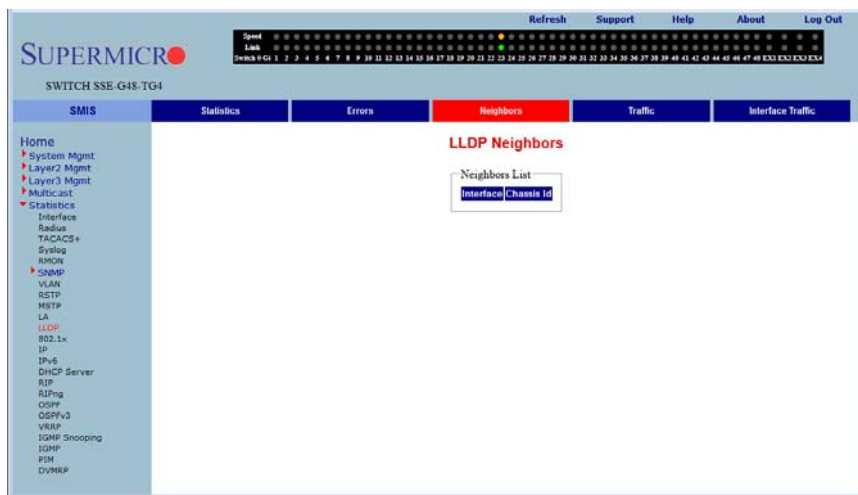
Clicking the ERRORS link brings up the LLDP ERRORS page (Figure 5-187), which displays LLDP error information. The parameters for this page are shown in Table 5-161.

Table 5-161. LLDP Errors Page Parameters

Parameter	Description
Total Memory Allocation Failures	This parameter specifies the number of memory allocation failed in LLDP feature.
Total Input Queue Overflows	This parameter specifies the number of times the LLDP input queue overflowed.
Total Table Overflows	This parameter specifies the number of times the LLDP remote table got overflowed.

Neighbors

Figure 5-188. LLDP Neighbors Page



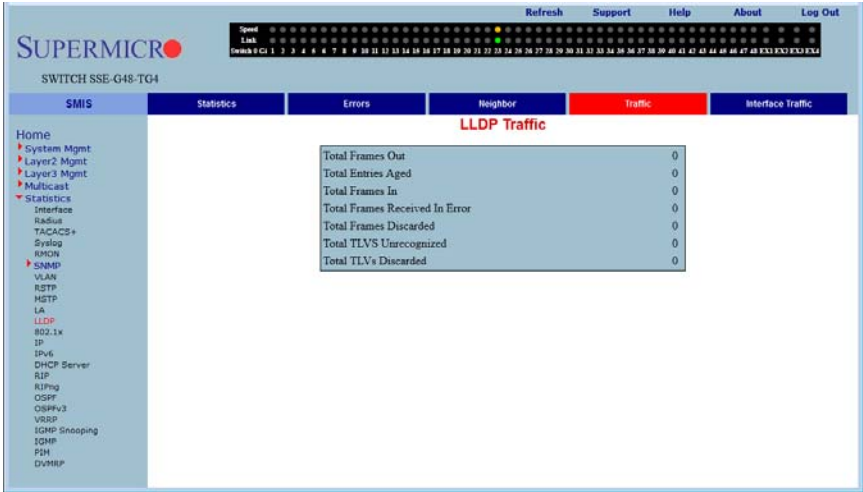
Clicking the NEIGHBORS link brings up the LLDP NEIGHBORS page (Figure 5-188), which displays LLDP error information. The parameters for this page are shown in Table 5-162.

Table 5-162. LLDP Neighbors Page Parameters

Parameter	Description
Neighbor List	This table specifies the Interface and Chassis ID.
Interface	This parameter specifies the Interface name on which this neighbor is learned.
Chassis ID	This parameter specifies the value of the chassis identifier.

Traffic

Figure 5-189. LLDP Traffic Page



Clicking the TRAFFIC link brings up the LLDP TRAFFIC page (Figure 5-189), which displays LLDP error information. The parameters for this page are shown in Table 5-163.

Table 5-163. LLDP Traffic Page Parameters

Parameter	Description
Total Frames Out	This parameter specifies the number of LLDP packets sent out from switch in all interfaces.
Total Entries Aged	This parameter specifies the number of LLDP neighbor entries aged out.
Total Frames In	This parameter specifies the number of LLDP packets received in by switch in all interfaces.
Total Frames Received In Error	This parameter specifies the number of LLDP packets received with Error.
Total Frames Discarded	This parameter specifies the number of LLDP packets discarded due to error and other failure conditions.
Total TLVs Unrecognized	This parameter specifies the number of TLVs received could not recognized properly.
Total TLVs Discarded	This parameter specifies the number of TLVs discarded due to invalidity.

Interface Traffic

Figure 5-190. LLDP Interface Traffic Page

Interface	Total Frames Out	Total Entries Aged	Total Frames In	Total Frames Received In Error	Total Frames Discarded	Total TLV's Unrecognized	Total TLV's Discarded
Gi0/1	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0
Gi0/8	0	0	0	0	0	0	0
Gi0/9	0	0	0	0	0	0	0
Gi0/10	0	0	0	0	0	0	0
Gi0/11	0	0	0	0	0	0	0
Gi0/12	0	0	0	0	0	0	0
Gi0/13	0	0	0	0	0	0	0
Gi0/14	0	0	0	0	0	0	0
Gi0/15	0	0	0	0	0	0	0

Clicking the INTERFACE TRAFFIC link brings up the LLDP INTERFACE TRAFFIC page (Figure 5-190), which displays LLDP error information. The parameters for this page are shown in Table 5-164.

Table 5-164. LLDP Interface Traffic Page Parameters

Parameter	Description
Interface	This parameter specifies the Interface index.
Total Frames Out	This parameter specifies the number of LLDP packets sent out from switch in all interfaces.
Total Entries Aged	This parameter specifies the number of LLDP neighbor entries aged out.
Total Frames In	This parameter specifies the number of LLDP packets received in by switch in all interfaces.
Total Frames Received In Error	This parameter specifies the number of LLDP packets received with Error.
Total Frames Discarded	This parameter specifies the number of LLDP packets discarded due to error and other failure conditions.
Total TLVS Unrecognized	This parameter specifies the number of TLVs received could not recognized properly.
Total TLVs Discarded	This parameter specifies the number of TLVs discarded due to invalidity.

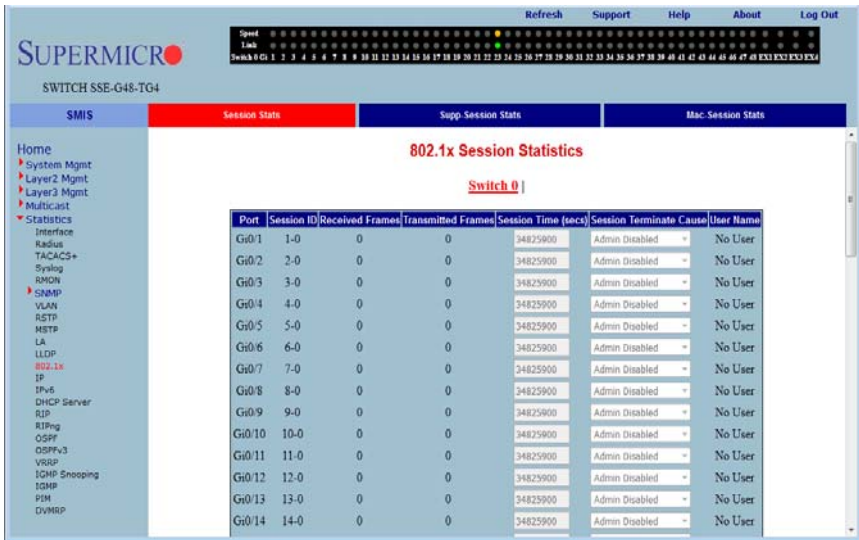
802.1X

- [Session Stats](#)

- [Supp-Session Stats](#)
- [Mac-Session Stats](#)

Session Stats

Figure 5-191. 802.1x Session Statistics Page



Clicking the SESSION STATS tab brings up the 802.1x SESSION STATISTICS page (Figure 5-191), which displays 802.1x statistics information. The parameters for this page are shown in Table 5-165.

Table 5-165. 802.1x Session Statistics Page Parameters

Parameter	Description
Port	This parameter specifies the port index.
Session ID	This parameter specifies the session identifier.
Received Frames	This parameter specifies the number of packets received.
Transmitted Frames	This parameter specifies the number of packets transmitted.
Session Time (secs)	This parameter specifies the session time in seconds.
Session Terminate Cause	This parameter specifies the reason for session termination.
User Name	This parameter specifies the name of the user authenticated.

Supp-Session Stats

Figure 5-192. 802.1x Supplicant Session Statistics Page

The screenshot shows the SUPERMICR web management utility interface. The main content area is titled "802.1x Supplicant Session Statistics" for "Switch 0". A table displays statistics for 15 ports (Gi0/1 to Gi0/15). The table has 14 columns: Port, Eapol FrRx, Eapol FrTx, Eapol Start FrTx, Eapol Logoff FrTx, Eapol Respld FrTx, Eapol Resp FrTx, Eapol ReqId FrRx, Eapol Req FrRx, Invalid Eapol FrRx, Eap LemEr FrRx, Last Eapol FrVersion, and Last Eapol FrSource. All values in the table are 0.

Port	Eapol FrRx	Eapol FrTx	Eapol Start FrTx	Eapol Logoff FrTx	Eapol Respld FrTx	Eapol Resp FrTx	Eapol ReqId FrRx	Eapol Req FrRx	Invalid Eapol FrRx	Eap LemEr FrRx	Last Eapol FrVersion	Last Eapol FrSource
Gi0/1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/5	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/6	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/7	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/8	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/9	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/10	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/11	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/12	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/13	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/14	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
Gi0/15	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00

Clicking the SUPP SESSION STATS tab brings up the 802.1x SUPPLICANT SESSION STATISTICS page (Figure 5-192), which displays information about the 802.1x supplicant session. The parameters for this page are shown in Table 5-166.

Table 5-166. 802.1x Supplicant Session Statistics Page Parameters

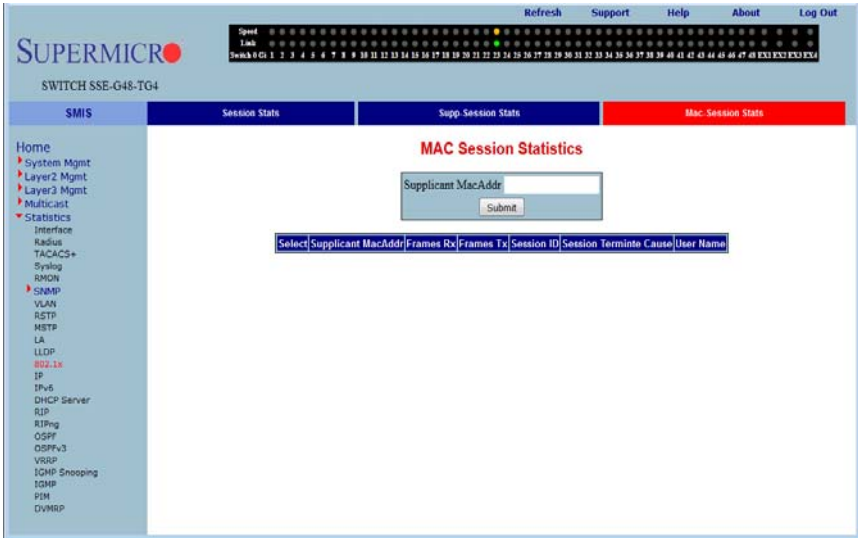
Parameter	Description
Port	This parameter specifies the port index.
Eapol FrRx	This parameter specifies the number of the EAPOL packets received.
Eapol FrTx	This parameter specifies the number of the EAPOL packets transmitted.
Eapol Start FrTx	This parameter specifies the number of the EAPOL start packet transmitted.
Eapol Logoff FrTx	This parameter specifies the number of the EAPOL logoff packet transmitted.
Eapol Respld FrTx	This parameter specifies the number of the EAPOL response identifier packet transmitted.
Eapol Resp FrTx	This parameter specifies the number of the EAPOL response packet frame transmitted.
Eapol ReqId FrRx	This parameter specifies the number of the EAPOL request identifier packet received.
Eapol Req FrRx	This parameter specifies the number of the EAPOL request frame received.
Invalid Eapol FrRx	This parameter specifies the number of the invalid EAPOL frame received.

Table 5-166. 802.1x Supplicant Session Statistics Page Parameters (Continued)

Parameter	Description
Eap LenErr FrRx	This parameter specifies the number of EAPOL packets received with an invalid length.
Last Eapol FrVersion	This parameter specifies the version on the last EAPOL packet.
Last Eapol FrSource	This parameter specifies the source of the last EAPOL packet.

Mac-Session Stats

Figure 5-193. MAC Session Statistics Page



Clicking the MAC SESSION STATS tab brings up the MAC SESSION STATISTICS page (Figure 5-193), which displays statistics information about 802.1x MAC sessions. The parameters for this page are shown in Table 5-167.

Table 5-167. MAC Session Statistics Page Parameters

Parameter	Description
Supplicant MacAddr	This parameter specifies the supplicant MAC address.
Frames Rx	This parameter specifies the number of packets received.
Frames Tx	This parameter specifies the number of packets transmitted.
Session ID	This parameter specifies the session identifier.
Session Terminate Cause	This parameter specifies the reason for session termination.
User Name	This parameter specifies the name of user authenticated.

IP

The IP link allows you to view IP statistics through the following pages:

- [ARP Cache](#)
- [ICMP Statistics](#)

ARP Cache

Figure 5-194. ARP Cache Page

The screenshot shows the SUPERMICRO web management utility interface. The top navigation bar includes 'Refresh', 'Support', 'Help', 'About', and 'Log Out'. The main content area is titled 'ARP Cache' and displays a table with the following data:

Interface	MAC Address	IP Address	Media Type
vlan1	00:25:90:67:3d:ce	172.31.32.101	Dynamic
vlan1	00:30:48:64:b1:00	172.31.35.41	Dynamic

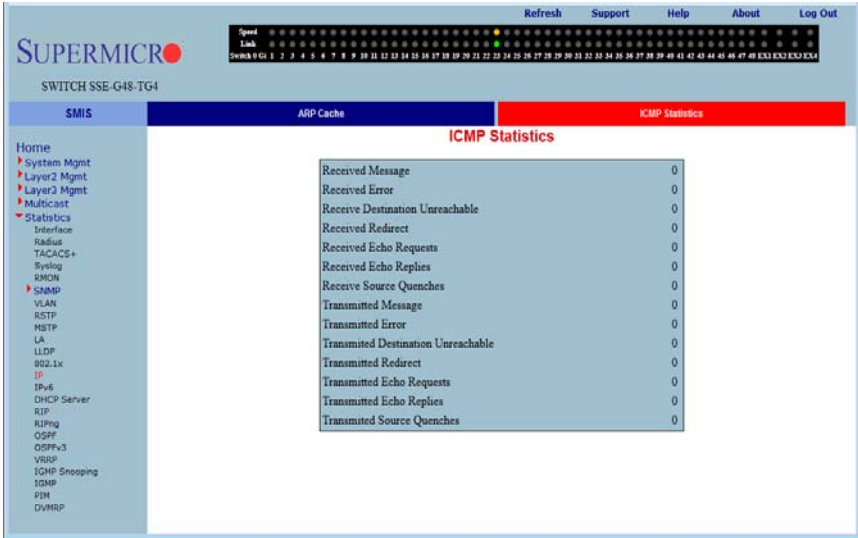
Clicking the ARP CACHE tab brings up the ARP CACHE page (Figure 5-194), which displays ARP entries. The parameters for this page are shown in Table 5-168.

Table 5-168. ARP Cache Page Parameters

Parameter	Description
Interface	This parameter specifies the interface from which this ARP entry is learned.
MAC Address	This parameter specifies the MAC address.
IP Address	This parameter specifies the IP address.
Media Type	This parameter specifies the static ARP or dynamic ARP.

ICMP Statistics

Figure 5-195. ICMP Statistics Page



Clicking the ICMP STATISTICS tab brings up the ICMP STATISTICS page (Figure 5-195), which displays ICMP statistics information. The parameters for this page are shown in Table 5-169.

Table 5-169. ICMP Statistics Page Parameters

Parameter	Description
Received Message	This parameter specifies the number of received messages.
Received Error	This parameter specifies the number of received errors.
Receive Destination Unreachable	This parameter specifies the number of received destination unreachables.
Received Redirect	This parameter specifies the number of received redirects.
Received Echo Requests	This parameter specifies the number of echo requests..
Received Echo Replies	This parameter specifies the number of echo replies.
Receive Source Quenches	This parameter specifies the number of source quenches.
Transmitted Message	This parameter specifies the number of transmitted messages.
Transmitted Error	This parameter specifies the number of transmitted errors.

Table 5-169. ICMP Statistics Page Parameters (Continued)

Parameter	Description
Transmitted Destination Unreachable	This parameter specifies the number of transmitted destination unreachable.
Transmitted Redirect	This parameter specifies the number of transmitted redirects.
Transmitted Echo Requests	This parameter specifies the number of transmitted echo requests.
Transmitted Echo Replies	This parameter specifies the number of transmitted echo replies.
Transmitted Source Quenches	This parameter specifies the number of transmitted source quenches.

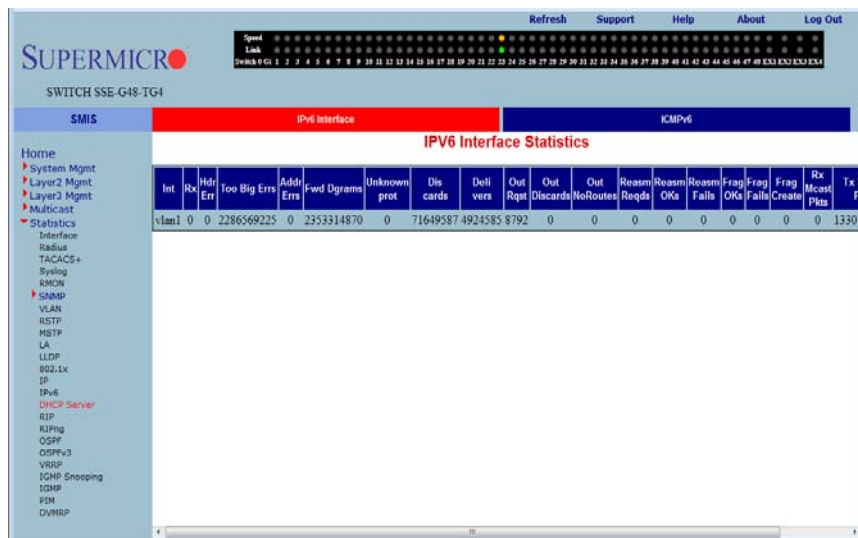
IPv6

The IPv6 link allows you to view IPv6 statistics through the following pages:

- [IPv6 Interface](#)
- [ICMPv6](#)

IPv6 Interface

Figure 5-196. IPV6 Interface Statistics Page



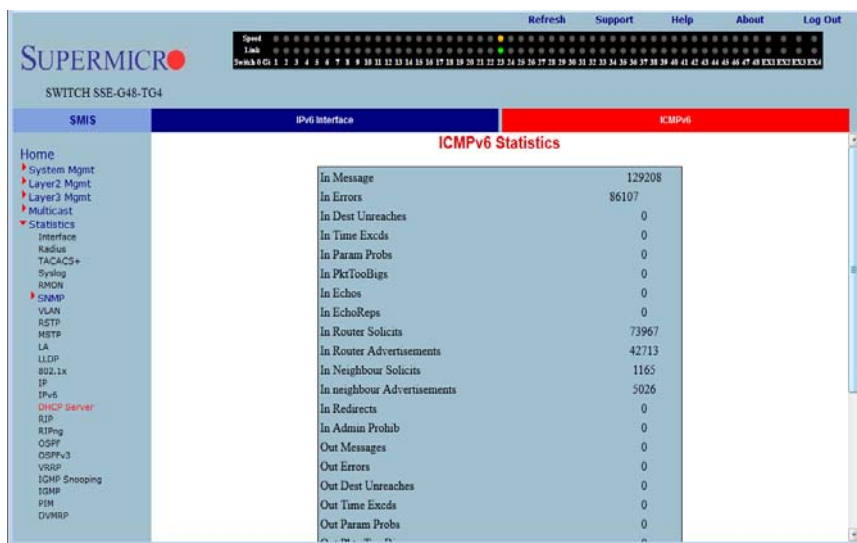
Clicking the IPV6 INTERFACE tab brings up the IPV6 INTERFACE STATISTICS page (Figure 5-196), which displays IPv6 port statistics. The parameters for this page are shown in Table 5-170.

Table 5-170. IPV6 Interface Statistics Page Parameters

Parameter	Description
Interface	This parameter specifies the Port index.
Rcvd	This parameter specifies the number of IPv6 packets received.
Hdr Err	This parameter specifies the number of IPv6 packets received with header error.
Too Big Errs	This parameter specifies the number of too big IPv6 packets received.
Addr Errs	This parameter specifies the number of IPv6 packets received with address errors.
Fwd Dgrams	This parameter specifies the number of IPv6 datagrams forwarded in this port.
Unknown protos	This parameter specifies the number of packets received with unknown protocol.
Discards	This parameter specifies the number of received packets discarded due to errors.
Delivers	This parameter specifies the number of packets delivered.
Out Rqst	This parameter specifies the number of transmit requests.
Out Discards	This parameter specifies the number of transmit discards due to errors.
Out No Routes	This parameter specifies the number of packets to be transmitted but no routes.
Reasm Reqds	This parameter specifies the number of reassembly requests.
Reasm OKs	This parameter specifies the number of successful reassemblies.
Reasm Fails	This parameter specifies the number of reassemblies failed.
Frag OKs	This parameter specifies the number of good fragments received.
Frag Fails	This parameter specifies the number of fragments incompletely received.
Frag Creates	This parameter specifies the number of fragments created.
Rcvd Mcast Pkts	This parameter specifies the number of received IPv6 multicast packets.
Send Mcast Pkts	This parameter specifies the number of IPv6 multicast packets transmitted.
Trunctd Pkts	This parameter specifies the number of packets truncated.

ICMPv6

Figure 5-197. ICMPv6 Statistics Page



Clicking the ICMPv6 tab brings up the ICMPv6 STATISTICS page (Figure 5-197), which displays ICMPv6 statistics. The parameters for this page are shown in Table 5-171.

Table 5-171. ICMPv6 Statistics Page Parameters

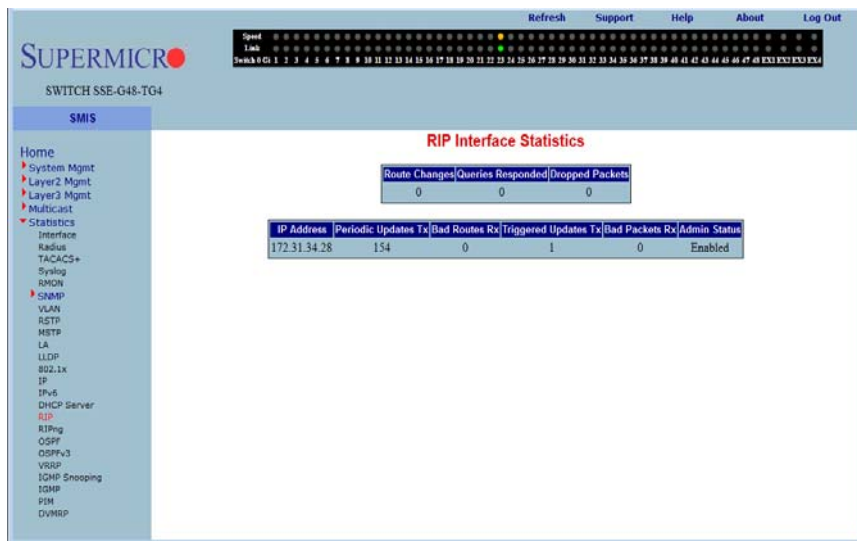
Parameter	Description
In Message	This parameter specifies the number of messages received.
In Errors	This parameter specifies the number of messages received with errors.
In Dest Unreaches	This parameter specifies the number of destination unreachable messages received.
In Time Excds	This parameter specifies the number of receive timeouts.
In Param Probs	This parameter specifies the number of parameters probed.
In PktTooBigs	This parameter specifies the number of too big packets received.
In Echos	This parameter specifies the number of echo requests received.
In EchoReps	This parameter specifies the number of echo responses received.
In Router Solicits	This parameter specifies the number of received router solicitations.
In Router Advertisements	This parameter specifies the number of routers advertisement received.
In Neighbor Solicits	This parameter specifies the number of received neighbor solicitations.
In Neighbor Advertisements	This parameter specifies the number of received neighbor advertisements.

Table 5-171. ICMPv6 Statistics Page Parameters (Continued)

Parameter	Description
In Redirects	This parameter specifies the number of redirect packets received.
In Admin Prohib	This parameter specifies the number of receive admin prohibited.
Out Messages	This parameter specifies the number of messages transmitted.
Out Errors	This parameter specifies the number of messages transmitted with errors.
Out Dest Unreaches	This parameter specifies the number of destination unreachable messages transmitted.
Out Time Excds	This parameter specifies the number of transmit timeouts.
Out Param Probs	This parameter specifies the number of parameters probed.
Out Pkts Too Big	This parameter specifies the number of too big packets transmitted.
Out Echos	This parameter specifies the number of echo requests transmitted.
Out Echo Reps	This parameter specifies the number of echo responses transmitted.
Out Route Solicits	This parameter specifies the number of transmitted router solicits.
Out Router Advertisements	This parameter specifies the number of transmitted neighbor solicits.
Out Neighbour Solicits	This parameter specifies the number of transmitted neighbor solicits.
Out Neighbour Advertisements	This parameter specifies the number of transmitted neighbor solicits.
Out Redirects	This parameter specifies the number of redirect packets transmitted.
Out Admin Prohib	This parameter specifies the number of transmit admin prohibited.
In Bad Code	This parameter specifies the number of bad code packets.

RIP

Figure 5-198. RIP Interface Statistics Page



Clicking the RIP link brings up the RIP INTERFACE STATISTICS page (Figure 5-198), which displays RIP statistics. The parameters for this page are shown in Table 5-172.

Table 5-172. RIP Interface Statistics Page Parameters

Parameter	Description
IP Address	This parameter specifies the IP address.
Received Bad Packets	This parameter specifies the number of received bad packets.
Received Bad Routes	This parameter specifies the number of received bad routes.
Transmitted Updates	This parameter specifies the the number of transmitted updates.

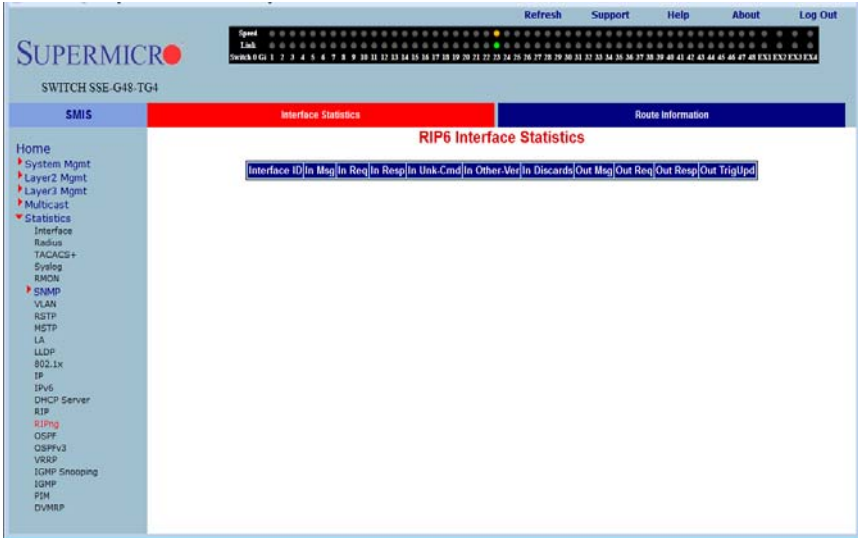
RIP6

The RIP6 link allows you to view RIP6 statistics through the following pages:

- [Interface Statistics](#)
- [Route Information](#)

Interface Statistics

Figure 5-199. RIP6 Interface Statistics Page



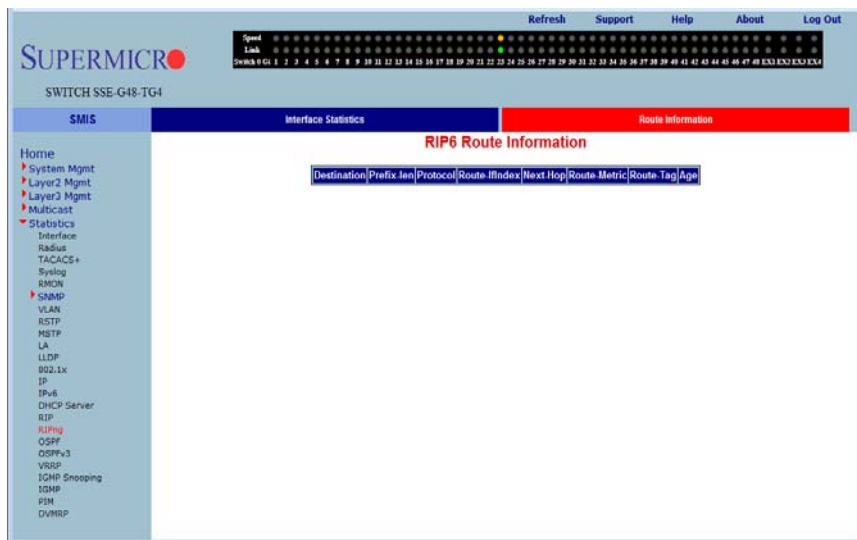
Clicking the INTERFACE STATISTICS tab brings up the RIP6 INTERFACE STATISTICS page (Figure 5-199), which displays RIPng statistics. The parameters for this page are shown in Table 5-173.

Table 5-173. RIP6 Interface Statistics Page Parameters

Parameter	Description
Interface ID	This parameter specifies the interface identifier.
In Msg	This parameter specifies the number of RIPng packets received.
In Req	This parameter specifies the number of RIPng request packets received.
In Resp	This parameter specifies the number of RIPng response packets received.
In Unk-Cmd	This parameter specifies the number of RIPng unknown command packets received.
In Other-Ver	This parameter specifies the number of RIPng other version packets received.
In Discards	This parameter specifies the number of received packets discarded.
Out Msg	This parameter specifies the number of RIPng packets transmitted.
Out Req	This parameter specifies the number of RIPng request packets transmitted.
Out Resp	This parameter specifies the number of RIPng response packets transmitted.
Out TrigUpd	This parameter specifies the number of RIPng triggered updates transmitted.

Route Information

Figure 5-200. RIP6 Route Information Page



Clicking the ROUTE INFORMATION tab brings up the RIP6 ROUTE INFORMATION page (Figure 5-200), which displays information about RIPng routes. The parameters for this page are shown in Table 5-174.

Table 5-174. RIP6 Route Information Page Parameters

Parameter	Description
Destination	This parameter specifies the route destination.
Prefix-len	This parameter specifies the length of the route prefix.
Protocol	This parameter specifies the routing protocol
Route-IfIndex	This parameter specifies the interface index.
Next-Hop	This parameter specifies the next hop for this route.
Route-Metric	This parameter specifies the metric of this route.
Route-Tag	This parameter specifies the route tag identifier.
Age	This parameter specifies the route age in seconds.

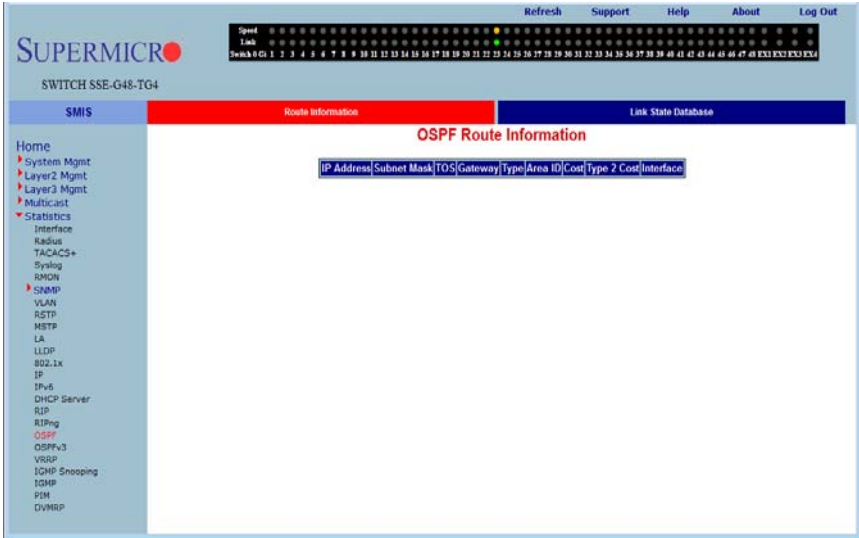
OSPF

The OSPF link allows you to view OSPF statistics through the following pages:

- [Route Information](#)
- [Link State Database](#)

Route Information

Figure 5-201. OSPF Route Information Page



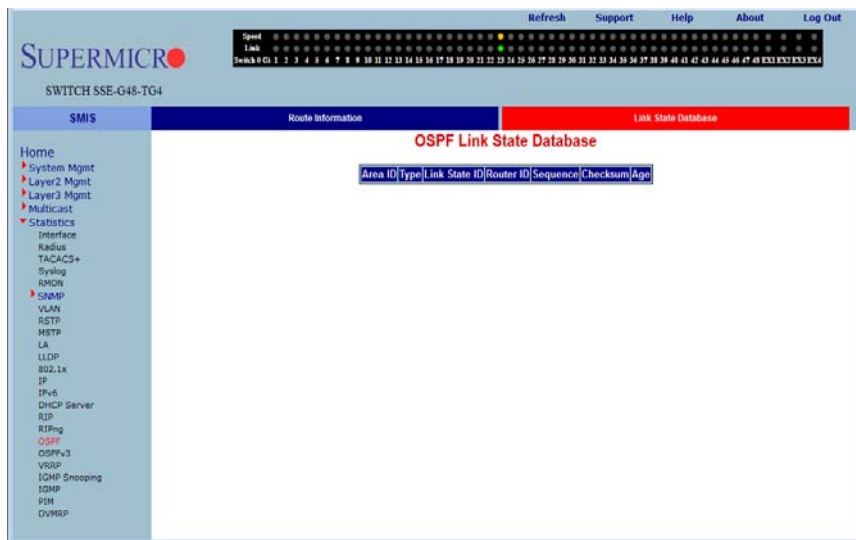
Clicking the ROUTE INFORMATION tab brings up the OSPF ROUTE INFORMATION page (Figure 5-201), which displays information about OSPF routes. The parameters for this page are shown in Table 5-175.

Table 5-175. OSPF Route Information Page Parameters

Parameter	Description
IP Address	This parameter specifies the IP address.
Subnet Mask	This parameter specifies the Subnet Mask.
TOS	This parameter specifies the TOS.
Gateway	This parameter specifies the gateway.
Type	This parameter specifies the type.
Area ID	This parameter specifies the Area ID.
Cost	This parameter specifies the cost.
Type 2 Cost	This parameter specifies the Type 2 cost.
Interface	This parameter specifies the interface.

Link State Database

Figure 5-202. OSPF Link State Database Page



Clicking the LINK STATE DATABASE tab brings up the OSPF LINK STATE DATABASE page (Figure 5-202), which displays information about OSPF link state database. The parameters for this page are shown in Table 5-176.

Table 5-176. OSPF Link State Database Page Parameters

Parameter	Description
Area ID	This parameter specifies the area identifier.
Type	This parameter specifies the link state type.
Link State ID	This parameter specifies the link state identifier.
Router ID	This parameter specifies the router identifier.
Sequence	This parameter specifies the sequence number of this link state information.
Checksum	This parameter specifies the checksum.
Age	This parameter specifies the link state information age in seconds.

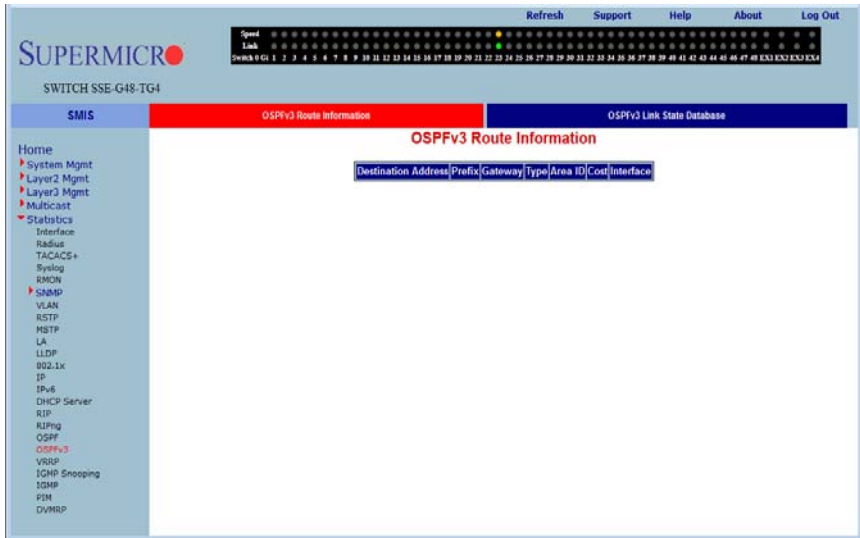
OSPFv3

The OSPFv3 link allows you to view OSPFv3 statistics through the following pages:

- [OSPFv3 Route Information](#)
- [OSPFv3 Link State Database](#)

OSPFv3 Route Information

Figure 5-203. OSPFv3 Route Information Page



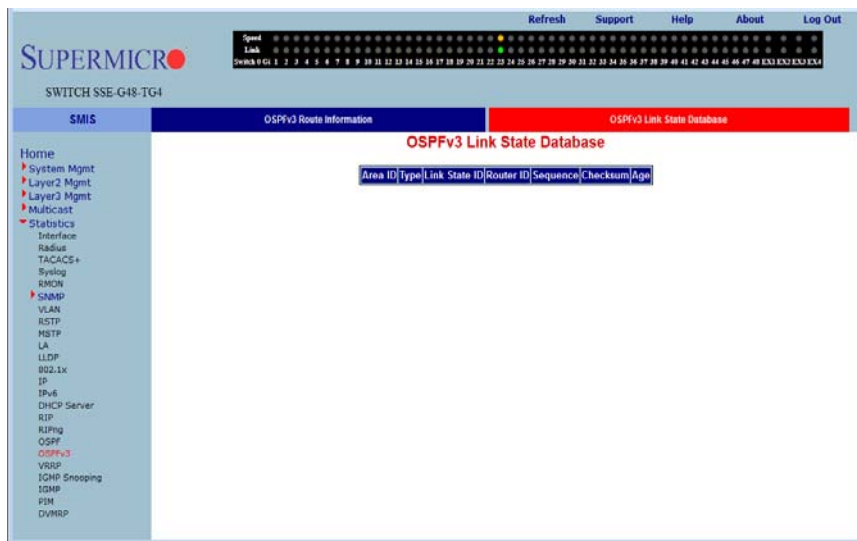
Clicking the OSPFv3 ROUTE INFORMATION tab brings up the OSPFv3 ROUTE INFORMATION page (Figure 5-203), which displays information about OSPFv3 routes. The parameters for this page are shown in Table 5-177.

Table 5-177. OSPFv3 Route Information Page Parameters

Parameter	Description
Destination Address	This parameter specifies the destination address.
Prefix	This parameter specifies the prefix.
Gateway	This parameter specifies the gateway.
Type	This parameter specifies the type.
Area ID	This parameter specifies the Area ID.
Cost	This parameter specifies the cost.
Interface	This parameter specifies the interface.

OSPFv3 Link State Database

Figure 5-204. OSPFv3 Link State Database Page



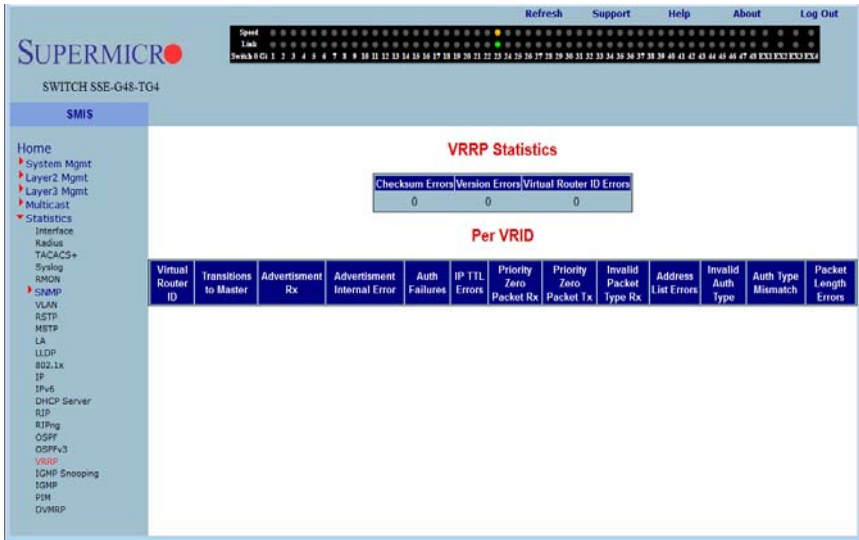
Clicking the OSPFv3 LINK STATE DATABASE tab brings up the OSPFv3 LINK STATE DATABASE page (Figure 5-204), which displays information about OSPF link state database. The parameters for this page are shown in Table 5-178.

Table 5-178. OSPFv3 Link State Database Page Parameters

Parameter	Description
Area ID	This parameter specifies the area identifier.
Type	This parameter specifies the link state type.
Link State ID	This parameter specifies the link state identifier.
Router ID	This parameter specifies the router identifier.
Sequence	This parameter specifies the sequence number of this link state information.
Checksum	This parameter specifies the checksum.
Age	This parameter specifies the link state information age in seconds.

VRRP

Figure 5-205. VRRP Statistics Page



Clicking the VRRP link brings up the VRRP STATISTICS page (Figure 5-205), which displays VRRP global statistics and VRRP router specific statistics. The parameters for this page are shown in Table 5-179.

Table 5-179. VRRP Statistics Page Parameters

Parameter	Description
VRRP Global Statistics	
Checksum Errors	This parameter specifies the number of checksum errors.
Version Errors	This parameter specifies the number of version errors.
Virtual Router ID Errors	This parameter specifies the number of Virtual Router ID errors.
VRRP Router Specific Statistics	
Virtual Router ID	This parameter specifies the Virtual Router identifier.
Transitions to Master	This parameter specifies the number of transitions as Master.
Advertisement Receive	This parameter specifies the number of advertisement packets received.
Advertisement Internal Error	This parameter specifies the number of advertisement errors happened.
Authentication Failures	This parameter specifies the number of authentication failures.
IP TTL Errors	This parameter specifies the number of IP TTL errors happened.

Table 5-179. VRRP Statistics Page Parameters (Continued)

Parameter	Description
Priority Zero Packet Received	This parameter specifies the number of priority zero packets received.
Priority Zero Packet Transmitted	This parameter specifies the number of priority zero packets transmitted.
Invalid Packet Type Received	This parameter specifies the number of invalid packets received.
Address List Errors	This parameter specifies the number of address list errors.
Invalid Authentication Type	This parameter specifies the number of invalid authentication types received.
Authentication Type Mismatch	This parameter specifies the number of authentication type mismatch received.
Packet Length Errors	This parameter specifies the number of VRRP packets received with invalid length.

Notes

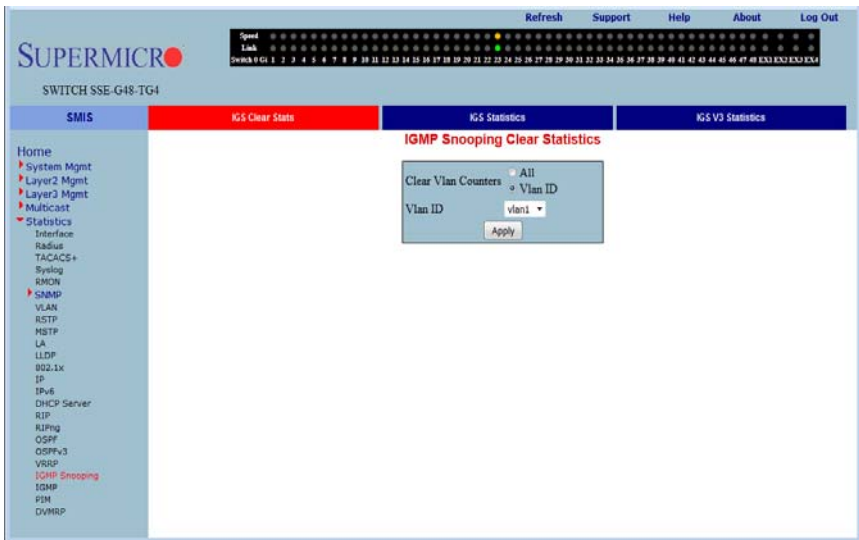
IGMP Snooping

The IGMP link allows you to view IGMP statistics through the following pages:

- [IGS Clear Stats](#)
- [IGS Statistics](#)
- [IGS V3 Statistics](#)

IGS Clear Stats

Figure 5-206. IGMP Snooping Clear Statistics Page



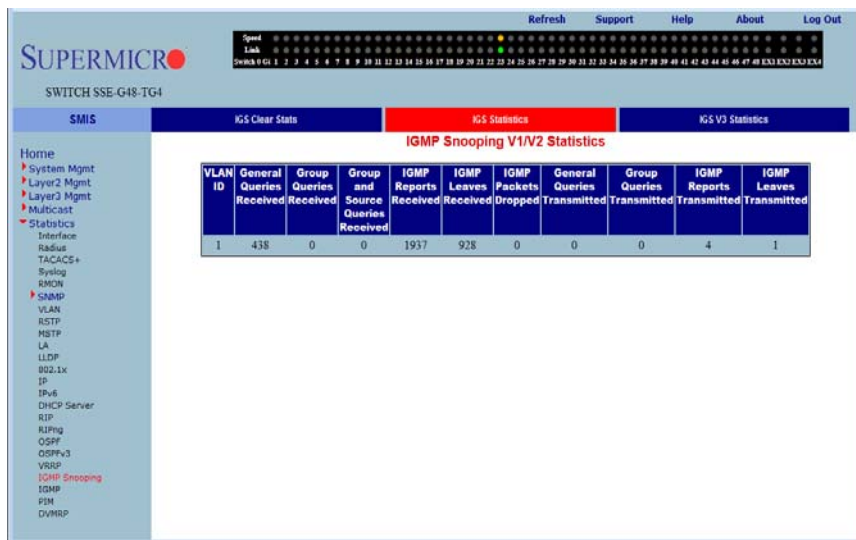
Clicking the IGS CLEAR STATS tab brings up the IGMP SNOOPING CLEAR STATISTICS page (Figure 5-206), which displays clearing IGMP snooping statistics. The parameters for this page are shown in Table 5-180.

Table 5-180. IGMP Snooping Clear Statistics Page Parameters

Parameter	Description
All	This parameter gives you the option to clear all the IGMP statistics.
Vlan ID	This parameter give you the option to clear IGMP statistics for a particular VLAN.

IGS Statistics

Figure 5-207. IGMP Snooping V1/V2 Statistics Page



Clicking the IGS STATISTICS tab brings up the IGMP SNOOPING V1/V2 STATISTICS page (Figure 5-207), which displays IGMP snooping statistics. The parameters for this page are shown in Table 5-181.

Table 5-181. IGMP Snooping V1/V2 Statistics Page Parameters

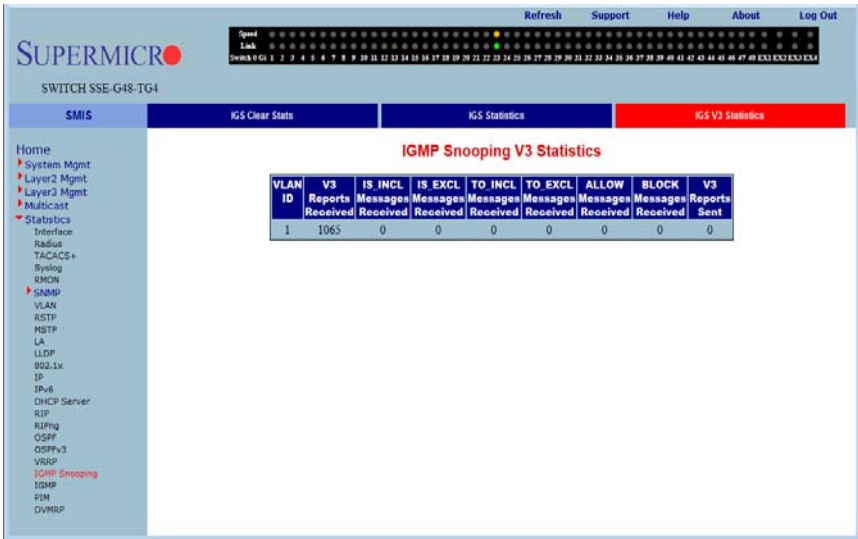
Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
General Queries Received	This parameter specifies the number of general query packets received.
Group Queries Received	This parameter specifies the number of group query packets received.
Group and Source Queries Received	This parameter specifies the number of group and source query packets received.
IGMP Reports Received	This parameter specifies the number of IGMP report packets received.
IGMP Leaves Received	This parameter specifies the number of IGMP leave packets received.
IGMP Packets Dropped	This parameter specifies the number of IGMP dackets dropped.
General Queries Transmitted	This parameter specifies the number of general query packets transmitted.

Table 5-181. IGMP Snooping V1/V2 Statistics Page Parameters (Continued)

Parameter	Description
Group Queries Transmitted	This parameter specifies the number of group query packets transmitted.
IGMP Reports Transmitted	This parameter specifies the number of IGMP report packets transmitted.
IGMP Leaves Transmitted	This parameter specifies the number of IGMP leave packets transmitted.

IGS V3 Statistics

Figure 5-208. IGMP Snooping V3 Statistics Page



Clicking the IGS V3 STATISTICS tab brings up the IGMP SNOOPING V3 STATISTICS page (Figure 5-208), which displays IGMP snooping V3 statistics information. The parameters for this page are shown in Table 5-182.

Table 5-182. IGMP Snooping V3 Statistics Page Parameters

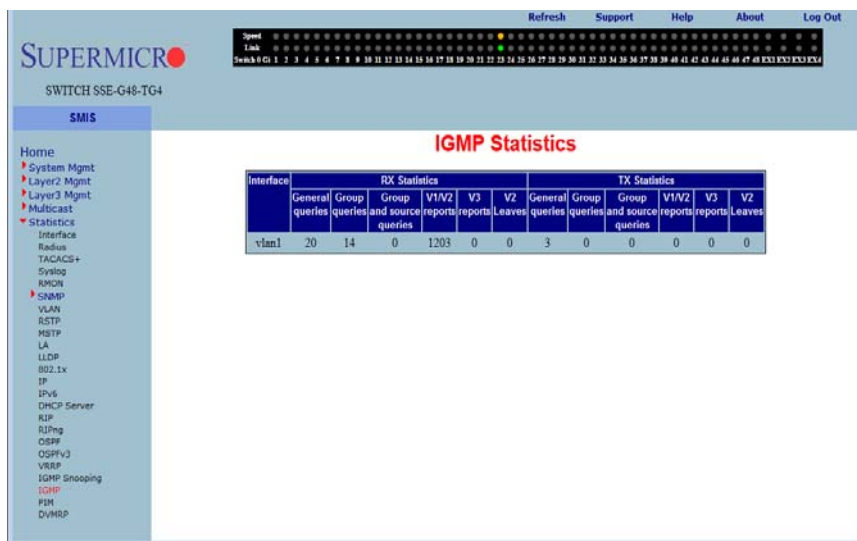
Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
V3 Reports Received	This parameter specifies the number of Reports messages received.
IS_INCL Messages Received	This parameter specifies the number of messages received with is include field.
IS_EXCL Messages Received	This parameter specifies the number of messages received with is exclude field.

Table 5-182. IGMP Snooping V3 Statistics Page Parameters (Continued)

Parameter	Description
TO_INCL Messages Received	This parameter specifies the number of messages received with to include field.
TO_EXCL Messages Received	This parameter specifies the number of messages received with to exclude field.
ALLOW Messages Received	This parameter specifies the number of allow messages received.
BLOCK Messages Received	This parameter specifies the number of block messages received.
V3 Reports Sent	This parameter specifies the number of V3 reports transmitted.

IGMP

Figure 5-209. IGMP Route StatisticsPage



Clicking the IGMP link brings up the IGMP ROUTE STATISTICS page (Figure 5-209), which displays IGMP route information. The parameters for this page are shown in Table 5-183.

Table 5-183. IGMP Route Statistics Page Parameters

Parameter	Description
Interface	This parameter specifies the interface identifier.
General Queries Received	This parameter specifies the number of general query packets received.

Table 5-183. IGMP Route Statistics Page Parameters (Continued)

Parameter	Description
Group Queries Received	This parameter specifies the number of group query packets received.
Group and Source Queries Received	This parameter specifies the number of group and source query packets received.
IGMP V1/V2 Reports Received	This parameter specifies the number of IGMP V1/V2 report packets received.
IGMP V3 Reports Received	This parameter specifies the number of IGMP V3 report packets received.
General Queries Transmitted	This parameter specifies the number of general query packets transmitted.
Group Queries Transmitted	This parameter specifies the number of group query packets transmitted.
Group and Source Queries Transmitted	This parameter specifies the number of group and source query packets transmitted.
IGMP V1/V2 Reports Transmitted	This parameter specifies the number of IGMP V1/V2 report packets transmitted.
IGMP V3 Reports Transmitted	This parameter specifies the number of IGMP V3 report packets transmitted.
IGMP V2 Leaves Transmitted	This parameter specifies the number of IGMP V2 leaves packets transmitted.

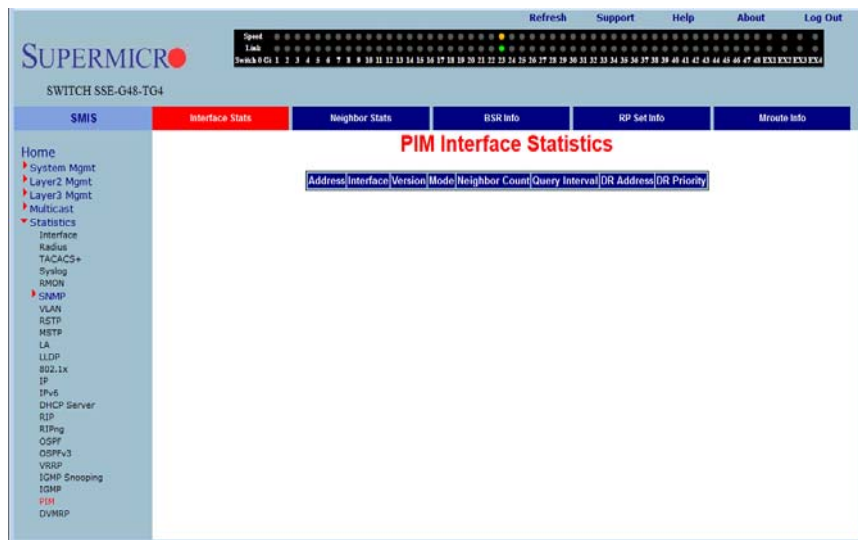
PIM

The PIM link allows you to view PIM statistics through the following pages:

- [Interface Stats](#)
- [Neighbor Stats](#)
- [BSR Info](#)
- [RP Set Info](#)
- [Mroute Info](#)

Interface Stats

Figure 5-210. PIM Interface Statistics Page



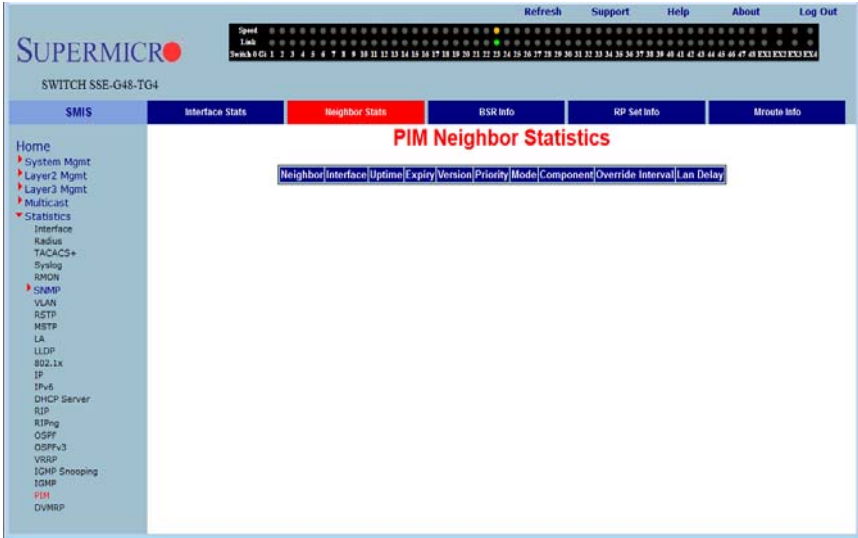
Clicking the INTERFACE STATS tab brings up the PIM INTERFACE STATISTICS page (Figure 5-210), which displays PIM interface statistics. The parameters for this page are shown in Table 5-184.

Table 5-184. PIM Interface Statistics Page Parameters

Parameter	Description
Address	This parameter specifies the address.
Interface	This parameter specifies the interface.
Version	This parameter specifies the version.
Mode	This parameter specifies the mode.
Neighbor Count	This parameter specifies the neighbor count.
Query Interval	This parameter specifies the query interval.
DR address	This parameter specifies the DR address.
DR Priority	This parameter specifies the DR priority.

Neighbor Stats

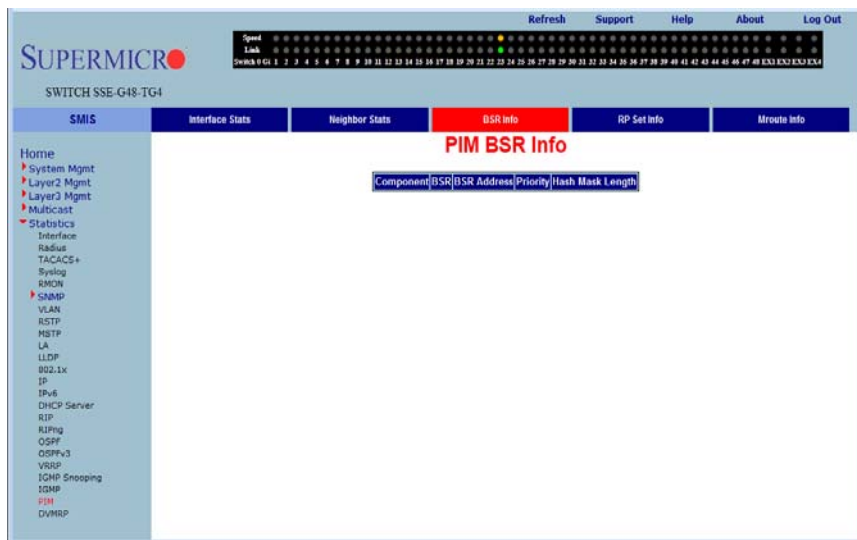
Figure 5-211. PIM Neighbor Statistics Page



Clicking the NEIGHBOR STATS tab brings up the PIM NEIGHBOR STATISTICS page (Figure 5-211), which displays PIM neighbor statistics. The parameters for this page are shown in Table 5-185.

Table 5-185. PIM Neighbor Statistics Page Parameters

Parameter	Description
Neighbor	This parameter specifies the neighbor.
Interface	This parameter specifies the interface.
Uptime	This parameter specifies the uptime.
Expiry	This parameter specifies the expiry.
Version	This parameter specifies the version.
Priority	This parameter specifies the priority.
Mode	This parameter specifies the mode.
Component	This parameter specifies the component.
Override Interval	This parameter specifies the override interval.
LAN Delay	This parameter specifies the LAN delay.

BSR Info**Figure 5-212. PIM BSR Info Page**

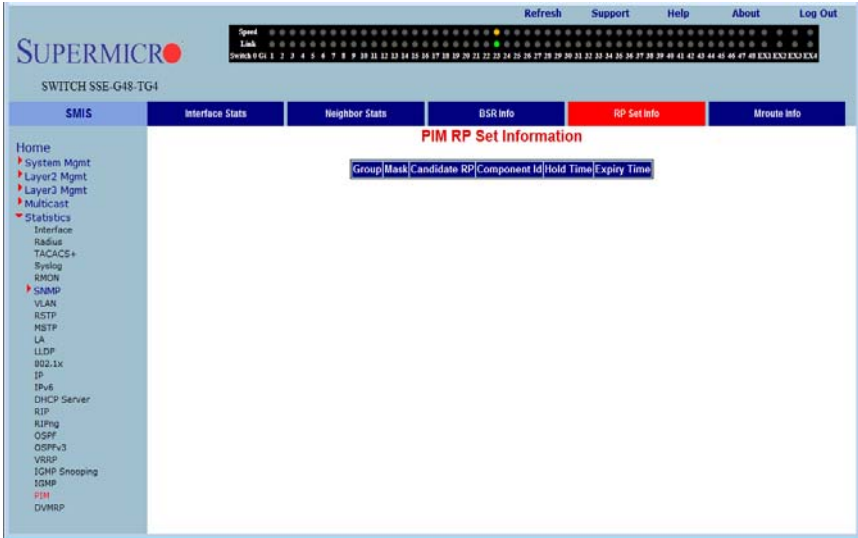
Clicking the BSR INFO tab brings up the PIM BSR INFO page (Figure 5-212). The parameters for this page are shown in Table 5-186.

Table 5-186. PIM BSR Info Page Parameters

Parameter	Description
Component	This parameter specifies the component.
BSR	This parameter specifies the BSR.
BSR Address	This parameter specifies the BSR address.
Priority	This parameter specifies the priority.
Hash Mask Length	This parameter specifies the Hash Mask Length.

RP Set Info

Figure 5-213. PIM RP Information Page



Clicking the RP SET INFO tab brings up the PIM RP INFORMATION page (Figure 5-213), which displays PIM RP information. The parameters for this page are shown in Table 5-187.

Table 5-187. PIM RP Information Page Parameters

Parameter	Description
Group	This parameter specifies the group address.
Mask	This parameter specifies the mask.
Candidate RP	This parameter specifies the candidate RP.
Hold Time	This parameter specifies the Hold time in seconds.
Expiry Time	This parameter specifies the expiry time in seconds.
Component	This parameter specifies the component identifier.

Mroute Info**Figure 5-214. PIM Route Information Page**

Clicking the MROUTE INFO tab brings up the PIM ROUTE INFORMATION page (Figure 5-214), which displays PIM route information. The parameters for this page are shown in Table 5-188.

Table 5-188. PIM Route Information Page Parameters

Parameter	Description
Component	This parameter specifies the PIM Component Identifier.
Source	This parameter specifies the source address.
Group	This parameter specifies the group address.
Up Time	This parameter specifies the up time in seconds.
Expiry Time	This parameter specifies the expiry time in seconds.
RP Address	This parameter specifies the RP Address.
Incoming Interface	This parameter specifies the Incoming Interface Name.
RPF Neighbor Addr	This parameter specifies the RPF Neighbor Address.
Route Flags	This parameter specifies the SPT Bit or Wild Card Bit or RPT Bit.
Name	This parameter specifies the Outgoing Interface Name
State	This parameter specifies the Outgoing Interface State.
Mode	This parameter specifies the Outgoing Interface Mode.

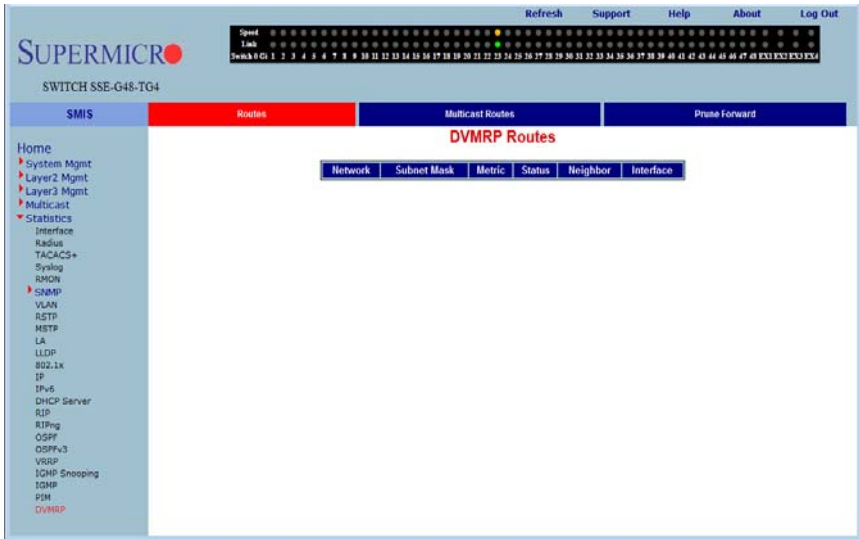
DVMRP

The DVMRP link allows you to view DVMRP statistics through the following pages:

- [Routes](#)
- [Multicast Routes](#)
- [Prune Forward](#)

Routes

Figure 5-215. DVMRP Routes Page



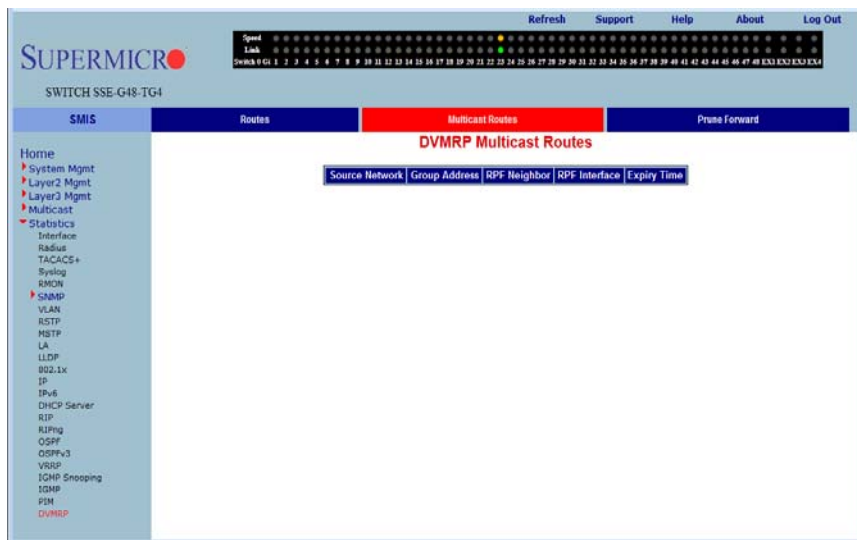
Clicking the ROUTES tab brings up the DVMRP ROUTES page (Figure 5-215), which displays DVMRP routes information. The parameters for this page are shown in Table 5-189.

Table 5-189. DVMRP Routes Page Parameters

Parameter	Description
Network	This parameter specifies the network address for this route.
Subnet Mask	This parameter specifies the network mask for this route.
Metric	This parameter specifies the metric value for this route.
Status	This parameter specifies the status of this route.
Neighbor	This parameter specifies the neighbor address for this route.
Interface	This parameter specifies the interface identifier.

Multicast Routes

Figure 5-216. DVMRP Multicast Routes Page



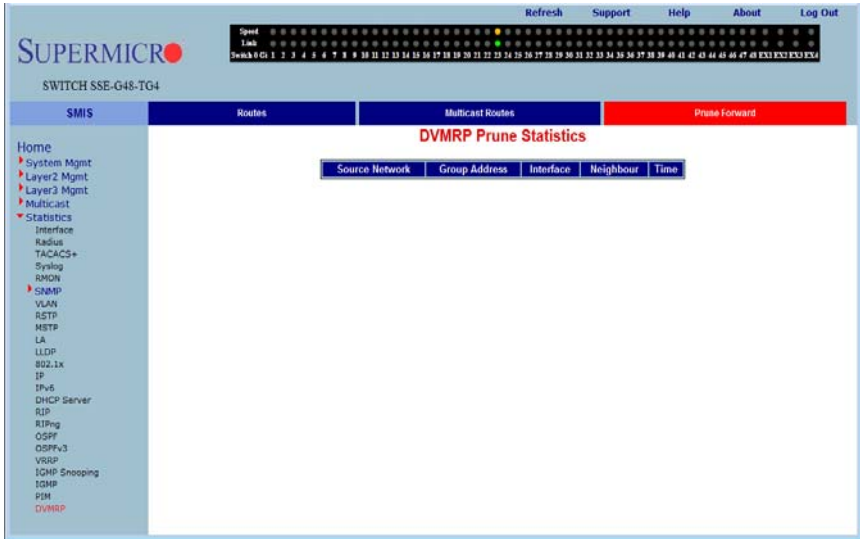
Clicking the MULTICAST ROUTES tab brings up the DVMRP MULTICAST ROUTES page (Figure 5-216), which displays DVMRP multicast routes information. The parameters for this page are shown in Table 5-190.

Table 5-190. DVMRP Multicast Routes Page Parameters

Parameter	Description
Source Network	This parameter specifies the source network.
Group Address	This parameter specifies the group address.
RPF Neighbor	This parameter specifies the RPF neighbor.
RPF Interface	This parameter specifies the RPF interface.
Expiry Time	This parameter specifies the expiry time in seconds.

Prune Forward

Figure 5-217. DVMRP Prune Statistics Page



Clicking the PRUNE FORWARD tab brings up the DVMRP PRUNE STATISTICS page (Figure 5-217), which DVMRP prune statistics information. The parameters for this page are shown in Table 5-191.

Table 5-191. DVMRP Prune Statistics Page Parameters

Parameter	Description
Source Network Address	This parameter specifies the source network address.
Group Address	This parameter specifies the group address.
Interface Identifier.	This parameter specifies the interface identifier.
Neighbor Address	This parameter specifies the neighbor address.
Time	This parameter specifies the time in seconds.

Appendix A

Rack Installation

A-1 Overview

Some Supermicro switches can be equipped with an optional rail kit (CSE-PT52L) to make it easy to install them in a rack. This manual provides instructions for installing the CSE-PT52L mounting rails onto a rack and for installing the switch into the mounting rails. Following these steps in the order given should enable you to have the system operational within a minimum amount of time.

A-2 Unpacking the System

You should inspect the box the switch was shipped in and note if it was damaged in any way. If the switch itself shows damage you should file a damage claim with the carrier who delivered it.

Decide on a suitable location for the rack unit that will hold your switch. It should be situated in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated. You will also need it placed near a grounded power outlet. Be sure to read the Rack, General and Lithium Battery Precautions in the next section.

A-3 Preparing for Setup

The optional rail kit (CSE-PT52L) ships in a separate box and that box should include two sets of rail assemblies, two rail mounting brackets and the mounting screws needed to install the system into the rack. Read this section in its entirety before you begin the installation procedure outlined in the sections that follow.

Choosing a Setup Location

- Leave enough clearance in front of the rack to enable you to open the front door completely (~25 inches).
- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.
- This product is for installation only in a Restricted Access Location (dedicated equipment rooms, service closets and similar environments).

A-4 Warnings and Precautions!

Rack Precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In a single rack installation, stabilizers should be attached to the rack.
- In multiple rack installations, the racks should be coupled together.
- Always make sure the rack is stable before extending a component from the rack.
- You should extend only one component at a time - extending two or more simultaneously may cause the rack to become unstable.

General Precautions

- Review the electrical and general safety precautions that came with the components you are adding to your switch (if any).
- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the servers and switches from power surges, voltage spikes and to keep your system operating in case of a power failure.
- Always keep the rack's front door and all panels and components closed when not servicing to maintain proper cooling.
- Do not remove the cover of the switch, there are no user-serviceable components inside. Take unit to service center for repairs and servicing.
- Disconnect all power cords before servicing.

WARNING: Slide/rail mounted equipment is not to be used as a shelf or work space.

Lithium Battery Precaution

This switch may contain a lithium battery. There is a danger of explosion if the battery is incorrectly replaced.

- Installing the battery upside-down may reverse the polarities and cause the battery to explode.
- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.
- Do not damage the battery in any way, a damaged battery may release hazardous materials into the environment.
- Do not discard a used battery in the garbage or a public landfill.
- Please comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

Rack Mounting Considerations

Ambient Operating Temperature

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (T_{mra}).

Reduced Airflow

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Mechanical Loading

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Ground

A reliable ground (earth) must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

A-5 Rack Mounting Instructions

This chapter provides information on installing the switch into a rack unit with the CSE-PT52L rail kit. There are a variety of rack units on the market, which may mean the assembly procedure will differ slightly. You should also refer to the installation instructions that came with the rack unit you are using.

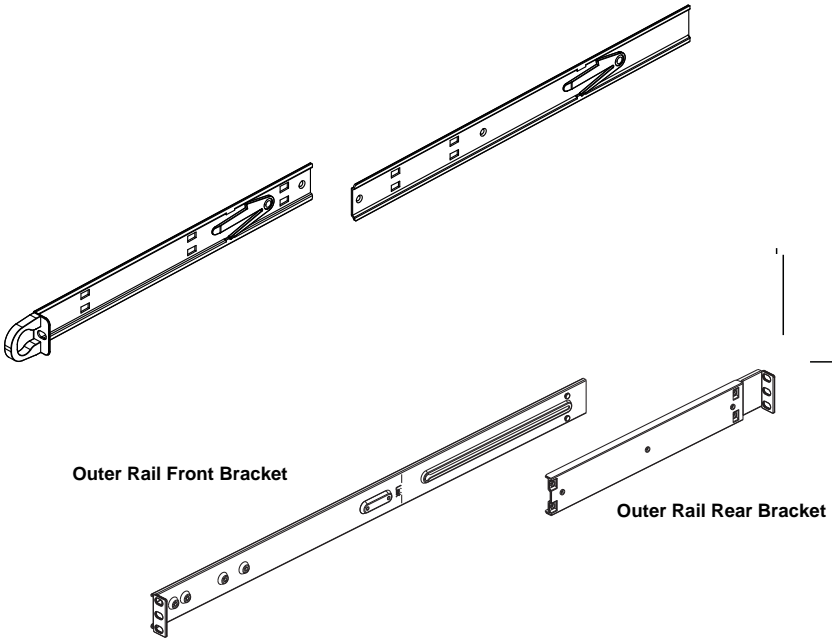
NOTE: This rail will fit a rack between 26" and 33.5" deep.

NOTE: Your switch may differ from the illustrations in this manual.

Identifying the Sections of the Rack Rails

The CSE-PT52L rail kit package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: a fixed inner rail that secures directly to the side of the switch, and a fixed outer rail that secures directly to the rack itself. See [Figure A-1](#) below for details.

Figure A-1. Identifying the Sections of the Rack Rails



Separating the Sections of the Rails

The CSE-PT52L rail kit ships with the front inner rail attached to the front outer rail. These must be separated prior to installation in the rack. Use the procedure below to separate the rails.

Separating the Rails

1. Separate the inner rail from the outer rail by depressing the black plastic flange inside the inner rail. This will release the outer rail.
2. Slide the inner rail forward and out of the outer rail.
3. The CSE-PT52L rail kit also includes a set of inner rail extensions. Only the inner rails are required and you may discard the inner rail extensions.

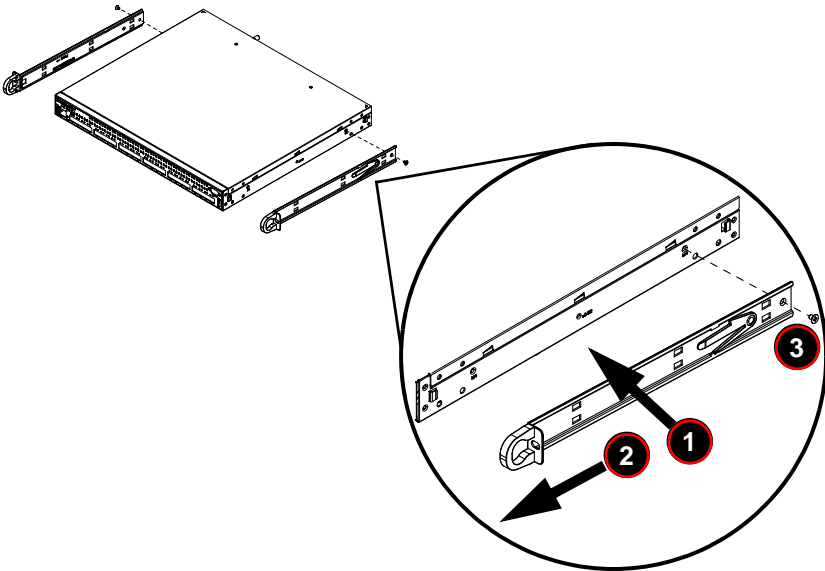
Installing the Inner Rails

Use the procedure below and [Figure A-2](#) to install the inner rails.

Installing the Inner Rails on the Switch

1. Place one of the inner rails on one side of the switch aligning the hook on the side of the switch with the mounting hole in the rail. Make sure the inner rail faces outward, as illustrated below.
2. Slide the inner rail forward so that the rail fits securely into the hook on the side of the switch.
3. Secure the inner rail to the switch with one screw as illustrated below.
4. Repeat steps 1-2 for the remaining inner rail.

Figure A-2. Installing the Inner Rail



Installing the Outer Rails

Use the procedure, [Figure A-3](#) and [Figure A-4](#) below to assemble and install the outer rails on the rack.

Installing the Outer Rails on the Rack

1. Attach the shorter outer rail to the outside of the longer outer rail. You must align the pins with the slides. Also, both bracket ends must face the same direction.
2. Adjust both the shorter and longer brackets to the proper length so that the rail fits snugly into the rack.
3. Secure the long bracket to the front side of the rack with two M5 screws and the short bracket to the rear side of the rack with three M5 screws.

4. Repeat steps 1-4 for the remaining outer rail.

Figure A-3. Assembling the Outer Rails

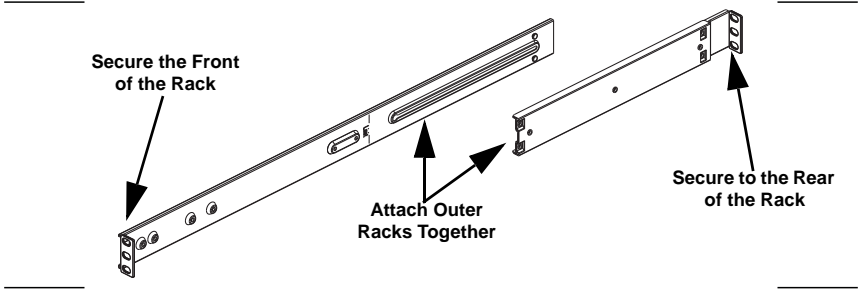
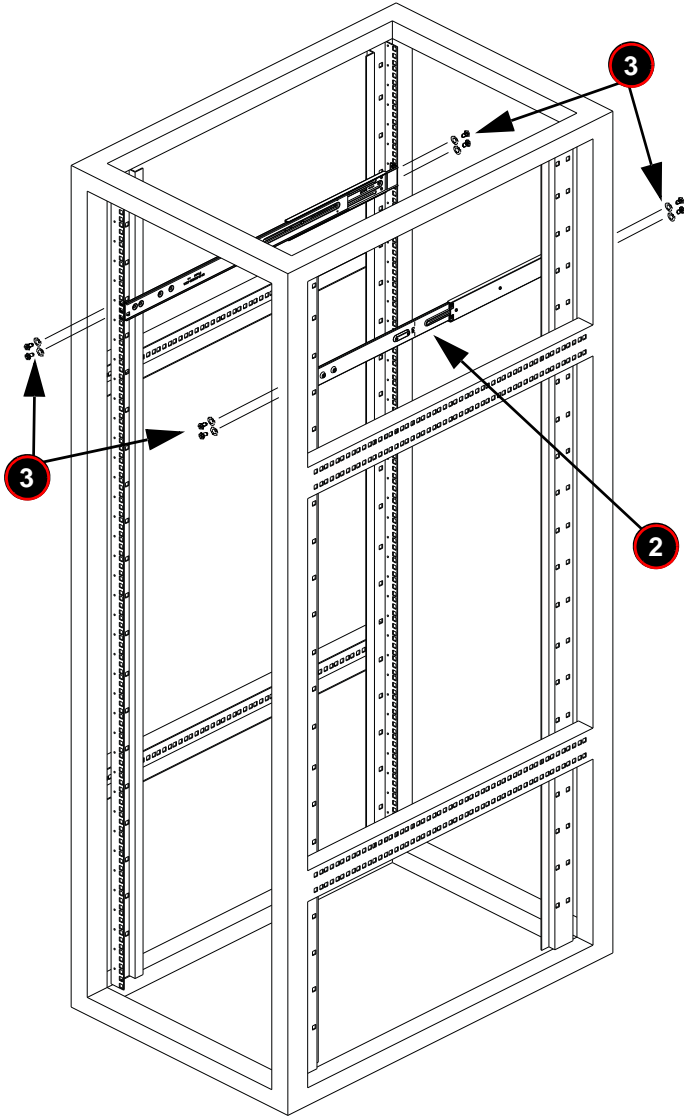


Figure A-4. Installing the Outer Rails onto the Rack



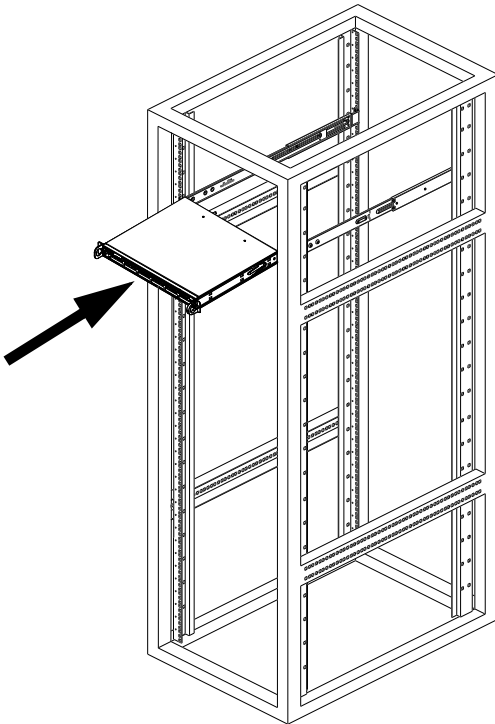
Installing the Switch into a Rack

Use the procedure and [Figure A-5](#) below to install the switch into a rack.

Installing the Switch

1. Confirm that inner rails have been secured to the switch.
2. Confirm that the outer rails are installed on the rack.
3. Align the ends of the inner rails on the switch with the front of the outer rails on the rack.
4. Slide the inner rails into the outer rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). When the switch has been pushed completely into the rack, you should hear the locking tabs click into the locked position.
5. (Optional) Insert and tighten the thumb screws which secure the front of the switch to the rack.

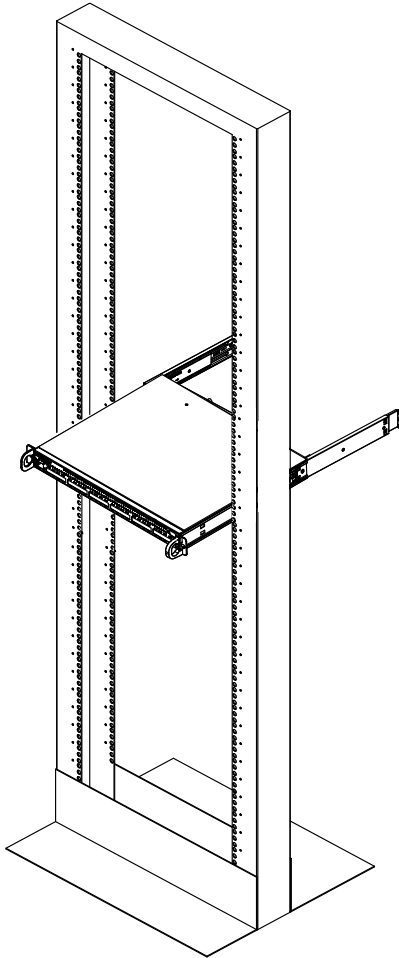
Figure A-5. Installing the Switch into a Rack



Installing the Switch into a Telco Rack

To install the switch into a Telco (post style) rack, use two L-shaped brackets on either side of the switch (four total). First, determine how far the switch will extend out the front of the rack. Larger switches should be positioned to balance the weight between front and back. Attach the two front brackets to each side of the switch, then position the two rear brackets with just enough space to accommodate the width of the telco rack. Finish by sliding the switch into the rack and tightening the brackets to the rack. See [Figure A-6](#) for details.

Figure A-6. Installing the Switch into a Telco Rack



Notes

Disclaimer

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.
