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
10-Gigabit Ethernet Switch

User's Manual

Revison 1.1

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, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

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 for further details.

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.

Manual Revison 1.1

Release Date: February 7, 2012

Table of Contents

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 switch 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 six switch products:

- SSE-G48-TG4
- SSE-G24-TG4
- SSE-X24S/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). This Ethernet switch also has 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. They contain two redundant hot-swappable power supplies installed at the factory. The SSE-X24S has a “normal” airflow direction for cooling – from the front of the unit to the back. The SSE-X24SR has a “reverse” airflow direction for cooling – from the back of the unit to the front. The two models are otherwise identical. The SSE-X24SR 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 or XFP 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

NOTE: The mounting ears can secure the 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:

- 1U form factor
- Dimensions: 440 x 387 x 44 mm (17.32 x 15.24 x 1.73 inch) (W x D x H)
- Weight: 5.6 kg (12.4 lbs) SSE-G24-TG4, 6.2 kg (13.7 lbs) SSE-G48-TG4, 8.18 kg (18.1 lbs) SSE-X24S/R
- 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 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.
	4F, No. 232-1, Liancheng Rd.
	Chung-Ho 235, Taipei County
	Taiwan, R.O.C.
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3991
Web Site:	www.supermicro.com.tw
Technical Support:	
Email:	support@supermicro.com.tw
Tel:	+886-2-8228-1366, ext. 132 or 139

Notes

Chapter 2
System Safety

This chapter provides system safety procedures for use with Layer 2/3 1/10 and 10-Gigabit Ethernet switches. Please read and understand this information before installing and using them.

2-1 Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the switch from damage:

- Be aware of how to power on/off the switch as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.
- Do not work alone when working with high voltage components.
- Power should always be disconnected from the switch when removing or installing it in a rack.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.

2-2 General Safety Precautions

Follow these rules to ensure general safety:

- Keep the area around the switch and rack components clean and free of clutter.
- Place the switch and any rack components that have been removed away from the rack or on a table so that they won't accidentally be stepped on.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.

2-3 Electrostatic Discharge Precautions

Electrostatic discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards.

The following measures are generally sufficient to neutralize this difference **before** contact is made to protect your equipment from ESD:

- Use a grounded wrist strap designed to prevent static discharge.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only; do not touch its components, peripheral chips, memory modules or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the mainboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure the blade enclosure provides excellent conductivity between the power supplies, the blade modules and the mainboard.

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).

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 steps in 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.

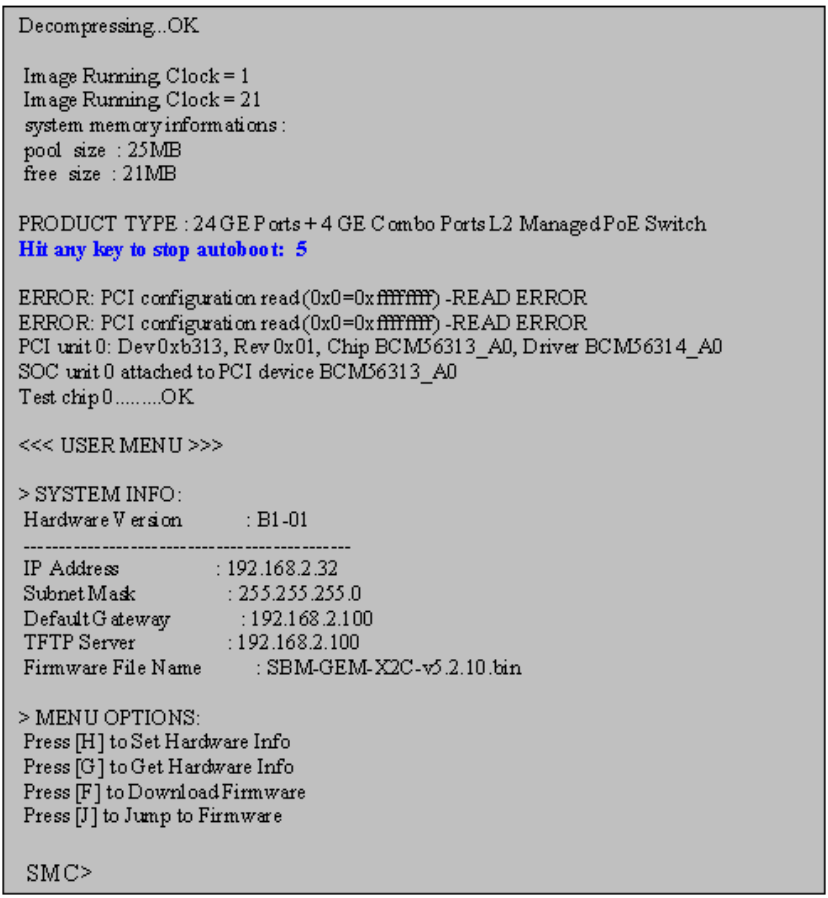
Booting using a Fallback Firmware Image

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
```

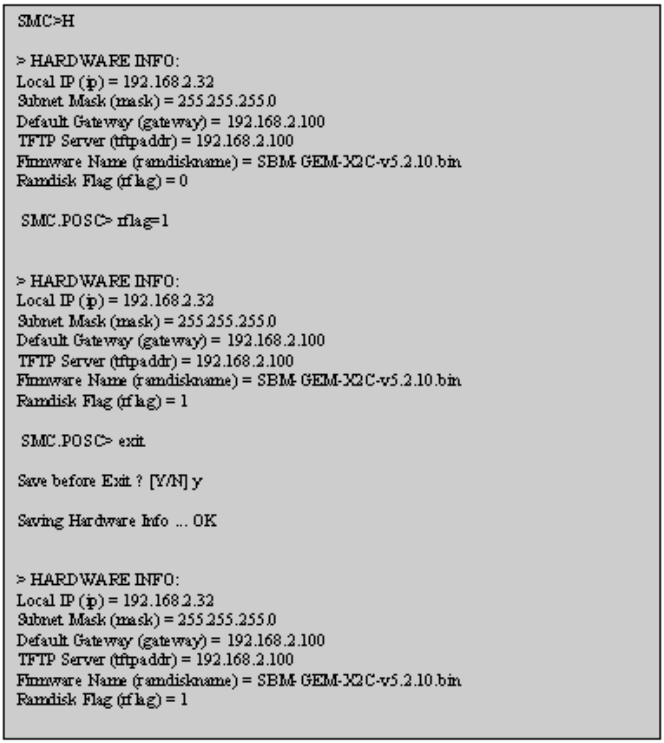
Figure 3-1. Displayed Text for Rebooting



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



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:fallbackl

   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.

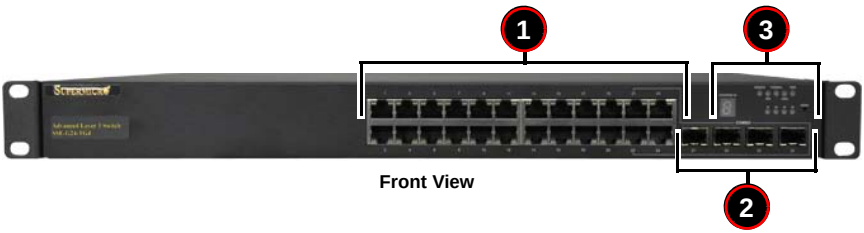
Notes

Chapter 4
Ports and Indicators

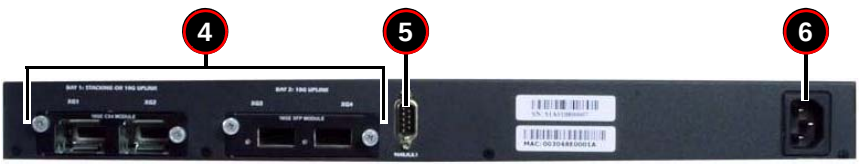
This chapter covers the ports and LED indicators found on Layer 2/3 1/10 and 10-Gigabit Ethernet switches.

4-1 SSE-G24-TG4 Ports and Indicators

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



Front View



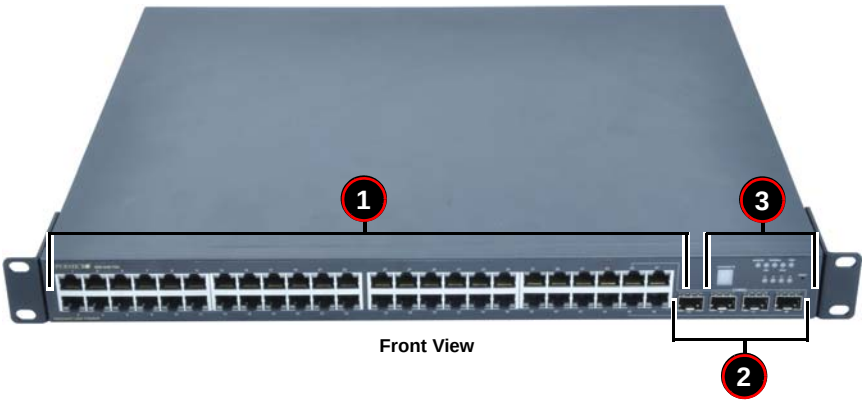
Rear View

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

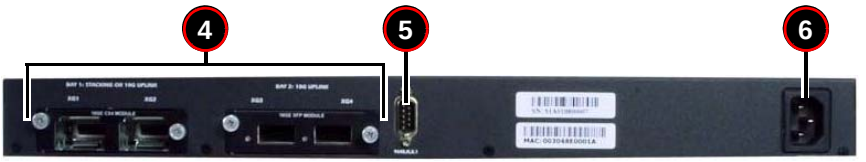
Item	Description
1	RJ45 10/100/1000 Ethernet ports (24)
2	SFP Combo Ports (4)
3	LEDs and Stacking Indicator ID
4	10-Gb/s Port Module Bays (2 bays for up to 4 ports for CX-4 or XFP)
5	Serial Port
6	Power Port

4-2 SSE-G48-TG4 Ports and Indicators

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



Front View



Rear View

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

4-3 SSE-X24S/R Ports and Indicators

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

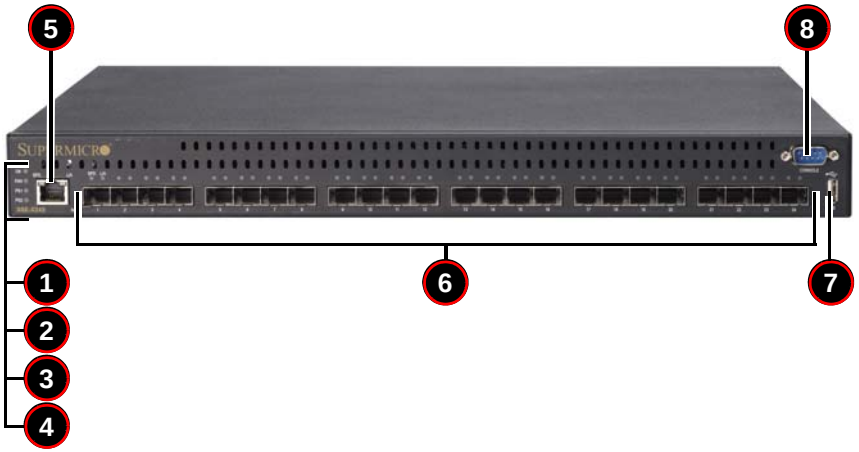


Table 4-3. SSE-X24S/R Switch Module Ports and Indicators

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

4-4 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.

10-Gb/s Port Module Bays

Figure 4-4. 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 4-4). 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.
- **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.

4-5 Indicators

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

Table 4-4. 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://192.168.1.1 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 switches you can connect to the 1G Ethernet RJ45 port, or the serial console port (on the front of the unit) to manage the switch.

5-2 Login

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 and SSE-X24S/R switches from Supermicro share a common management interface (including the associated feature set) with Supermicro's SBM-GEM-X2C Layer 2/3 1/10G Ethernet switch 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 and SSE-X24S/R switch.

Figure 5-2. Home Page

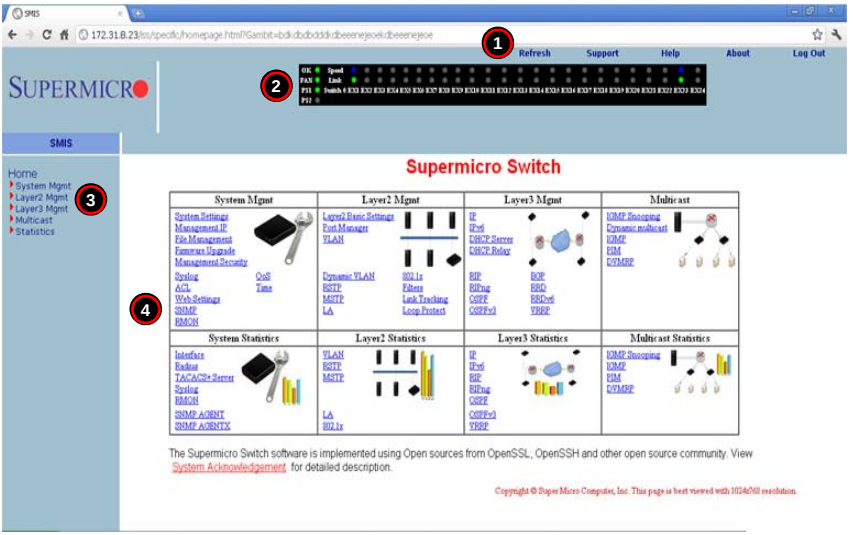


Table 5-1. Home Page Controls and Components

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.

Table 5-1. Home Page Controls and Components

Number	Name	Description
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 Supermico's 10-Gb/s switches.

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

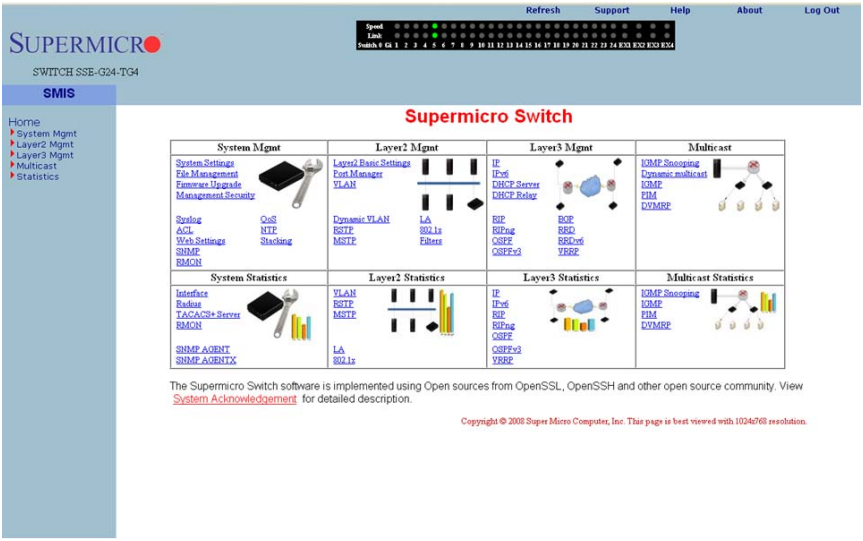


Figure 5-4. SSE-G48-TG4 Home Page

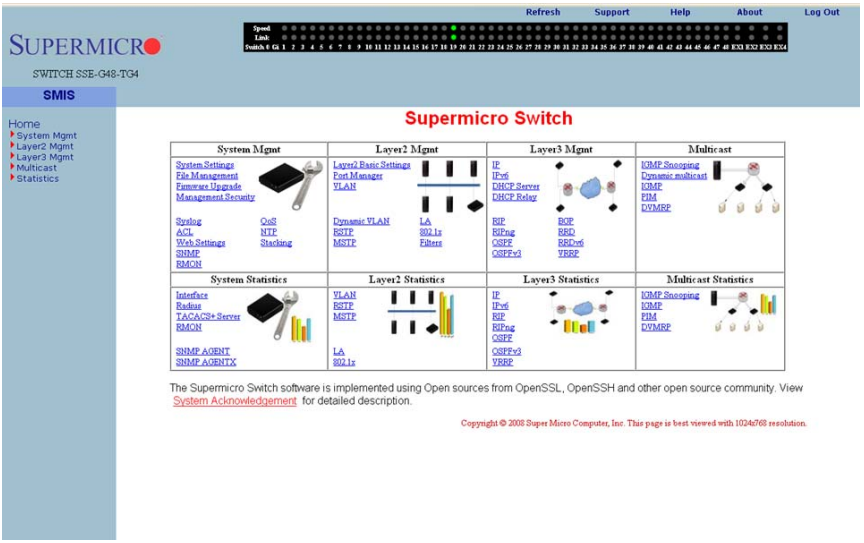
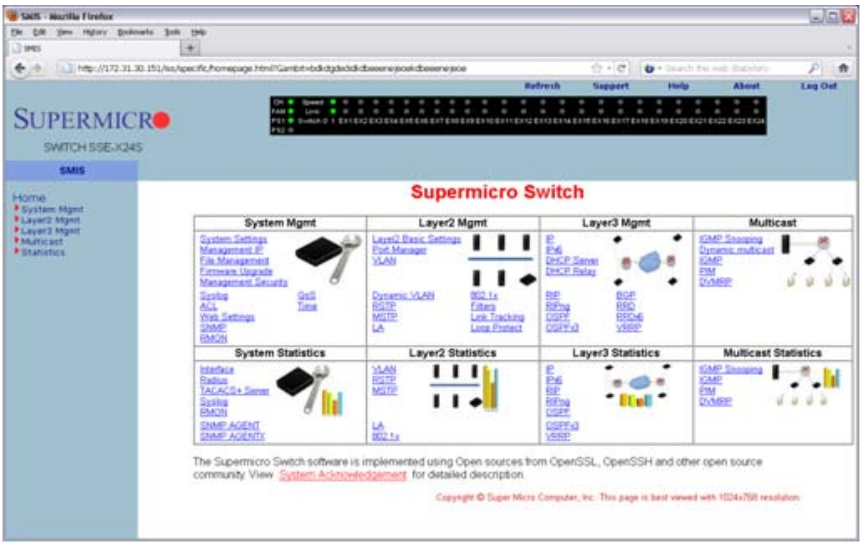


Figure 5-5. SSE-X24S/R Home Page



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 the SSE-G24-TG4 and SSE-G48-TG4 switches, this display displays 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 switch, it displays twenty-four 10-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 switch.

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.

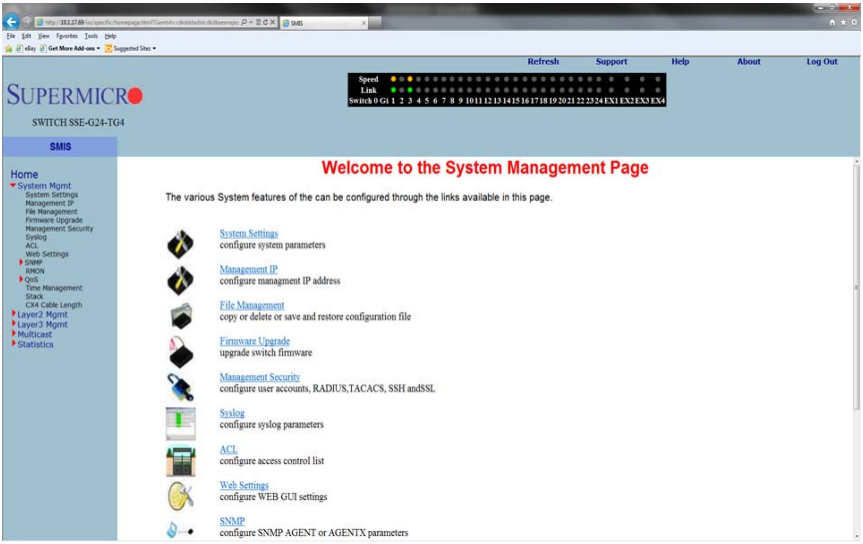
This tree is displayed on the left navigation pane on all configuration pages. This makes it easier for you to choose any configuration page directly without going back to the home page every time. To go to one of a MANAGEMENT page's sub-pages, click on the ▶ symbol to expand the list.

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 5-6. System Management Page



The SYSTEM MANAGEMENT page (Figure 5-6) 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

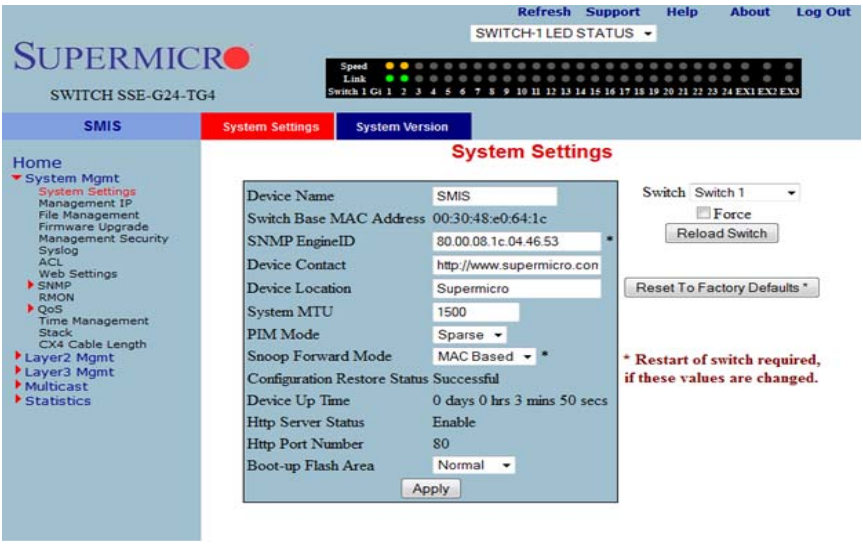
System Settings

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

- System Settings
- System Version

System Settings

Figure 5-7. System Settings Page



Clicking the SYSTEM INFORMATION tab brings up the SYSTEM SETTINGS page (Figure 5-7). 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	Displays the MAC Address 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 "Normal" (primary boot up image) or "Fallback"(secondary boot up image). The factory default is "Normal".

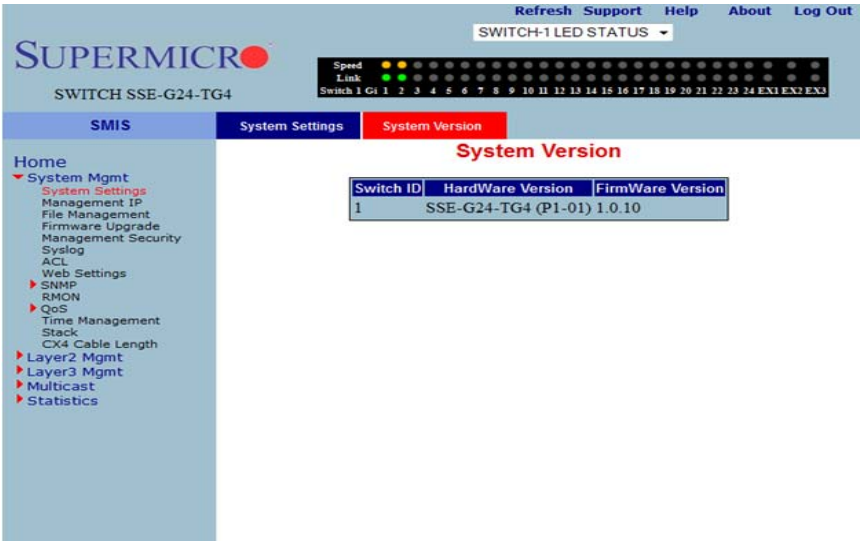
This page also has a control to **Reset To Factory Defaults**. This clears all switch configuration and local user accounts information. This reset requires reboot of the switch.

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

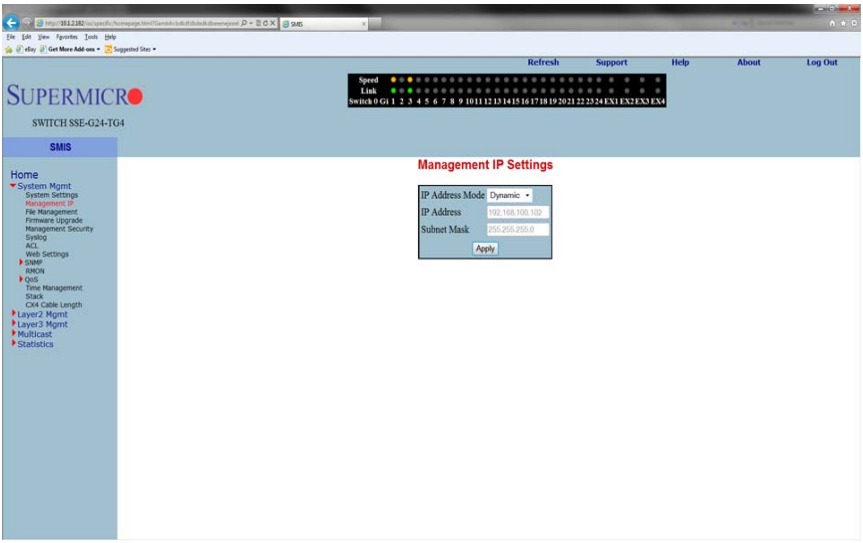
Figure 5-8. System Version Page



Clicking the SYSTEM VERSION tab brings up the SYSTEM VERSION page (Figure 5-8). 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 5-9. Management IP Page



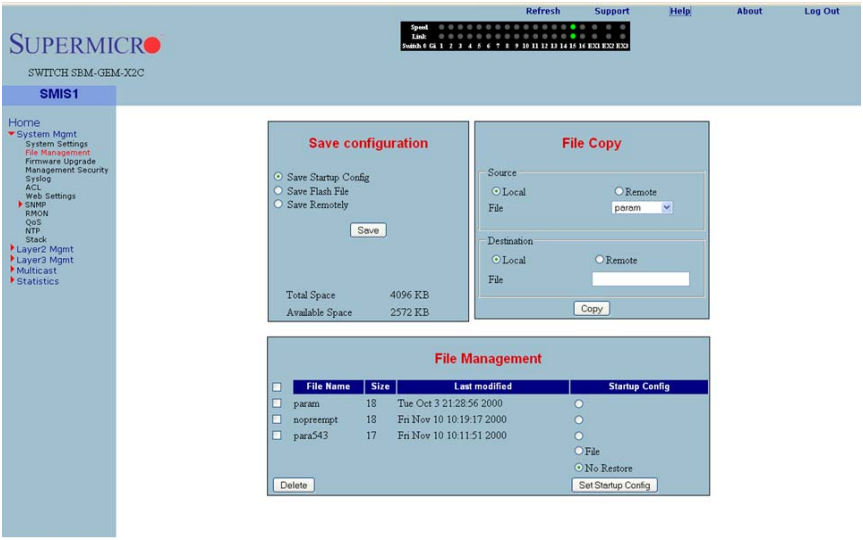
Clicking the MANAGEMENT IP tab brings up the MANAGEMENT IP page (Figure 5-9). This page helps you to manage the IP address for the switch. This page allows to configure the following settings:

- IP Address Mode
- IP Address
- Subnet Mask

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 5-10. File Management Page



Clicking the FILE MANAGEMENT link brings up the FILE MANAGEMENT page (Figure 5-10). 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 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.

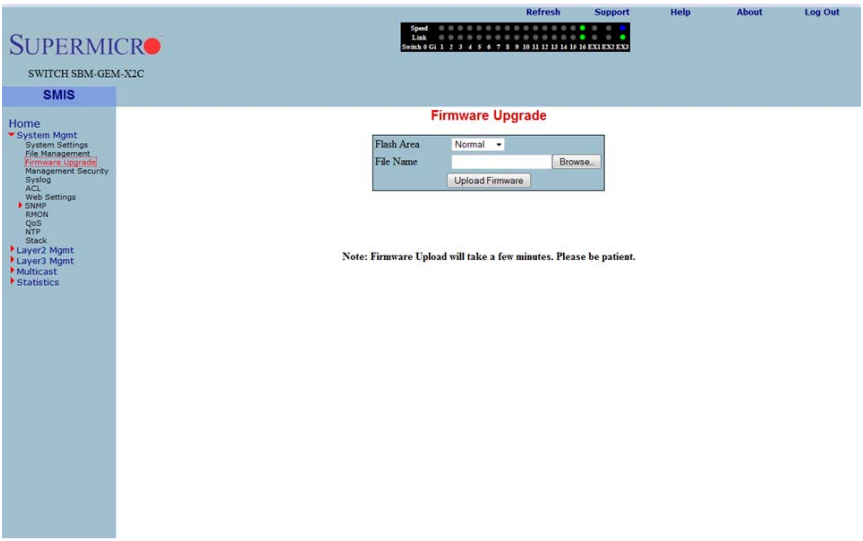
File Management

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.
- You can also choose the NO RESTORE option for not loading any configuration files on the next reboot of the switch.

Firmware Upgrade

Figure 5-11. Firmware Upgrade Page



Clicking the FIRMWARE UPGRADE link brings up the FIRMWARE UPGRADE page (Figure 5-11). This page allows you to upgrade the firmware in normal or fallback memory. In stacking, the firmware is upgraded in all stack members automatically.

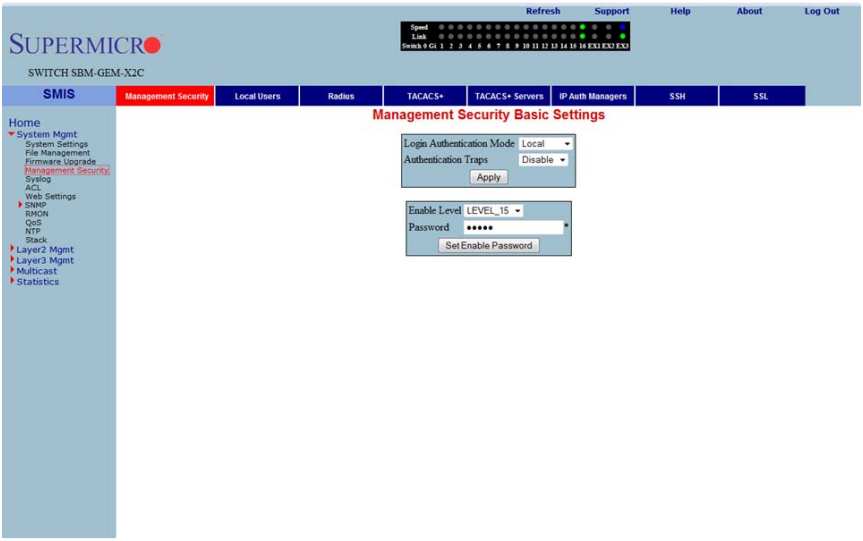
Management Security

The MANAGEMENT SECURITY link provides configuration for the following features:

- Management Security Basic Settings
- Management User Account
- Radius
- TACACS+ Global Settings
- TACACS+ Server Configuration
- IP Authorized Manager
- SSH Configuration
- SSLConfiguration

Management Security Basic Settings

Figure 5-12. Management Security Basic Settings Page



Clicking the MANAGEMENT SECURITY tab brings up the MANAGEMENT SECURITY BASIC SETTINGS page (Figure 5-12). This page allows you to setup the below listed basic security parameters (Table 5-3).

Table 5-3. Management Security Basic Settings Page Parameters

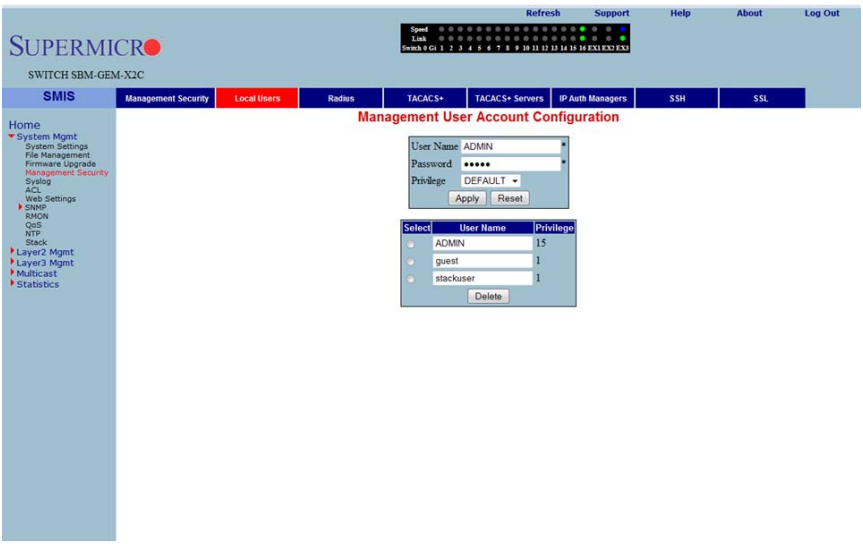
Parameter	Description
Authentication mode	The authentication modes supported are LOCAL, RADIUS and TACACS. The default option is "Local" mode where the user name and password is authenticated using a local user data base. In RADIUS mode, the authentication request is sent to the configured RADIUS servers. 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.

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.

Management User Account

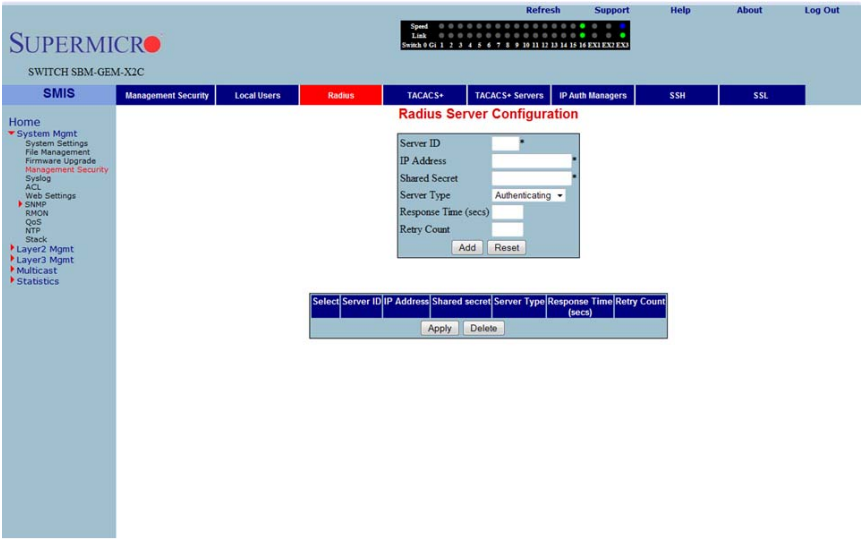
Figure 5-13. Management User Account Page



Clicking the LOCAL USERS tab brings up the MANAGEMENT USER ACCOUNT CONFIGURATION page (Figure 5-13). 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.

Radius

Figure 5-14. Radius Server Configuration Page



Clicking the RADIUS tab brings up the RADIUS SERVER CONFIGURATION page (Figure 5-14). This page allows you to configure the RADIUS server parameters as shown in Table 5-4.

Table 5-4. RADIUS Server Configuration Page Parameters

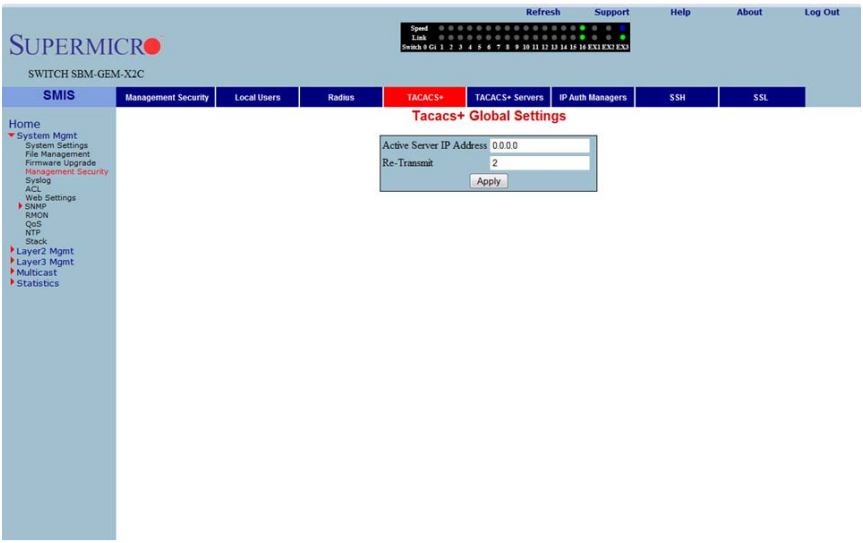
Parameter	Description
Server ID	This parameter specifies the unique identifier of the RADIUS Server Entry using a 2-characters input limit. The factory default is blank.
IP Address	This parameter specifies the IP Address of the RADIUS Server. The factory default is blank.
Shared Secret	This parameter 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: • 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

Table 5-4. RADIUS Server Configuration Page Parameters

Parameter	Description
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+ Global Settings

Figure 5-15. TACACS+ Global Settings Page



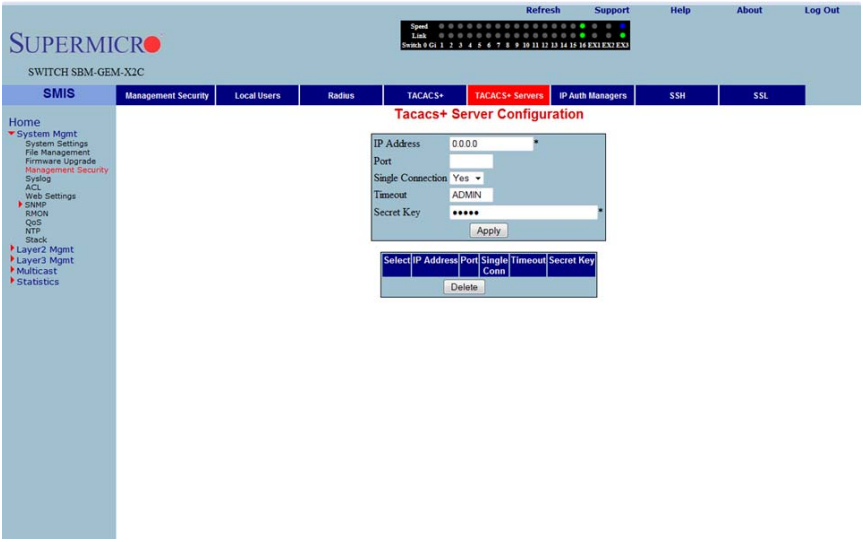
The TACACS+ GLOBAL SETTINGS page (Figure 5-15) allows you to configure TACACS retries and choose an active TACACS server. The parameters for this page are shown in Table 5-5.

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 following TACACS+ SERVER CONFIGURATION page (Figure 5-16). 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+ Server Configuration

Figure 5-16. TACACS+ Server Configuration Page



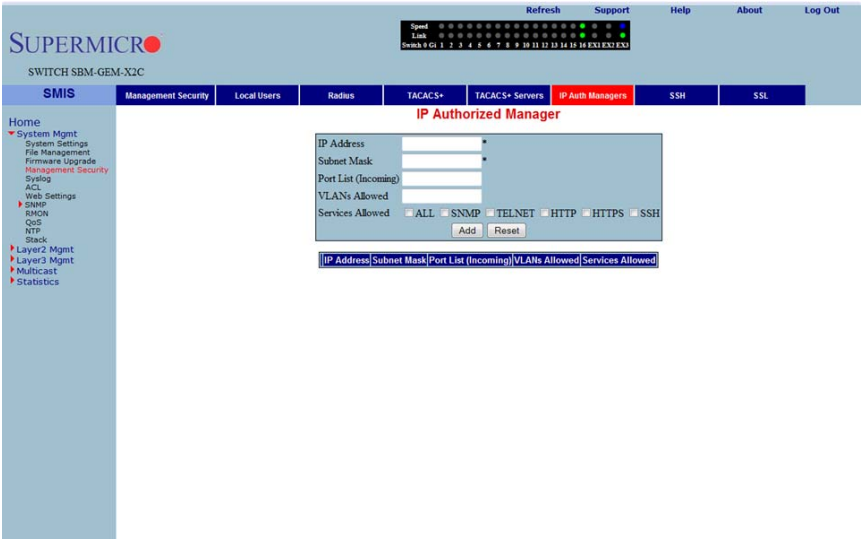
Clicking the TACACS+ SERVERS tab brings up the TACACS+ SERVER CONFIGURATION page (Figure 5-16), which allows you to configure TACACS servers. The parameters for this page are shown in Table 5-6.

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**.
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**..
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 Authorized Manager

Figure 5-17. IP Authorized Manager Page



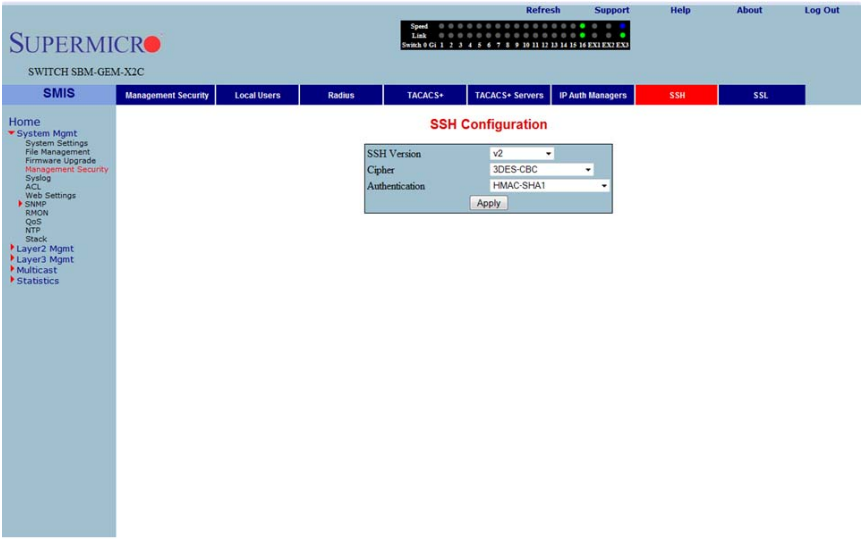
Clicking the IP AUTH MANAGER tab brings up the IP AUTHORIZED MANAGER page (Figure 5-17), which allows you to configure allowed management nodes for managing the switch. The parameters for this page are shown in Table 5-7.

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.
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 seperated 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 Configuration

Figure 5-18. SSH Configuration



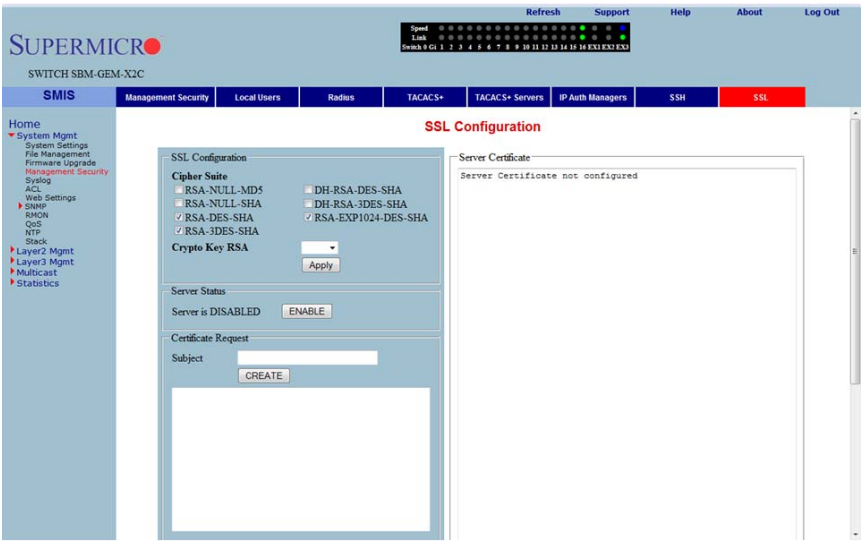
Clicking the SSH (Secure Shell) tab brings up the SSH CONFIGURATION page (Figure 5-18), which allows you to configure SSH version and keys. The parameters for this page are shown in Table 5-8.

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

SSLConfiguration

Figure 5-19. SSL Configuraiton Page



Clicking the SSL (Secure Socket Layers) tab brings up the SSL CONFIGURATION page (Figure 5-19), 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
```

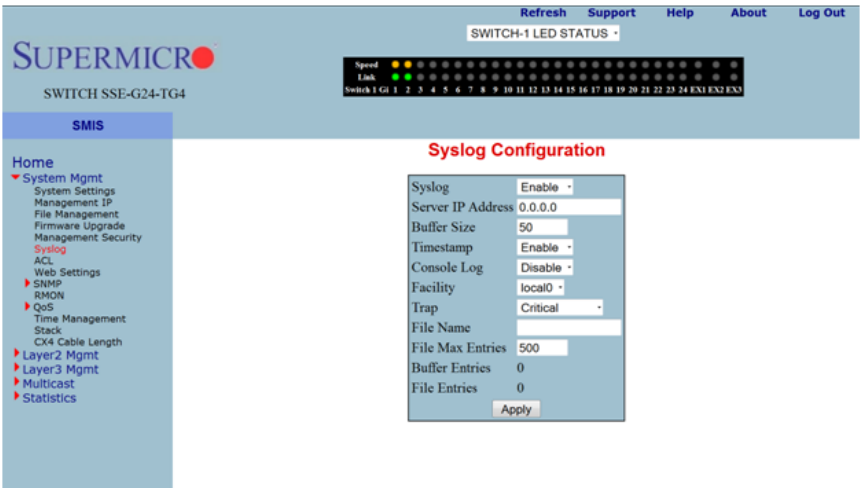
The above steps will generate the certificate file **cert.pem**.

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 5-20. Syslog Configuration Page



Clicking the LOGGING tab brings up the SYSLOG CONFIGURATION page (Figure 5-20), 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 specfied in log entries. Max entries buffered is **200**.
Timestamp	This parameter allows you to enable or disable the adding of a timestamp to the log messages.
Console Log	This parameter allows you to enable or disable logging to the console.
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, CRITICIAL, DEBUGGING, EMERGENCIES, ERROR, INFORMATIONAL, NOTIFICATION and WARNINGS.

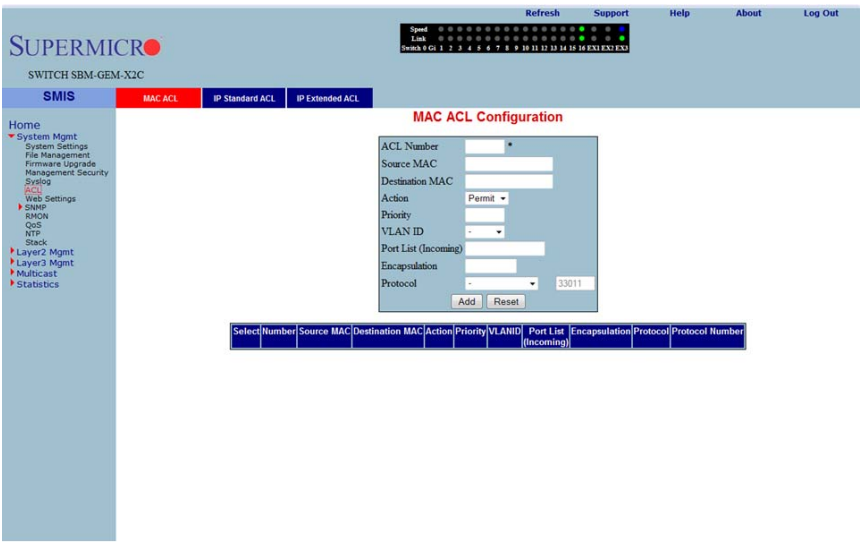
ACL

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

- MAC Based ACL
- IP Standard ACL
- IP Extended ACL

MAC Based ACL

Figure 5-21. MAC ACL Configuration Page



Clicking the MAC ACL tab brings up the MAC ACL CONFIGURATION page (Figure 5-21), 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

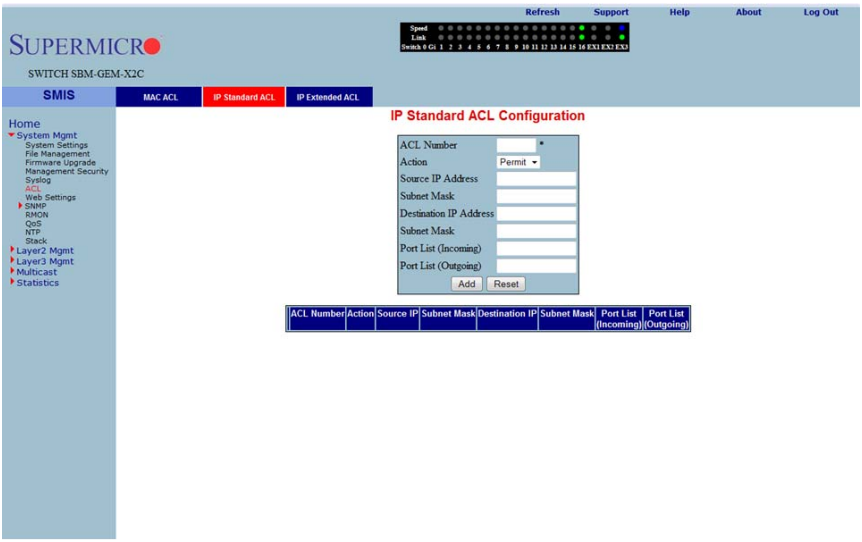
Parameter	Description
ACL Number	This specifies the unique Id for the access list. Valid range is *1* to *65535*. The factory default is blank.
Source and Destination MAC	This specifies both the Source MAC Address and Destination MAC Address, for which the access list must be applied. Both the Source and Destination MAC Addresses must be configured for the status of the access list to be active. The factory default is blank.

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

Parameter	Description
Action	This specifies the action to be taken for the access list. The factory default is **Permit**. • **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**.
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 blank.
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 5-22. IP Standard ACL Configuration Page



Clicking the IP STANDARD ACL (Access Control List) tab brings up the IP STANDARD ACL CONFIGURATION page (Figure 5-22), 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 *65535*. The factory default is blank.
Action	This specifies the action to be taken for the access list. The factory default is **Permit**. • **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.
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 5-23. IP Extended ACL Page

Clicking the IP EXTENDED ACL tab brings up the IP EXTENDED ACL CONFIGURATION page (Figure 5-23), 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

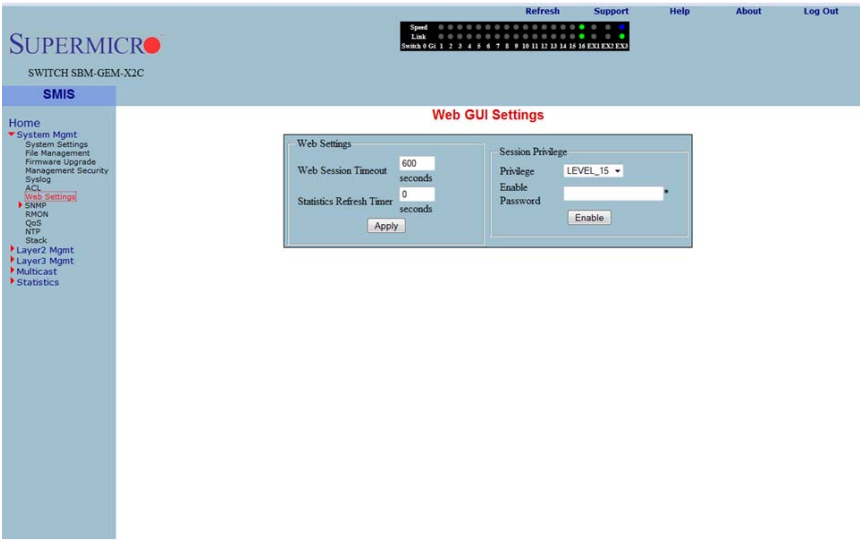
Parameter	Description
ACL Number	This specifies the unique ID for the access list. The valid range is between *1* to *65535*. The factory default is blank.
Subnet Mask	This specifies the Address Mask corresponding to the IP Address.
Action	This specifies the action to be taken for the access list. The factory default is **Permit**. • **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.
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 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.
Protocol	This chooses the protocol type to be checked in the packet to apply this ACL. The factory default is **icmp**.

Table 5-12. IP Extended ACL Configuration Page Parameters (Continued)

Parameter	Description
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 *255*, while the factory default is blank.
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 *Max-reliability*, *Max Throughput*, *Min-delay*, *Normal* 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 *Establish*, *Non-establish* or *Any*.
RST Bit	This specifies the TCP RST bit to be checked against the packet. It can be *Set*, *Notset* or *Any.*
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.

WEB Settings

Figure 5-24. Web GUI Settings Page



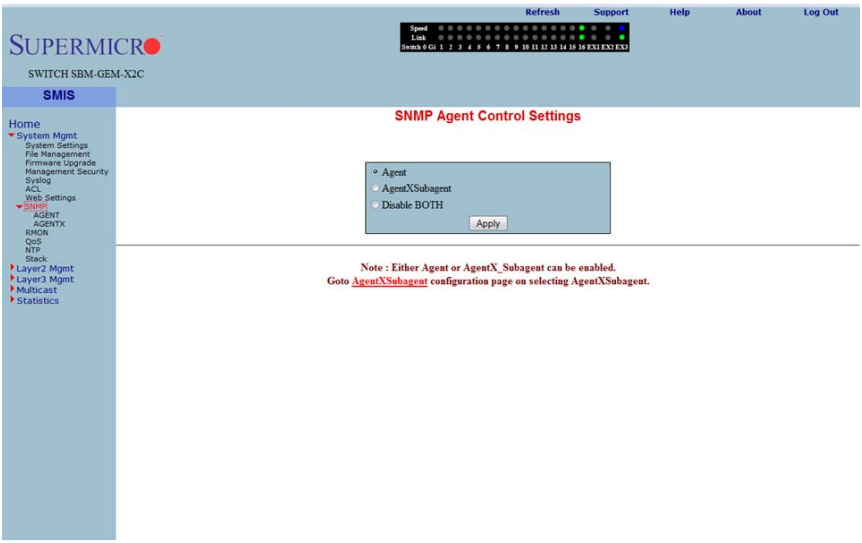
Clicking the WEB SETTINGS link brings up the WEB GUI SETTINGS page (Figure 5-24), which displays all basic Web GUI settings. The parameters for this page are shown in Table 5-13.

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 this page.
Enable Password	This parameter allows you to specify the Enable Password for the selected session priviledge.

SNMP

Figure 5-25. SNMP Agent Control Settings Page



Clicking the SNMP link brings up the SNMP AGENT CONTROL SETTINGS page (Figure 5-25). 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
SNMP Community Settings	This page allows you to configure the SNMP community including the COMMUNITY INDEX, NAME, SECURITY NAME, CONTEXT NAME, TRANSPORT TAG and STORAGE TYPE.
SNMP Group Settings	This page allows you to configure SNMP groups including GROUP NAME, SECURITY NAME, SECURITY MODEL and STORAGE TYPE.
SNMP Group Access Settings	This page allows you to configure SNMP group's access parameters including GROUP NAME, SECURITY MODEL, SECURITY LEVEL, STORAGE TYPE, AND READ, WRITEand NOTIFY VIEW.
SNMP View Tree Settings	This page allows you to configure an SNMP view tree including VIEW NAME, SUB TREE, MASK, TYPE OF THE VIEW and STORAGE TYPE.
SNMP Target Address Settings	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
SNMP Target Parameter Settings	This setting allows you to configure SNMP target parameters including PARAMETER NAME, MP MODEL, SECURITY MODEL, NAME, LEVEL and STORAGE TYPE.
SNMP User Settings	This setting allows you to configure SNMP security including user name, AUTHENTICATION PROTOCOL, AUTHENTICAITON KEY, PRIVACY PROTOCOL, PRIVACY KEY and STORAGE TYPE.
SNMP Trap Settings	This setting allows you to configure SNMP trap notifications including NOTIFY NAME, NOTIFY TAG, NOTIFY TYPE and STORAGE TYPE.

SNMP Community Settings

Figure 5-26. SNMP Community Settings Page

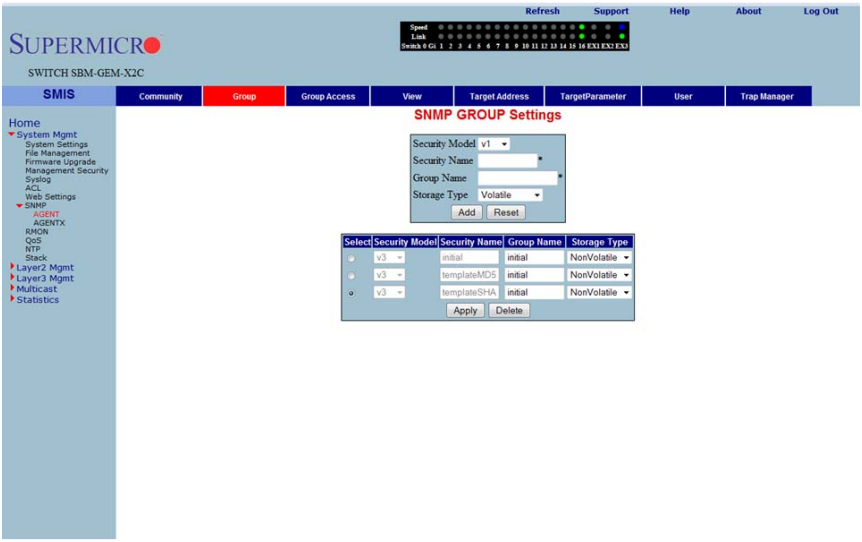
Clicking the COMMUNITY tab brings up the SNMP COMMUNITY SETTINGS page (Figure 5-26), which allows you to add SNMP managers or remove existing managers.. The parameters for this page are shown in Table 5-15.

Table 5-15. SNMP Community Settings Page Parameters

Parameter	Description
Community index	This parameter sets the COMMUNITY INDEX identifer.
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 Identifer.
Storage Type	This parameter sets the *Volatile Storage* or *Non-volatile Storage* setting.

SNMP Group Settings

Figure 5-27. SNMP Group Settings Page



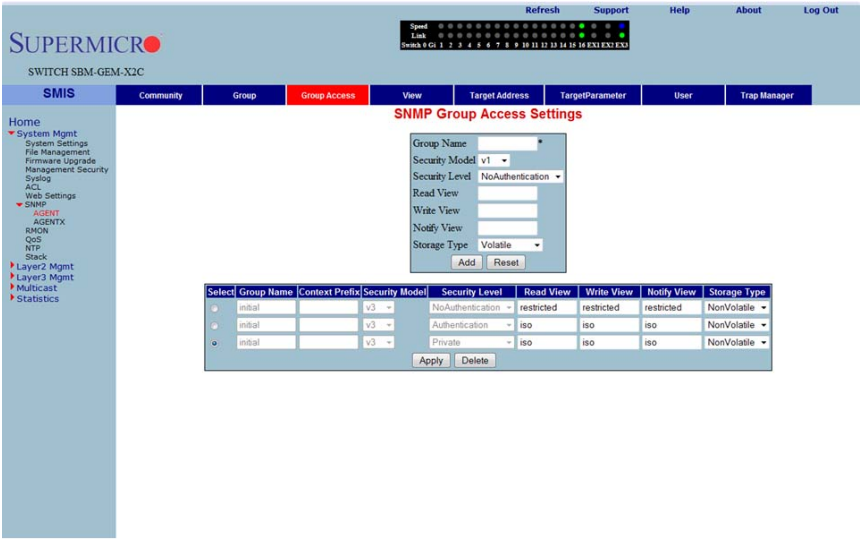
Clicking the GROUP tab brings up the SNMP GROUP SETTINGS page (Figure 5-27). This page helps you map a combination of the SECURITY MODEL and the SECURITY NAME into a GROUP NAME, which is used to define an access control policy. In addition, this page displays the STORAGE TYPE of the Group Table. The 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 *version 1*, *version 2* or *version 3* 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 *volatile* or *non-volatile*.

SNMP Group Access Settings

Figure 5-28. SNMP Group Access Settings Page



Clicking the GROUP ACCESS tab brings up the SNMP GROUP ACCESS SETTINGS page (Figure 5-28), 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

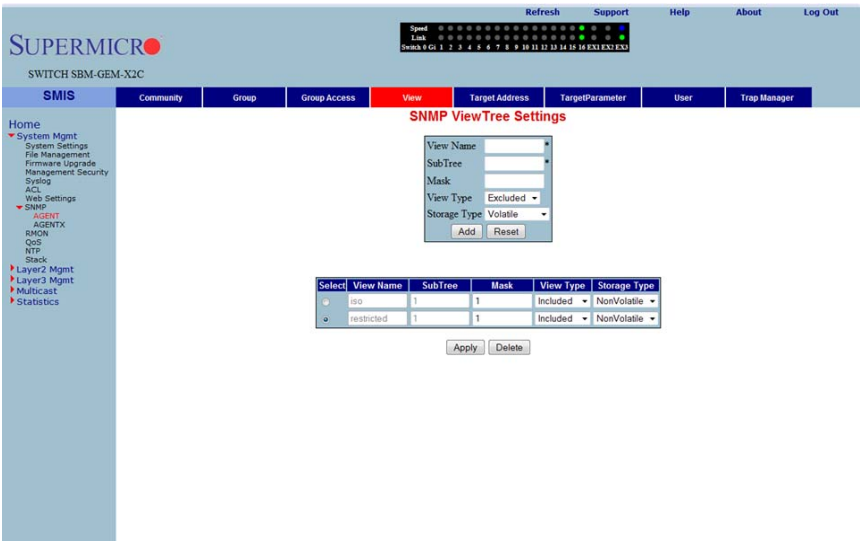
Parameter	Description
Group Name	This parameter allows you to specify the GROUP NAME string.
Security Model	This parameter allows you to specify whether SNMP *version v1, v2* or *v3* is used. *Version 3* is the most secure model as it allows packet encryption with the private key word.
Security Level	With this parameter the no-authentication option disables authentication. The AUTHENTICATION option enables *Message digest (MD5)* or *Secure Hash Algorithm (SHA)* 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.

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

Parameter	Description
Notify View	This parameter allows you to specify the NOTIFY VIEW identifier.
Storage Type	Use this parameter to specify whether the STORAGE TYPE is *volatile* or *non-volatile*.

SNMP View Tree Settings

Figure 5-29. SNMP View Tree Settings Page



Clicking the VIEW tab brings up the SNMP VIEW TREE SETTINGS page (Figure 5-29), 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

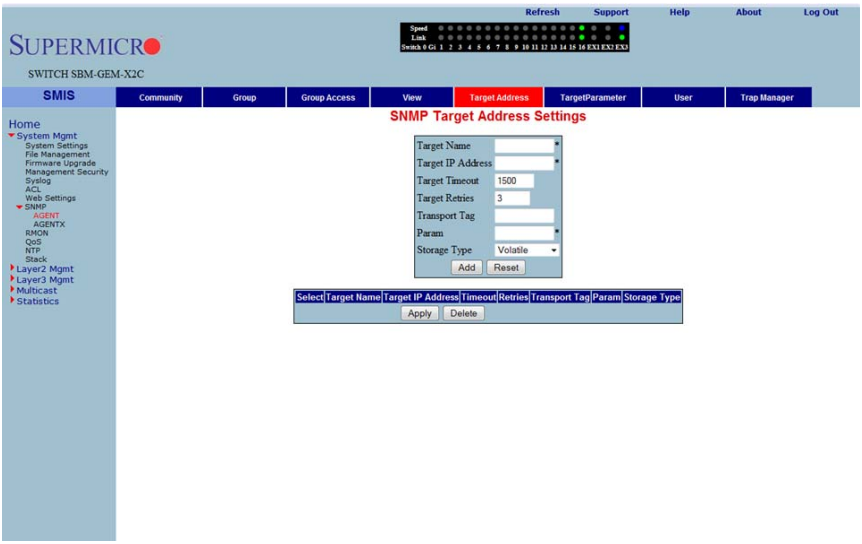
Parameter	Description
View Name	This parameter specifies a VIEW NAME string.
SubTree	This parameter specifies a tree OID.
Mask	This parameter specifies an OID mask.

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

Parameter	Description
View Type	This parameter specifies whether a VIEW TYPE is *Included* or *Excluded*.
Storage Type	Use this parameter to specify whether the STORAGE TYPE is *volatile* or *non-volatile*.

SNMP Target Address Settings

Figure 5-30. SNMP Target Address Settings Page



Clicking the TARGET ADDRESS tab brings up the SNMP TARGET ADDRESS SETTINGS page (Figure 5-30), 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

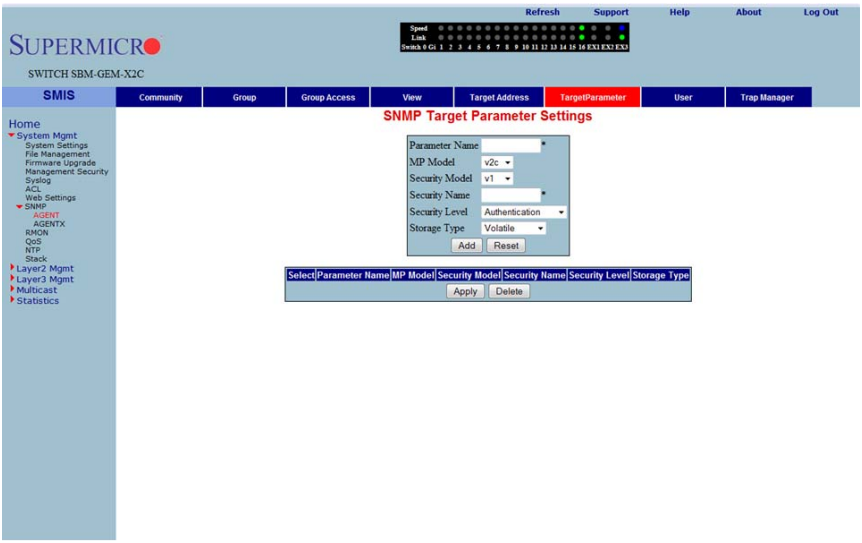
Parameter	Description
Target Name	This parameter specifies a TARGET NAME as a unique identifier.
Target IP Address	The TARGET IP ADDRESS specifies a target address to be used in the generation of SNMP operations.
Target Timeout	TARGET TIMEOUT specifies the maximum round trip for communicating with the 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 *volatile* or *non-volatile*.

SNMP Target Parameter Settings

Figure 5-31. SNMP Target Parameter Settings Page



Clicking the TARGET PARAMETER tab brings up the SNMP TARGET PARAMETER SETTINGS page (Figure 5-31), 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

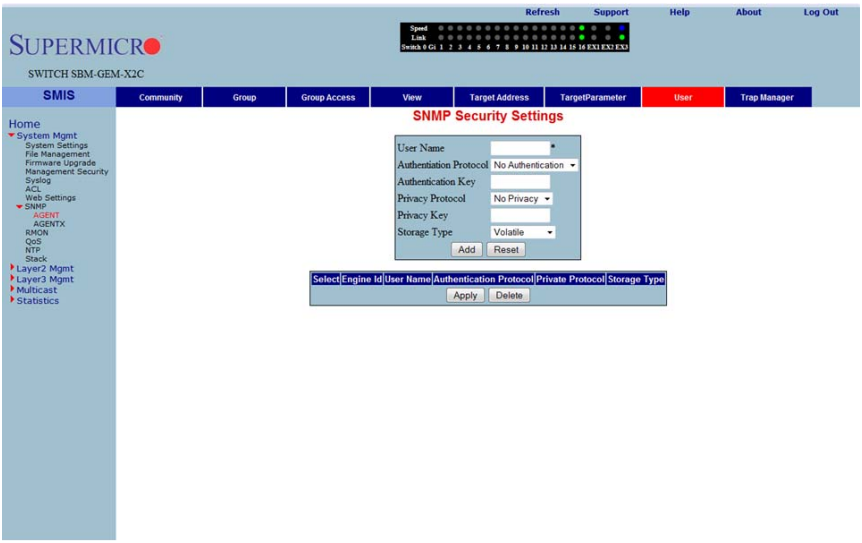
Parameter	Description
Parameter Name	The target parameter is an unique name that specifies SNMP target information to be used in the generation of SNMP messages.
MP Model	The Message Processing (MP) Model is used when generating SNMP messages using this entry.
Security Model	The SECURITY MODEL is used 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*.

SNMP User Settings

Figure 5-32. SNMP Security Settings Page



Clicking the USER tab brings up the SNMP SECURITY SETTINGS page (Figure 5-32), 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

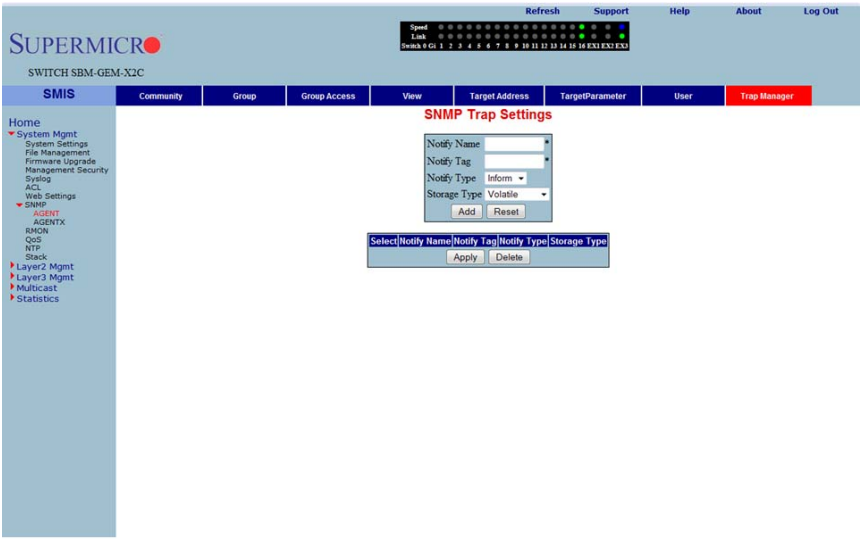
Parameter	Description
User Name	USER NAME is the (User-based Security) model dependent security ID.
Authentication Protocol	The AUTHENTICATION PROTOCOL is used for authentication.
Authentication Key	The AUTHENTICATION KEY is the secret authentication key used for messages sent on behalf of this user 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*.

SNMP Trap Settings

Figure 5-33. SNMP Trap Settings Page



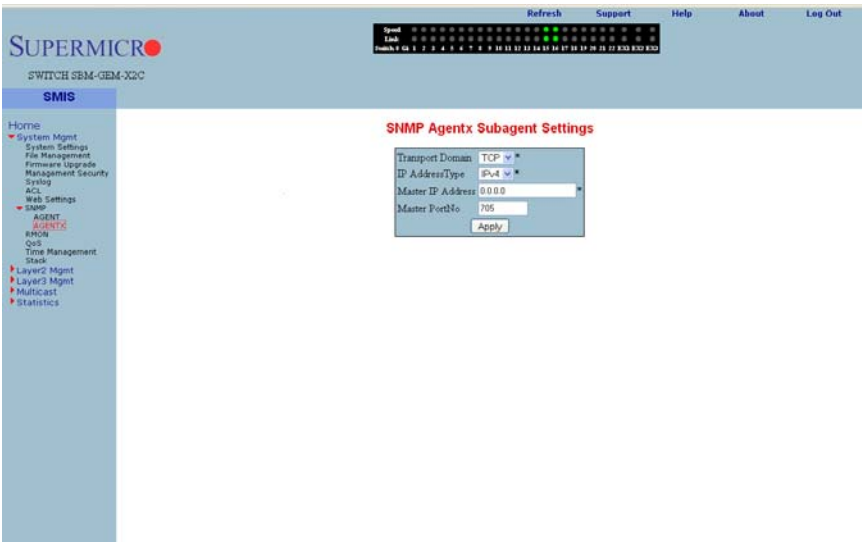
Clicking the TRAP MANAGER tab brings up the SNMP TRAP SETTINGS page (Figure 5-33), which configures the set of management targets that must receive notifications. The parameters for this page are shown in Table 5-22.

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 *Trap* or *Inform*.
Storage Type	STORAGE TYPE can be configured as *Volatile* or *Non-Volatile*.

SNMP AgentX

Figure 5-34. SNMP AgentX Subagent Settings Page



Clicking the AGENTX link brings up the SNMP AGENTX SUBAGENT SETTINGS page (Figure 5-34), 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 *IPv4* or *IPv6* 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.

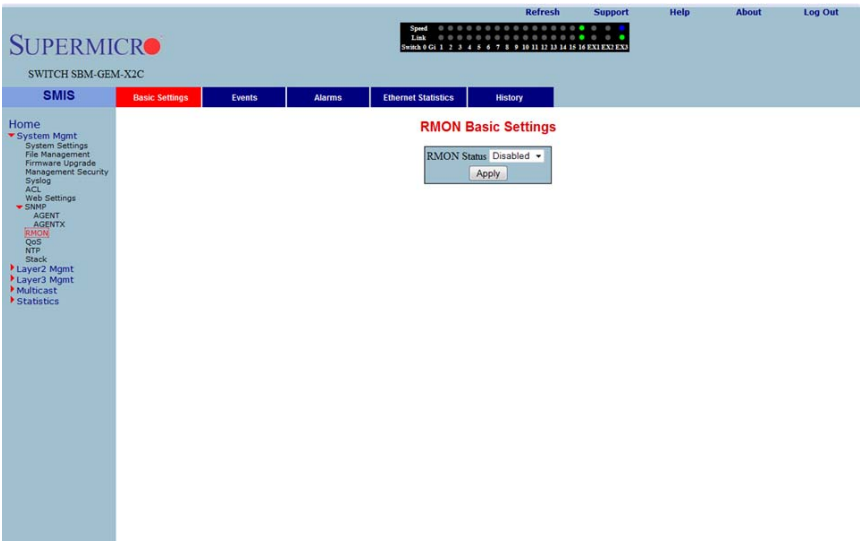
RMON

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

- RMON Basic Settings
- Event Configuration
- RMON Alarm Configuration
- Ethernet Statistics Configuration
- History Control Configuration

RMON Basic Settings

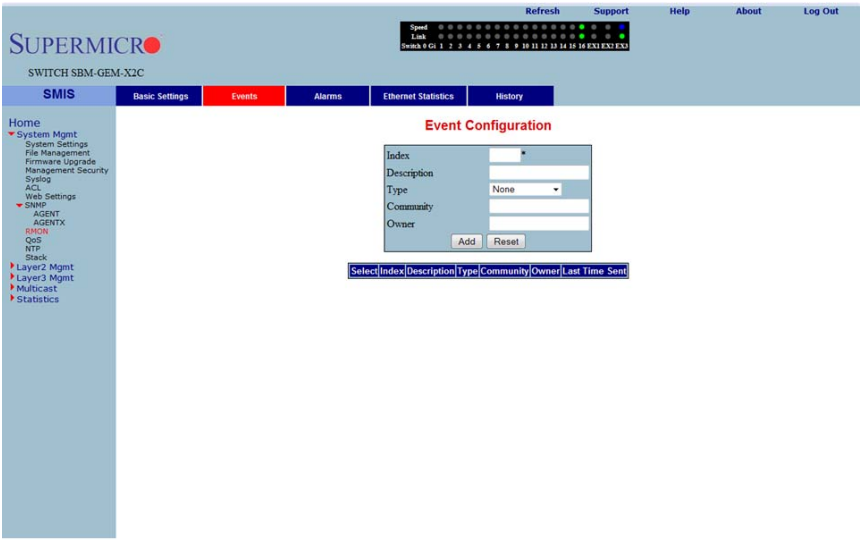
Figure 5-35. RMON Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the RMON BASIC SETTINGS page (Figure 5-35), which enables/disables the RMON feature using the RMON Status parameter.

Event Configuration

Figure 5-36. Event Configuration Settings Page



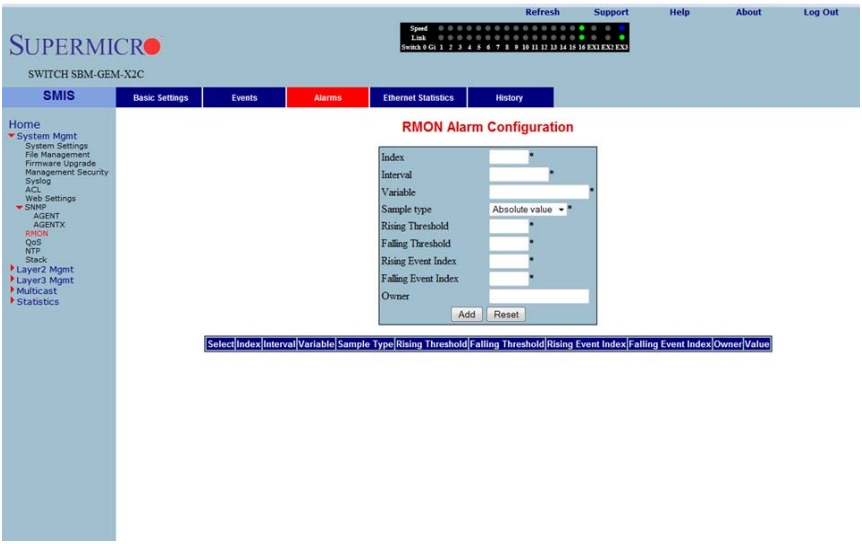
Clicking the EVENTS tab brings up the EVENT CONFIGURATIONS page (Figure 5-36), which configures RMON events. The parameters for this page are shown in Table 5-24.

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 *Log*, an *SNMP Trap*, *Both*, or *None*. For the event type to display, *TRAP and Log* and *TRAP Community* 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, *TRAP and Log* and *TRAP Community* 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.

RMON Alarm Configuration

Figure 5-37. RMON Alarm Configuration Page



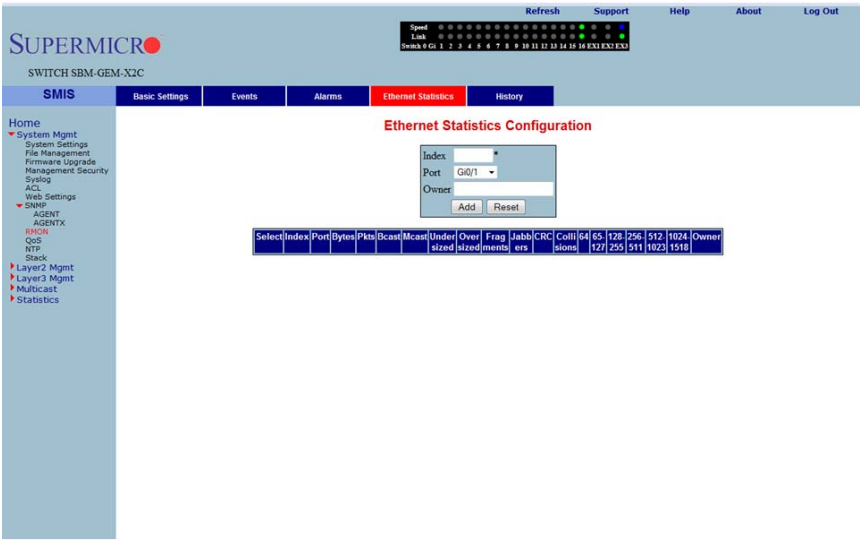
Clicking the ALARM tab brings up the RMON ALARM CONFIGURATION page (Figure 5-37), which configures RMON Alarm paramters. The parameters for this page are shown in Table 5-25.

Table 5-25. RMON Alarm Configuration Page Parameters

Parameter	Description
Index	This parameter specifies the table index.
Interval	This parameter specifies the time interval for which the alarm monitors the variable.
Variable	This parameter specifies the MIB object on which the alarm is set.
Sample Type	You can set this parameter to an *Absolute Value* or as just an *Incremental Value* of the timer.
Rising Threshold	If the startup alarm is set as *Rising Alarm* and this threshold is reached, an alarm is raised.
Falling Threshold	If the startup alarm is set as *Falling Alarm* and this threshold is reached, an alarm is raised.
Rising Event Index	Indicates the index of the event to be raised when the RISING THRESHOLD is reached.
Falling Event Index	Indicates the index of the event to be raised when the FALLING THRESHOLD is reached.
Owner	Specifies the owner of the alarm.

Ethernet Statistics Configuration

Figure 5-38. Ethernet Statistics Configuration Page



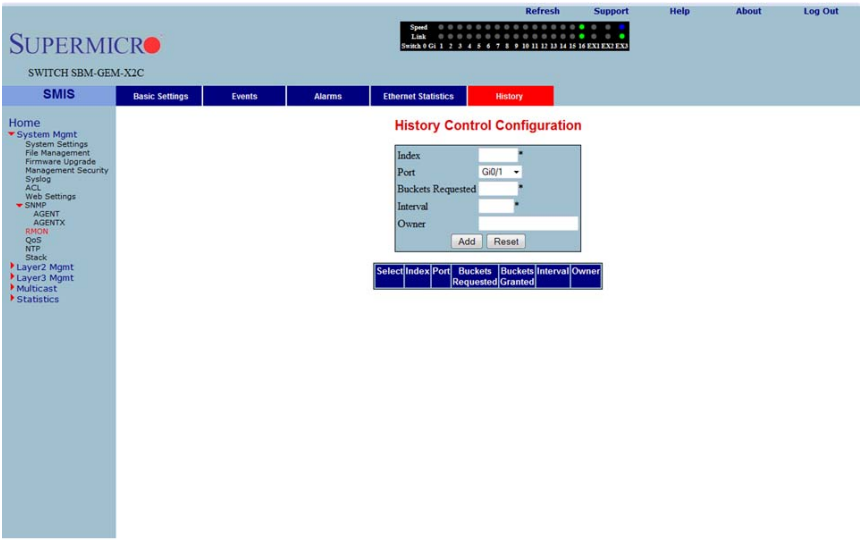
Clicking the ETHERNET STATISTICS tab brings up the ETHERNET STATISTICS CONFIGURATION page (Figure 5-38), which configures RMON Ethernet statistics parameters. The parameters for this page are shown in Table 5-26.

Table 5-26. Ethernet Statistics Configuration Page Parameters

Parameter	Description
Index	This parameter specifies the index to the table.
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.
Multicast Packets	This parameter specifies the total number of multicast packets received from the network.
Owner	This parameter specifies the owner string.

History Control Configuration

Figure 5-39. History Control Configuration Page



Clicking the HISTORY tab brings up the HISTORY CONTROL CONFIGURATION page (Figure 5-39), 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.
Interval	This parameter specifies the time interval between two successive polls to collect the statistics.
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 *Valid* or *Invalid*.

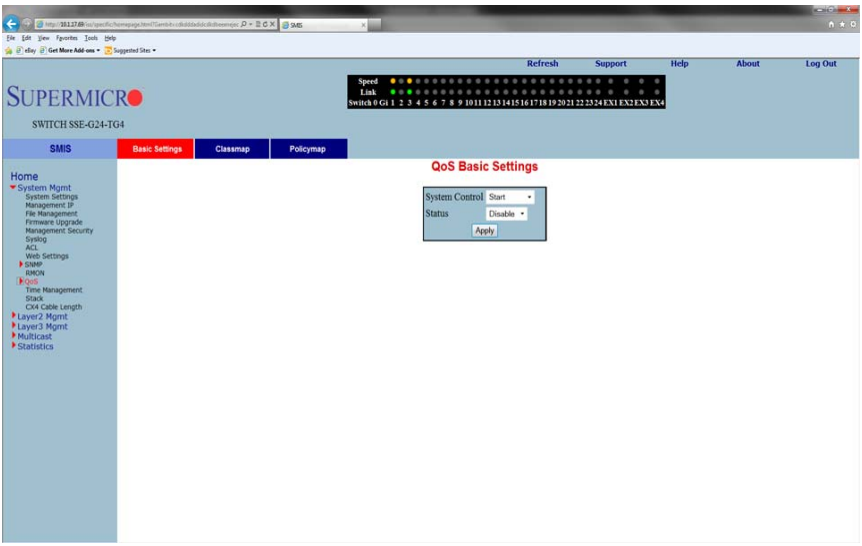
QoS

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

- QOS Basic Settings
- QOS Classmap Settings
- QOS Policymap Settings
- COS Queue Mapping

QOS Basic Settings

Figure 5-40. QOS Basic Settings Page



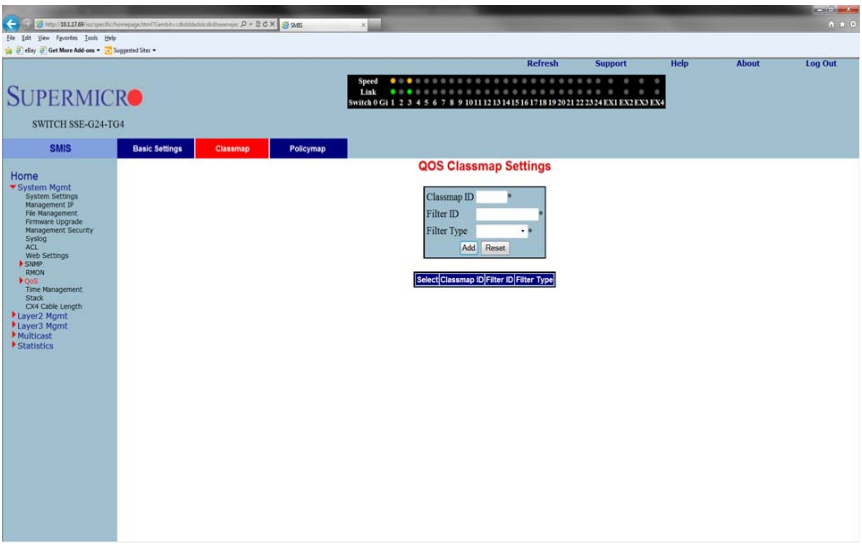
Clicking the BASIC SETTINGS tab brings up the QOS BASIC SETTINGS page (Figure 5-40), which allows you to configure QOS basic settings parameters. The parameters for this page are shown in Table 5-28.

Table 5-28. QOS Basic Settings Page Parameters

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

QOS Classmap Settings

Figure 5-41. QOS Classmap Settings Page



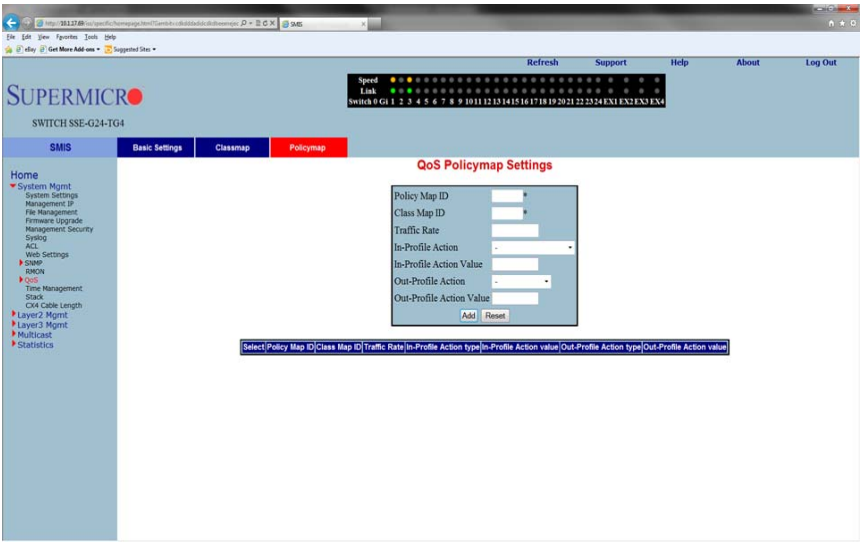
Clicking the CLASSMAP tab brings up the QOS CLASSMAP SETTINGS page (Figure 5-41), which is used to classify the stream of traffic. The parameters for this page are shown in Table 5-29.

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 *MAC filter (1)* or *IP filter (2)*.

QOS Policymap Settings

Figure 5-42. QOS Policymap Settings Page



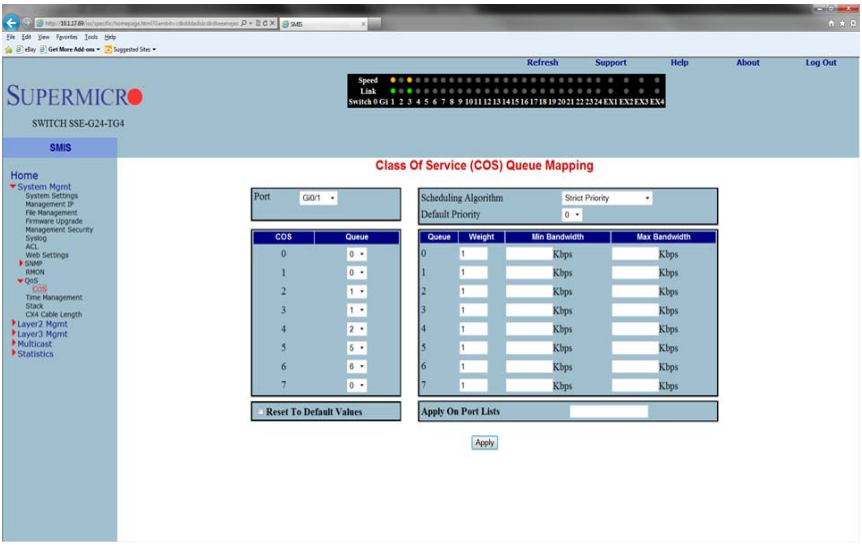
Clicking the POLICYMAP tab brings up the QOS POLICYMAP SETTINGS page (Figure 5-42), which is used to specify action for a specified classmap. The parameters for this page are shown in Table 5-30.

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.
In-Profile Action	This parameter specifies the action to be applied on matched data, and can be specified as either *Policy DSCP* or *Policy Precedence*.
Out-Profile Action	This parameter specifies the action to be applied on out-of-profile data, and can be specified as either *Policy DSCP* or *Drop*.
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 *Drop* or from *0* to *63* for DSCP.

COS Queue Mapping

Figure 5-43. COS Queue Mapping Page



Clicking COS (Class of Service) tab brings up the COS QUEUE MAPPING page (Figure 5-43), which configures the Class Of Server (COS) Queue Mapping. The parameters for this page are shown in Table 5-31.

Table 5-31. COSQ Scheduling Algorithm Settings 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: • *Strict Priority* • *Round Robin* • *Weighted Round Robin* • *Deficit Round Robin*
COS and Queue	This parameter allows you to select between 0 to 7 for you COS Queue value.
COS Queue Weight	This parameter allows you to select between 0 to 15 for your COS Queue WEIGHT value.
COS Queue Min Bandwidth	This parameter configures minimum bandwidth between 1 to 262143.
COSQ Max Bandwidth	This parameter configures maximum bandwidth between 1 to 262143.
COS Queue Flag	Use this parameter to set a flag for this queue.

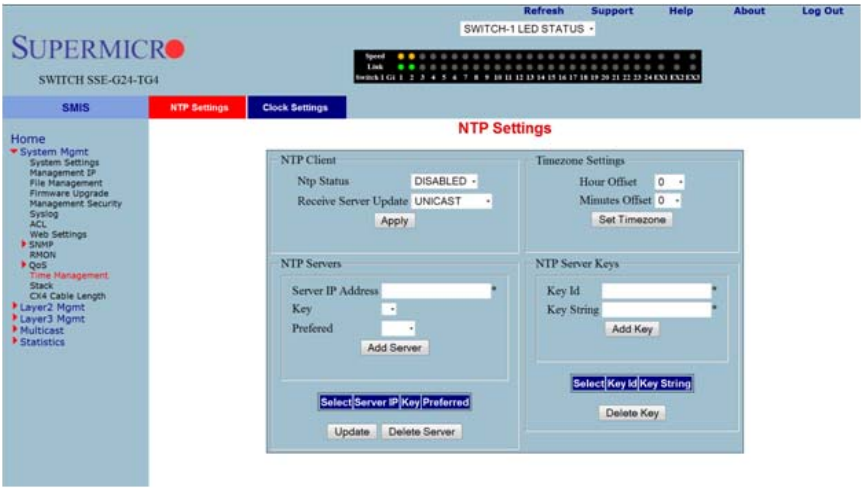
Time Management

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 5-44. NTP Settings Page



Clicking the NTP link brings up the NTP SETTINGS page (Figure 5-44), which configures the Network Time Protocol (NTP). The parameters for this page are shown in Table 5-32.

Table 5-32. NTP Settings Page Parameters

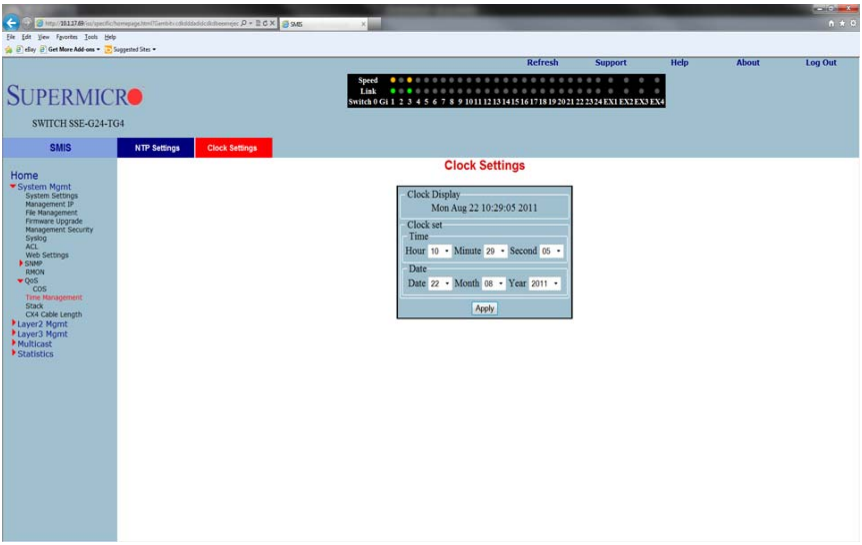
Parameter	Description
NTP Client Settings	
NTP Status	This field enables or disables NTP in the switch. Configure the NTP SERVERS section to enable NTP.
Receive Server Update	The value for this parameter could be *Broadcast* or *Unicast*. To process the broadcast NTP updates from the server, choose the *Broadcast* 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	

Table 5-32. NTP Settings Page Parameters (Continued)

Parameter	Description
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 *Yes* 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 paramter to specify any string to be used as a key to handshake with NTP servers.

Clock Settings

Figure 5-45. Clock Settings Page



Clicking the CLOCK SETTINGS link brings up the CLOCK SETTINGS page (Figure 5-45), which allows to configure the Time and Date in the switch. The parameters for this page are shown in Table 5-33.

Table 5-33. 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 Extrement 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.

Similarily 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

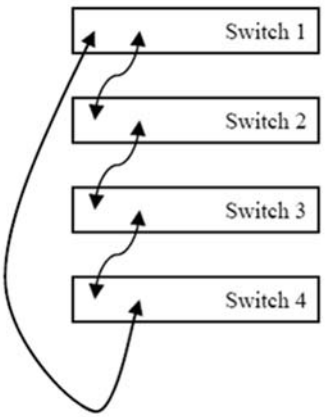
Connect the stacked switches using stacking cables. For better redundancy, connect the switches daisy chained as shown in the diagram below (Figure 5-46). This chain connectivity helps to maintain stacking in case a single link or switch fails.

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 specifical 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.

Figure 5-46. 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.

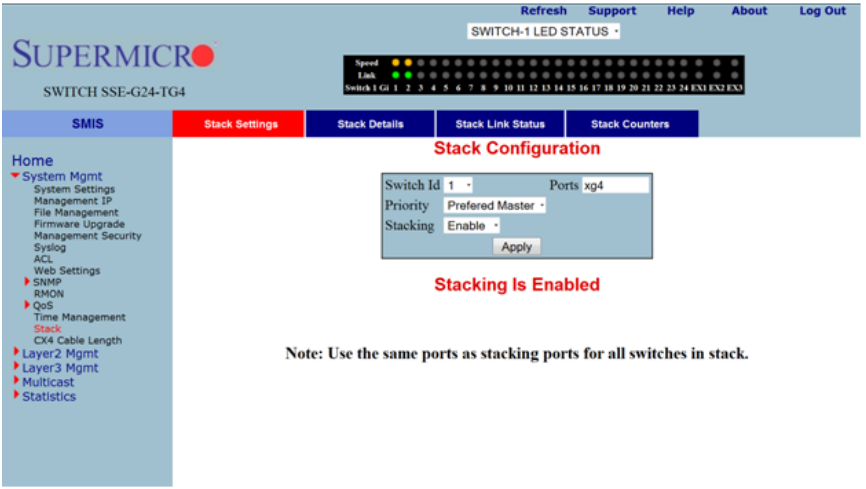
NOTE: When a switch is moved from stacking to stand-alone mode, the saved stacking configurations can not be loaded in stand-alone mode. When stacking is disabled, the switch software renames the existing configuration file to avoid automatic restoration of stacking configurations on a stand-alone switch.

The following pages are available for configuring Stack settings;

- Stack Configuration
- Stack Details
- Stack Link Status
- Stack Counters

Stack Configuration

Figure 5-47. Stack Configuration Page



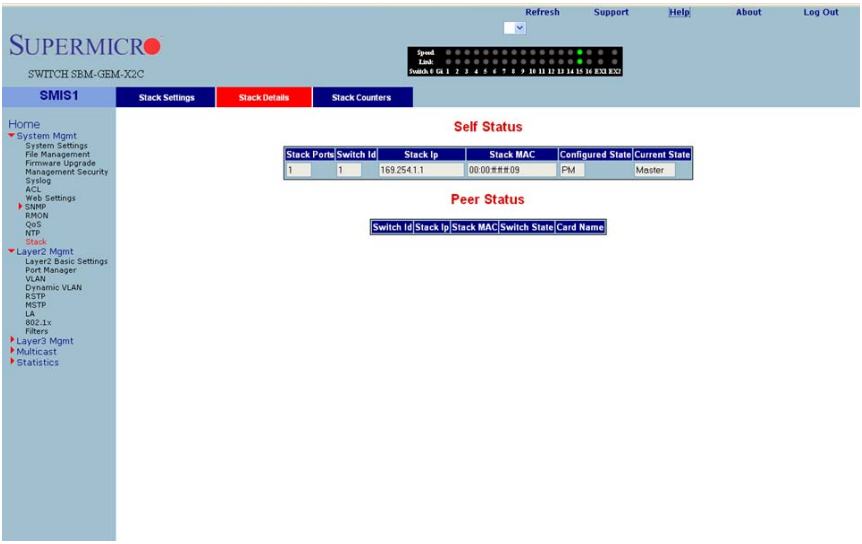
Clicking the STACK SETTINGS tab brings up the STACK CONFIGURATION page (Figure 5-47), which configures the stacking feature. The parameters for this page are shown in Table 5-34.

Table 5-34. 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 choosen as *2*, the physical interfaces will be referred as *Gi2/1*, *Gi2/1* and so on. For non-stacking, stand-alone cases this switch ID is considered as *zero*.
Priority	This parameter chooses the priority for this switch in the Stacking Master selection. It could be configured as *Preferred Master*, *Backup Master* or *Preferred Slave*.
Stacking	This parameter enables or disables stacking. **NOTE:** Any change in stacking status requires a reboot of the switch.

Stack Details

Figure 5-48. Stack Details Page



Clicking the STACK DETAILS tab brings up the STACK DETAILS page (Figure 5-48), which displays stacking details. The parameters for this page are shown in Table 5-35.

Table 5-35. Stack Details Page Parameters

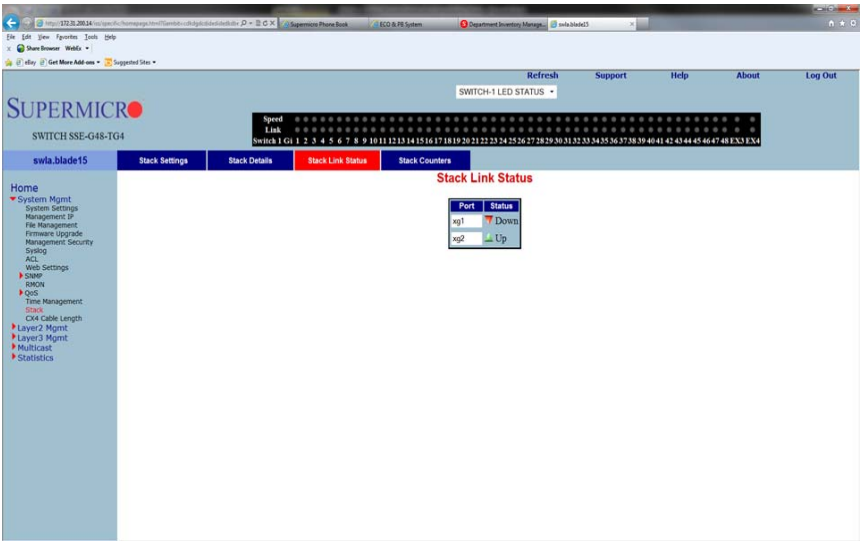
Parameter	Description
Self Status	
Stack Ports	This is the number of stacking ports configured in this switch.
Switch ID	This parameter is used to specify the switch identifier of this switch.
Stack IP	This parameter is used to specify the IP address of this switch. This IP address is used to communicate 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 *Master* or *Slave*.
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 5-35. 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 5-49. Stack Link Status Page



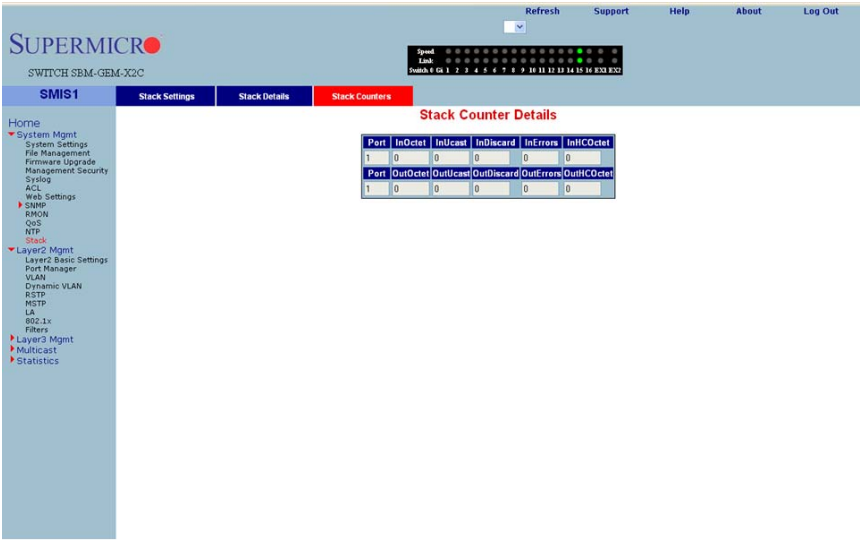
Clicking the STACK LINK STATUS tab brings up the STACK LINK STATUS page (Figure 5-49), which displays stacking link status. The parameters for this page are shown in Table 5-36.

Table 5-36. 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 5-50. Stack Counter Details Page



Clicking the STACK COUNTERS tab brings up the STACK COUNTERS DETAILS page (Figure 5-50), which displays statistics for stacking ports. The parameters for this page are shown in Table 5-37.

Table 5-37. 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

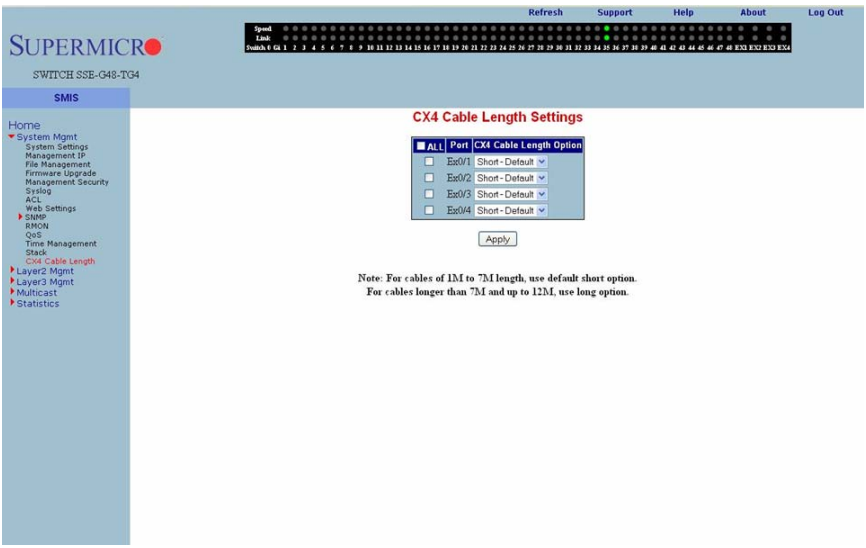
Stacking is supported with CX-4 cables only. The CX-4 cable used for stacking should be no more than 3-meters in length, because stacking internally runs at 12-Gbps and therefore requires a more robust signal than longer cable lengths might provide reliably. The industry standard stacking cable length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

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

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 5-51) and then selecting the "long" option.

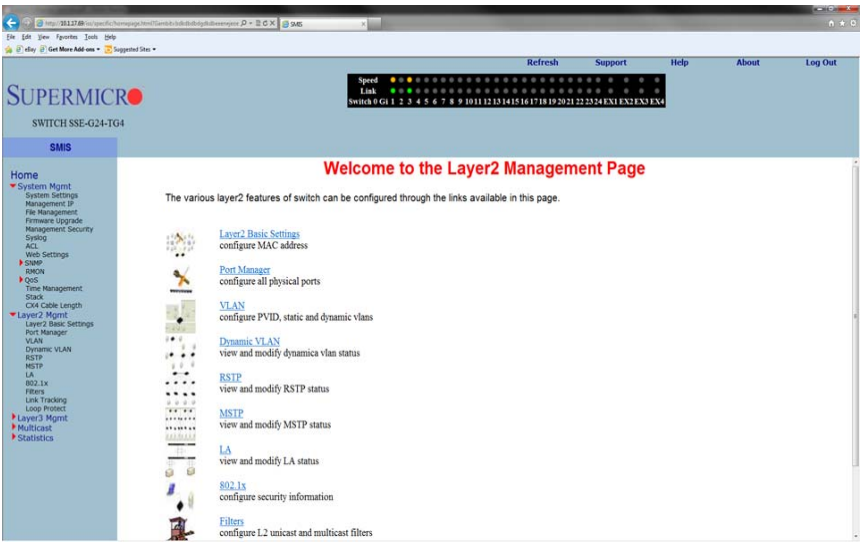
Figure 5-51. Configuring CX4 Cable Length



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 5-52. Layer2 Management Page

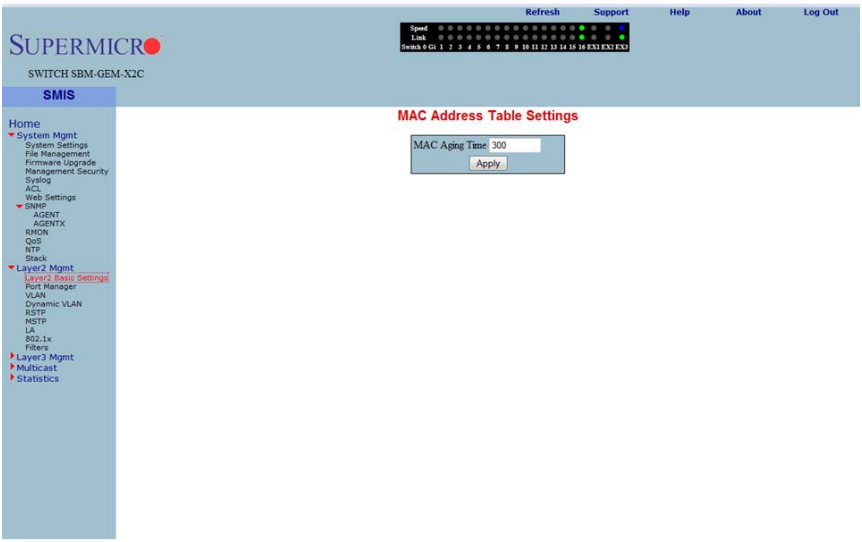


The LAYER2 MANAGEMENT page (Figure 5-52) contains the following links for Layer2 controls:

- Layer 2 Basic Settings
- Port Manager
- VLAN
- Dynamic Vlan
- RSTP
- MSTP
- LA
- 802.1x
- Filters
- Line Tracking
- Loop Protect

Layer 2 Basic Settings

Figure 5-53. MAC Address Table Settings Page



Clicking the LAYER2 BASIC STTINGS link brings up the MAC ADDRESS TABLE SETTINGS page (Figure 5-53), 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:

- Port Basic Settings
- Port Monitoring
- Storm Control/Rate Limiting

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.

Port Basic Settings

Figure 5-54. Port Basic Settings Page

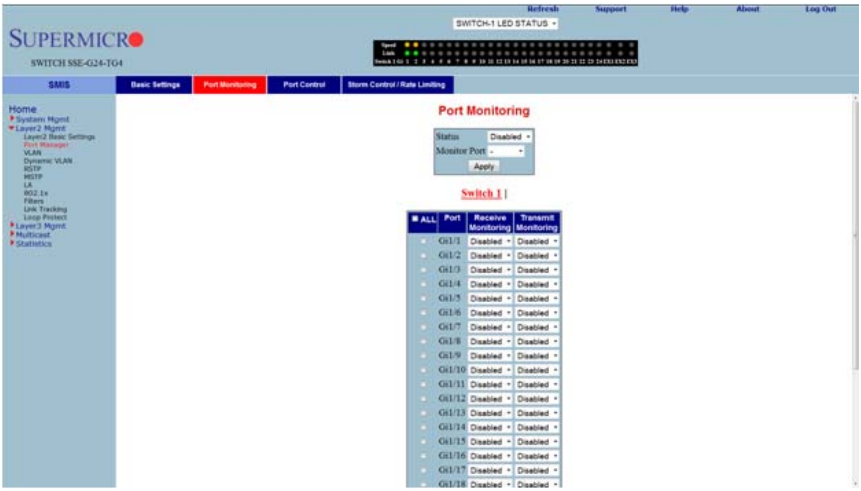
Clicking the BASIC SETTINGS tab brings up the PORT BASIC SETTINGS page (Figure 5-54), which allows you to configure port status and mode information. This page also helps configuring priority and MTU. The parameters for this page are shown in Table 5-38.

Table 5-38. 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 *Up* or *Down*.
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 *No*.
Switch Port Mode	Use this control allows to set the access mode as either *Trunk* or *Hybrid*.
MTU	This sets the MTU value. The Minimum is *90* and Maximum is *9210*. A port must be administrativly down in order 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.

Port Monitoring

Figure 5-55. Port Monitoring Page



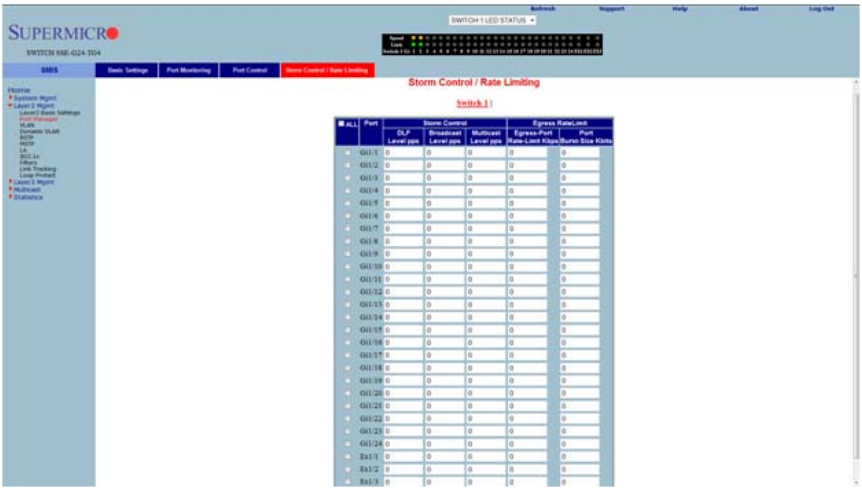
Clicking the PORT MONITORING tab brings up the PORT MONITORING page (Figure 5-55), which allows you to enable or disbale monitoring on port interface. The parameters for this page are shown in Table 5-39.

Table 5-39. Port Monitoring Page Parameters

Parameter	Description
Status	This parameter enables or disables the port monitoring.
Port	This displays the port number.
Receive Monitoring	This parameter enables or disables the receive monitoring.
Trasmit Monitoring	This parameter enables or disables the transmit monitoring.

Storm Control/Rate Limiting

Figure 5-56. Storm Control/Rate Limiting Page



Clicking the STORM CONTROL/RATE LIMITING tab brings up the STORM CONTROL/RATE LIMITING page (Figure 5-56), 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 5-40.

Table 5-40. Storm Control/Rate Limiting Page Parameters

Parameter	Description
Port	This displays the port number.
Mode	This parameter allows you to select either *Auto Negotiation* or *No-negotiation*.
Duplex	This parameter allows you to select either *Full Duplex* or *Half Duplex*.
Speed	This parameter allows you to select the speed as *10 Mbps*, *100 Mbps* or *1 Gb/s*.
Flow Control Admin Status	This parmeter allows you to specify the Flow Control Admin Status as either *Disabled*, Trasmit Flow Control *Enabled*, Receive Flow Control *Enabled* or both Transmit and Receive Flow Control *Enabled*.
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 5-40. 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.

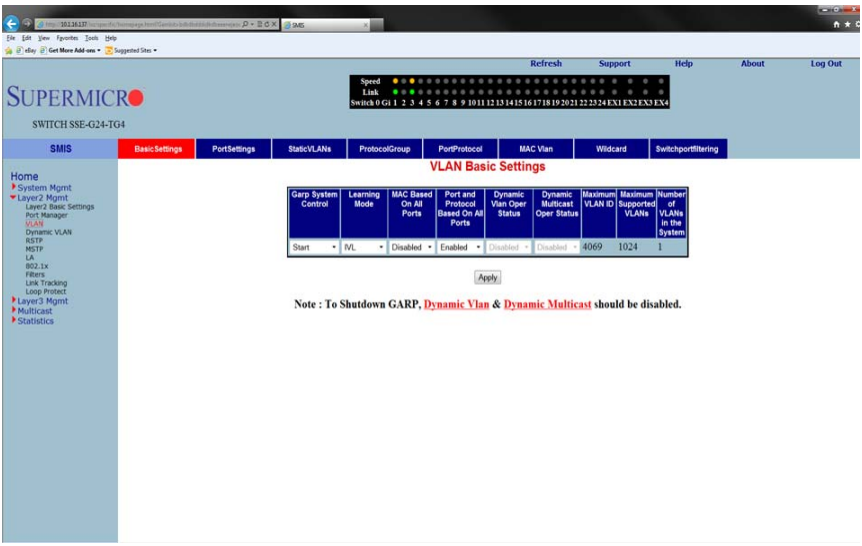
VLAN

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

- VLAN Basic Settings
- Port Settings
- Static VLAN
- Protocol Group
- Port Protocol
- MAC VLAN
- Wildcard
- Switch Port Filtering VLAN

VLAN Basic Settings

Figure 5-57. VLAN Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the VLAN BASIC SETTINGS page (Figure 5-57), which displays VLAN global configuration information. The parameters for this page are shown in Table 5-41.

Table 5-41. 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 (*Independent, Shared, Hybrid* or *VLAN Learning*).
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.
Dynamic VLAN Oper Status	This setting is disabled and cannot be changed.
Dynamic Multicast Oper Status	This setting is disabled and cannot be changed.
Maximum VLAN ID	This parameter specifies the largest (4094) valid VLAN ID, which this switch can accept, above which all will be discarded.

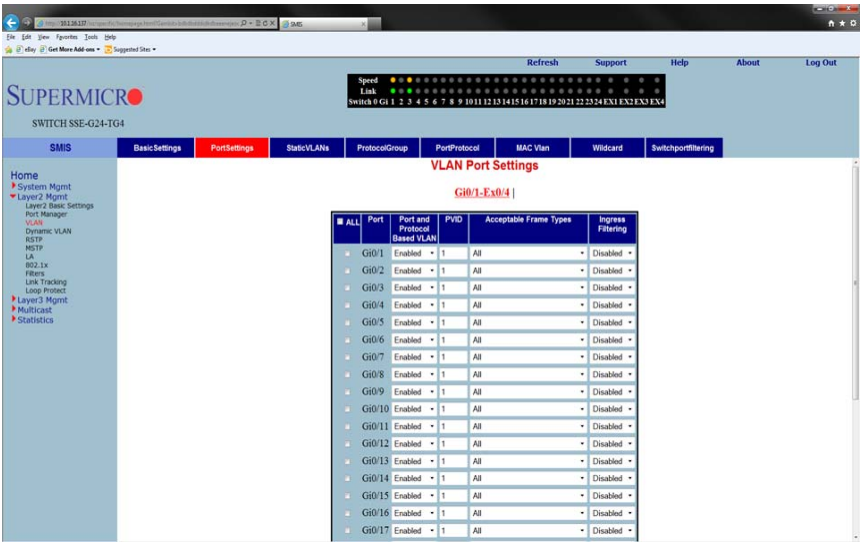
Table 5-41. VLAN Basic Settings Page Parameters (Continued)

Parameter	Description
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.

In addition, the BASIC SETTINGS page provides the configuration3 of Bridge Mode (*Customer /Provider*) and the priority for tunneled STP BPDUs. When you configure BRIDGE MODE TO PROVIDER, the Port Protocol based classification and MAC-based classification on all ports must be disabled.

Port Settings

Figure 5-58. VLAN Port Settings Page



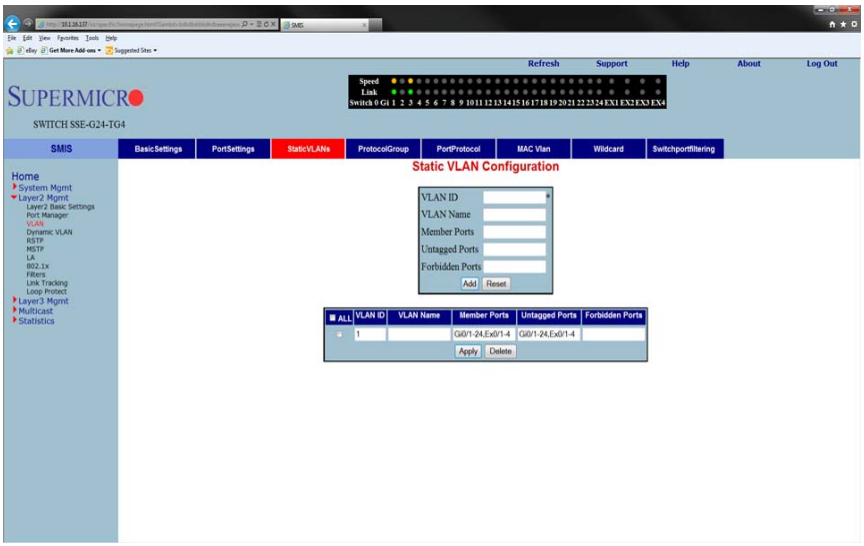
Clicking the PORT SETTINGS tab brings up the VLAN PORT SETTINGS page (Figure 5-58), which is used to associate the VLAN ID to the port for Port based VLAN classification.

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.

Static VLAN

Figure 5-59. Static VLAN Configuration Page



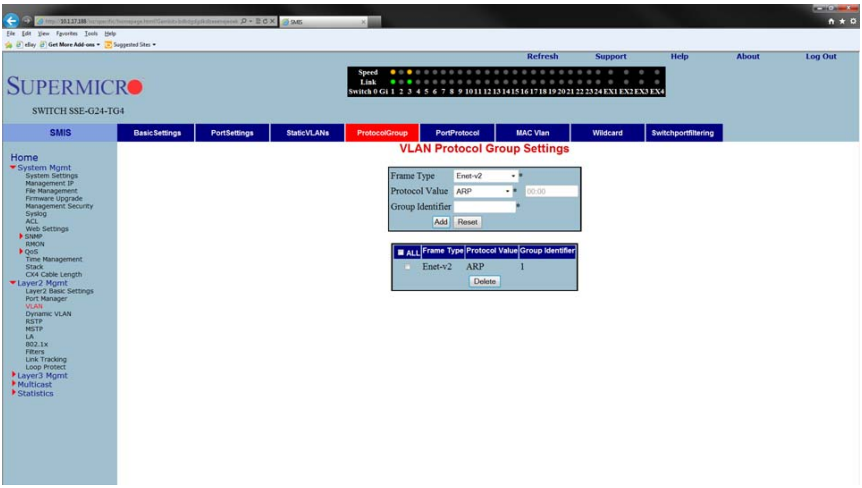
Clicking the STATIC VLANS tab brings up the STATIC VLAN CONFIGURATION page (Figure 5-59), which allows you to configure the VLAN related information statically.

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, MEMBER 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 5-60. VLAN Protocol Group Settings Page

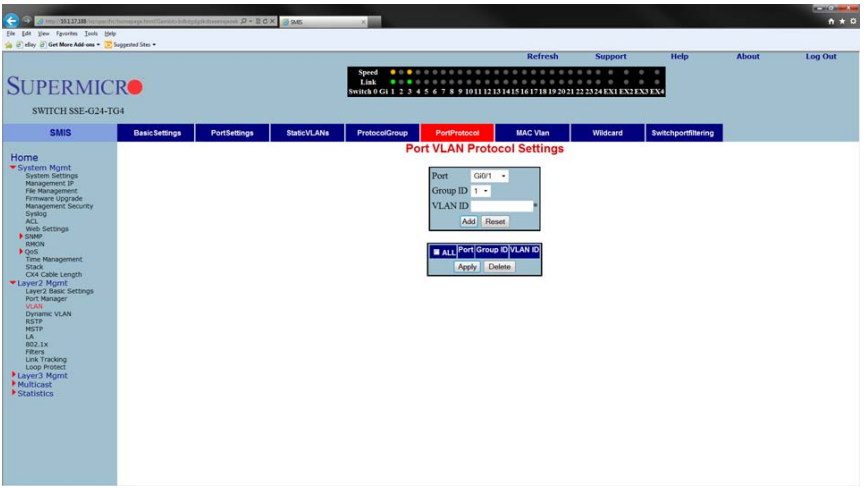


Clicking the PROTOCOL GROUP tab brings up the VLAN PROTOCOL GROUP SETTINGS page (Figure 5-60), which is used to map Protocol Templates to Protocol Group Identifiers.

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 5-61. Port VLAN Protocol Settings



Clicking the Port PROTOCOL tab brings up the PORT VLAN PROTOCOL SETTINGS page (Figure 5-61), 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 5-62. MAC Based VLAN Settings Page

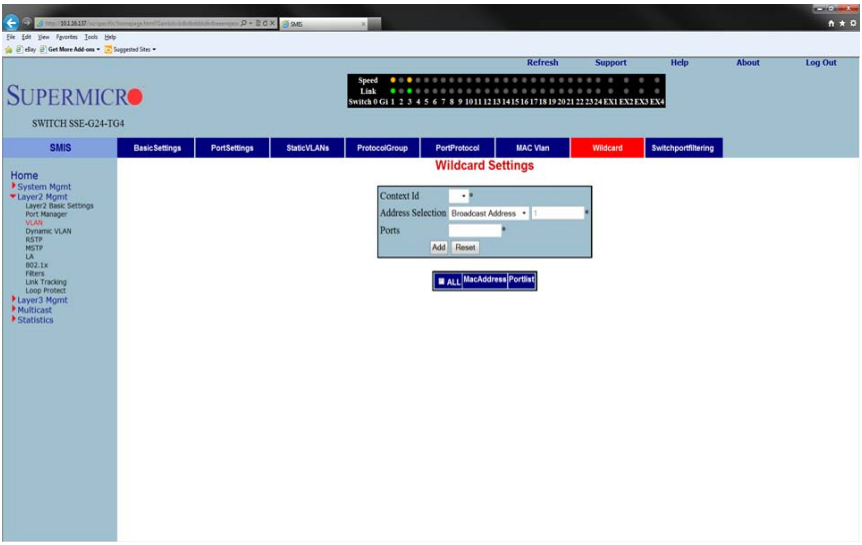
Clicking the MAC VLAN tab brings up the MAC BASED VLAN page (Figure 5-62), which allows to add the MAC Address and Vlan ID to VLANs system. The parameters for this page are shown in Table 5-42.

Table 5-42. 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.

Wildcard

Figure 5-63. Wildcard Settings Page



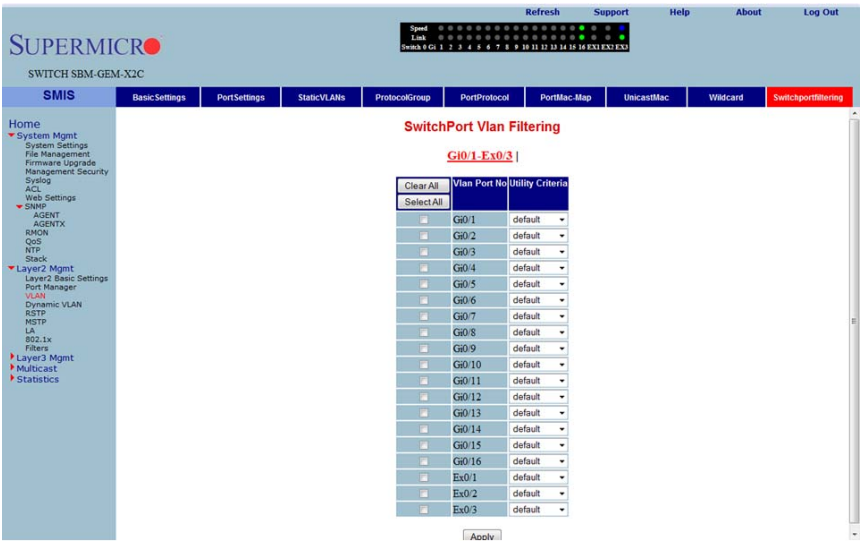
Clicking the WILDCARD tab brings up the WILDCARD SETTINGS page (Figure 5-63), which configures wildcard MAC addresses and ports for VLANs. The parameters for this page are shown in Table 5-43.

Table 5-43. 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.

Switch Port Filtering VLAN

Figure 5-64. Switch Port VLAN Filtering Page



Clicking the SWITCH PORT FILTERING tab brings up the SWITCHPORT VLAN FILTERING page (Figure 5-64), which configures utility criteria for SwitchPort Vlan filtering. The parameters for this page are shown in Table 5-44.

Table 5-44. SwitchPort Vlan Filtering Page Parameters

Parameter	Description
VLAN Port No.	This parameter displays the VLAN Port Number, which can be selected by the check box to the left of the column.
Utility Criteria	Use this parameter to select the utility criteria for the VLAN port selected.

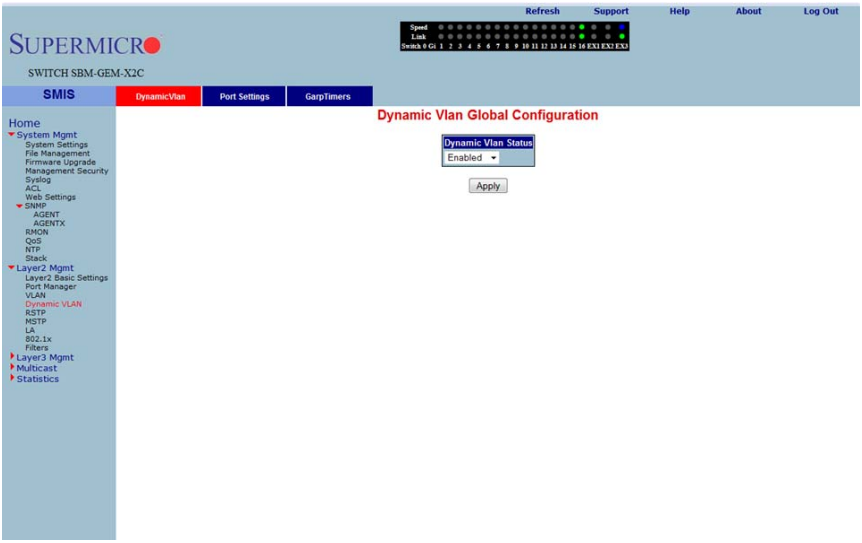
Dynamic Vlan

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 Global Configuration
- Port Configuration
- GARP Timers

Dynamic VLAN Global Configuration

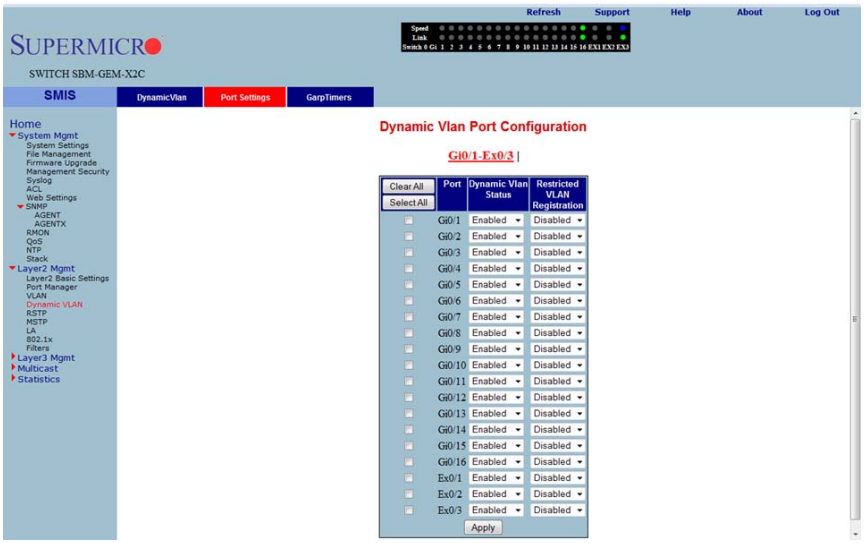
Figure 5-65. Dynamic VLAN Global Configuration Page



Clicking the DYNAMIC VLAN tab brings up the DYNAMIC VLAN GLOBAL CONFIGURATION page (Figure 5-65), which allows you to enable or disable Dynamic VLAN.

Port Configuration

Figure 5-66. Dynamic VLAN Port Configuration Page



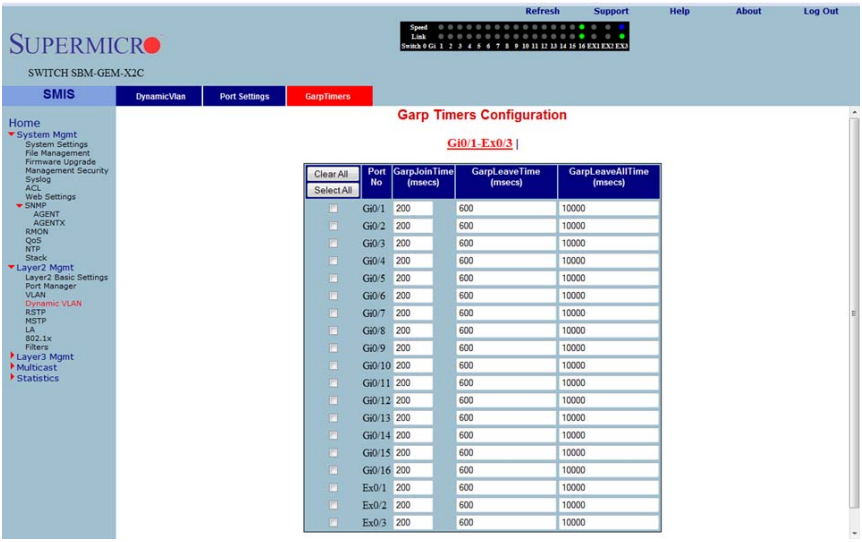
Clicking the PORT SETTINGS link brings up the DYNAMIC VLAN PORT CONFIGURATION page (Figure 5-66), which allows you to configure parameters for Dynamic VLAN ports. The parameters for this page are shown in Table 5-45.

Table 5-45. 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 5-67. Garp Timers Configuration Page



Clicking the GARP TIMERS tab brings up the GARP TIMERS CONFIGURATION page (Figure 5-67), which displays the various parameters for changing Garp times. The parameters for this page are shown in Table 5-46.

Table 5-46. Garp Timers Configuration Page Parameters

Parameter	Description
Port No	This parameter displays the Port Number.
Garp Join Time (msecs)	This parameter allows you to change the Garp Join Time.
Garp Leave Time (msecs)	This parameter allows you to change the Garp Leave Time.
Garp Leave All Time (msecs)	This parameter allows you to change the Garp Leave All Time.

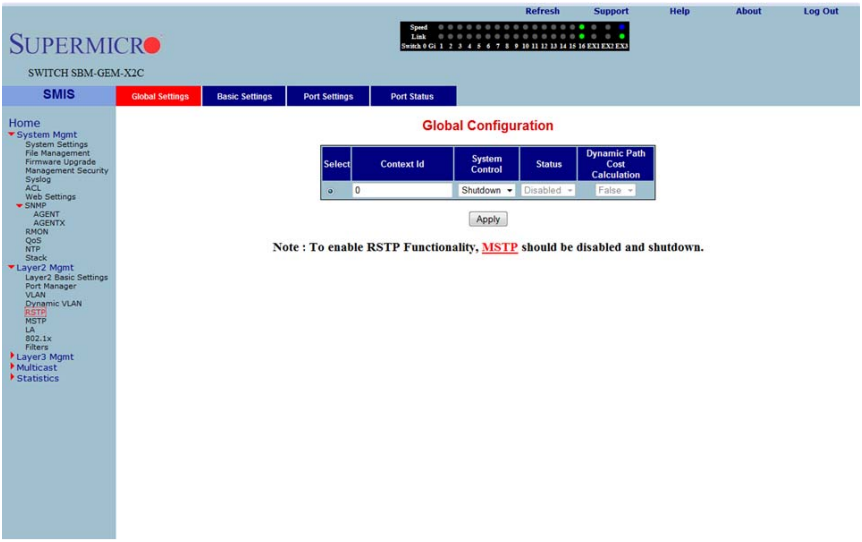
RSTP

The RSTP link provides links to the following configuration pages:

- RSTP Global Settings
- RSTP Basic Settings
- Port Settings
- Port Status

RSTP Global Settings

Figure 5-68. Global Configuration Page



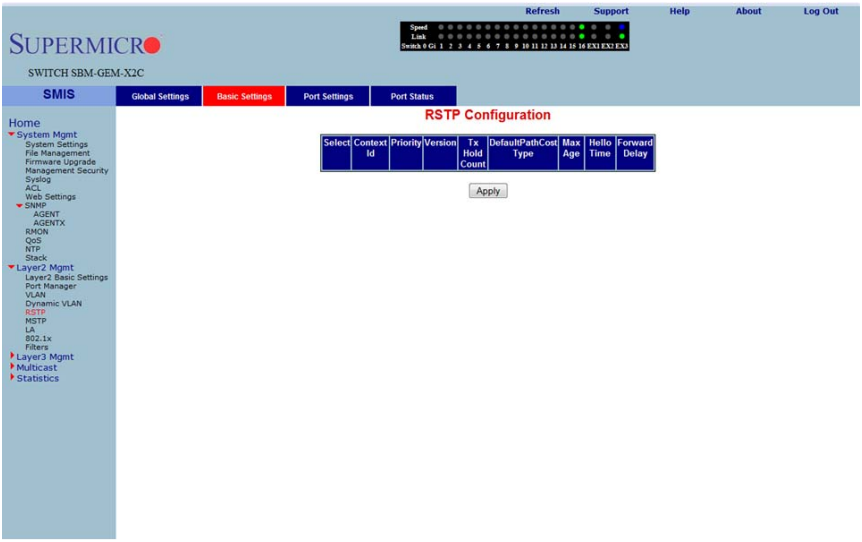
Clicking the GLOBAL SETTINGS tab brings up the GLOBAL CONFIGURATION page (Figure 5-68), which allows you to configure RSTP global parameters. The parameters for this page are shown in Table 5-47.

Table 5-47. Global 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.
System Control	This parameter starts or Shutsdown RSTP in the switch.
Status	This parameter allows you to enable/disable the protocol at a global level on the switch.
Dynamic Path Cost Calculation	This parameter allows you to enable or disable the DYNAMIC PATH COST CALCULATION.

RSTP Basic Settings

Figure 5-69. RSTP Configuration Page



Clicking the BASIC SETTINGS tab brings up the RSTP CONFIGURATION page (Figure 5-69), which displays the various parameters for RSTP configuration. The parameters for this page are shown in Table 5-48.

Table 5-48. 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	
Version	
Tx Hold Count	
Default 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.
Max Age	
Hello Time	
Forward Delay	

Port Settings

Figure 5-70. Port Status Configuration Page

Clicking the PORT SETTINGS tab brings up the PORT STATUS CONFIGURATION page (Figure 5-70), which allows you to set the configuration per port related to RSTP. The parameters for this page are shown in Table 5-49.

Table 5-49. Port Status Configuration Page Parameters

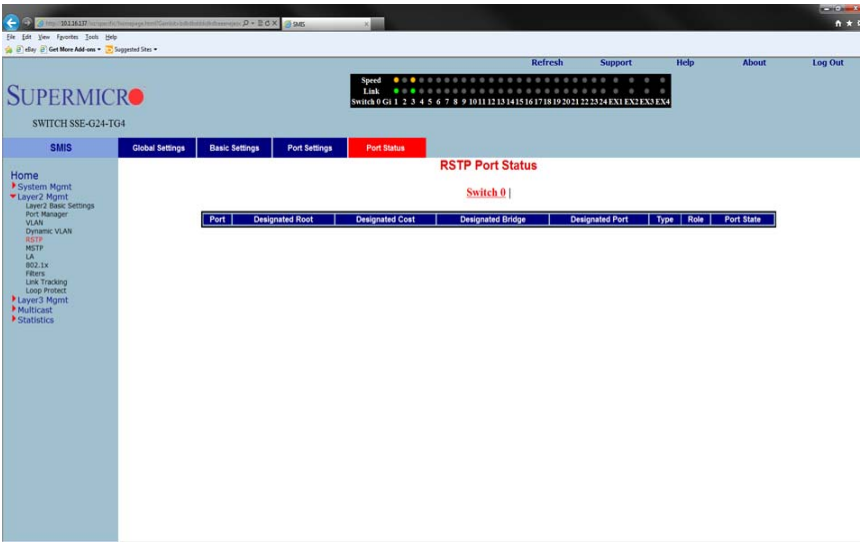
Parameter	Description
Port	This parameter specifies the port identifier.
Port Role	This parameter enables or disables the RSTP protocol status on a particular port.
Port Priority	This parameter specifies the port priority used in role selection.
RSTP Status	
Path Cost	This parameter specifies the path cost associated with this port.
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	
Admin Point-to-Point	This parameter allows you to configure ports explicitly as Point-to-point (Force true), Non-point-to-point or leave the decision to be made Dynamically (from the AL or MAC layer).
Auto Edge Detection	If this parameter is set to true, the edge port status is dynamically calculated.

Table 5-49. Port Status Configuration 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.

Port Status

Figure 5-71. RSTP Port Status Page



Clicking the PORT STATUS tab brings up the RSTP PORT STATUS page (Figure 5-71), which displays RSTP port specific information. The parameters for this page are shown in Table 5-50.

Table 5-50. 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.

Table 5-50. RSTP Port Status Page Parameters (Continued)

Parameter	Description
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*.
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.

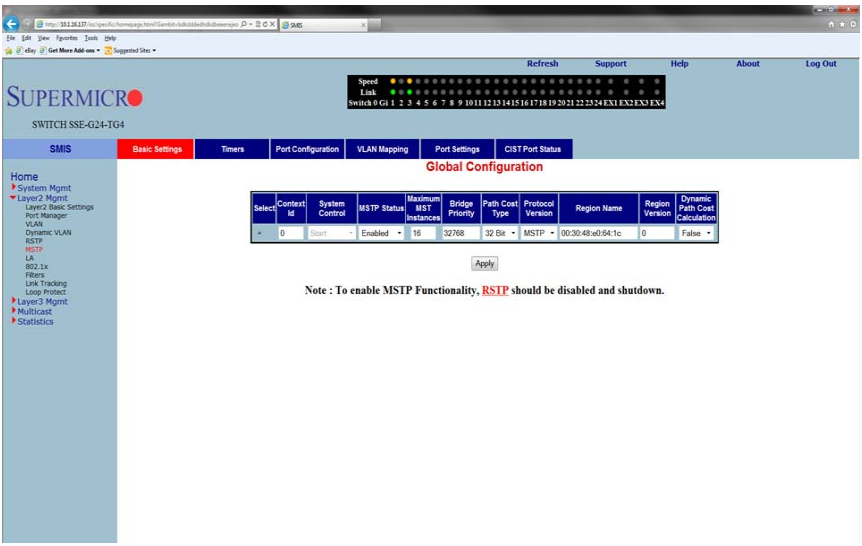
MSTP

The MSTP link leads you to the following configuration pages:

- MSTP Basic Settings–Global Configuration
- MSTP Timers
- Port Configuration
- VLAN Mapping
- Port Settings
- CIST Port Status

MSTP Basic Settings–Global Configuration

Figure 5-72. Global Configuration Page



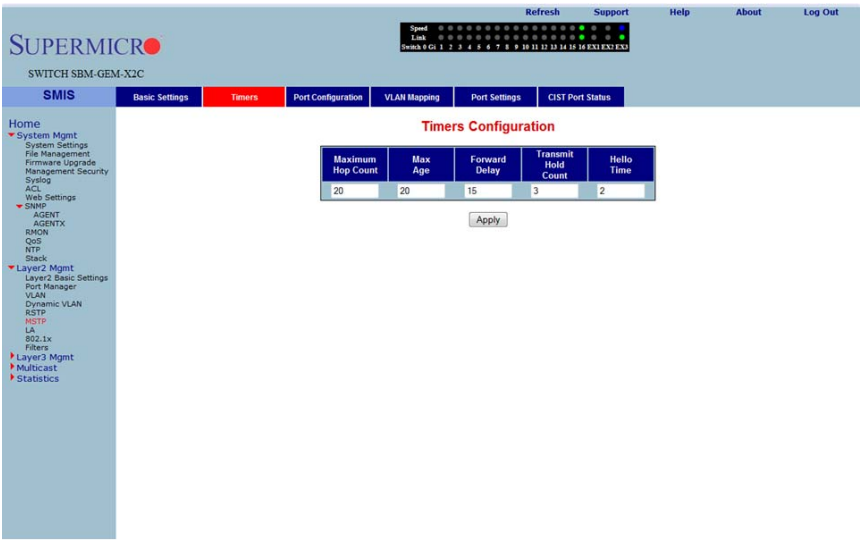
Clicking the BASIC SETTINGS tab brings up the GLOBAL CONFIGURATION page (Figure 5-72), which can access the MSTP global configuration. The parameters for this page are shown in Table 5-51.

Table 5-51. Global Configuration Page Parameters

Parameter	Description
Select	This parameter allows you to select Global Configuration to use in the switch.
Context ID	This parameter shows the unique ID of the Global Configuration.
System Control	This parameter *Starts* or *Shutsdown* MSTP in the switch.
MSTP Status	This parameter specifies the protocol that can be enabled/disabled at a global level on the switch using this field.
Maximum MST Instances	This parameter allows you to specify the maximum MST instances.
Bridge Priority	This parameter specifies the Priority value assigned to the bridge that is used to select the root bridge.
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.
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 number of the configuration to be used.
Dynamic Path Cost Calculation	This parameter allows you to enable or disable the Dynamic Path Cost Calculation.

MSTP Timers

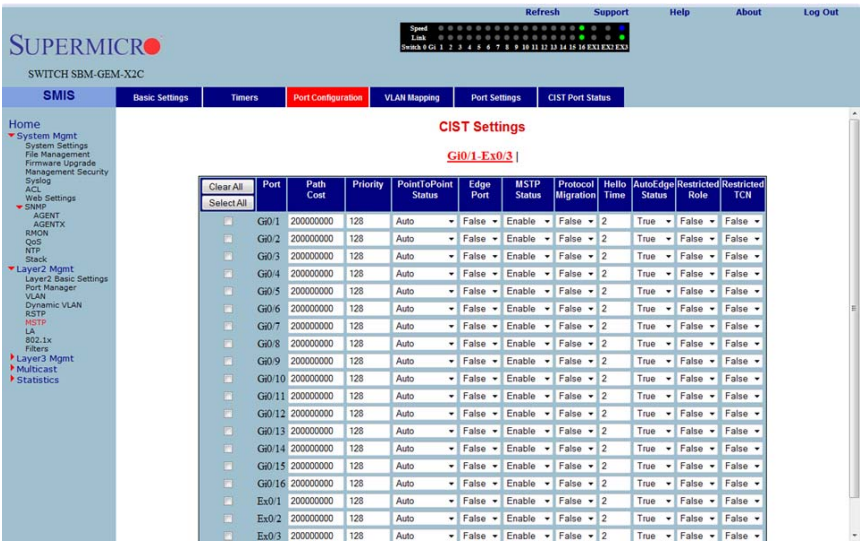
Figure 5-73. Timers Configuration Page



Clicking the TIMERS tab brings up the TIMERS CONFIGURATION page (Figure 5-73), which configures the time for MAXIMUM HOP COUNT, FORWARD DELAY, MAXIMUM AGE, TRANSMIT HOLD AGE and HELLO TIME.

Port Configuration

Figure 5-74. CIST Settings Page



Clicking the PORT CONFIGURATION tab brings up the CIST SETTINGS page (Figure 5-74), which sets the configuration per Port related to MSTP. The parameters for this page are shown in Table 5-52.

Table 5-52. CIST Settings Page Parameters

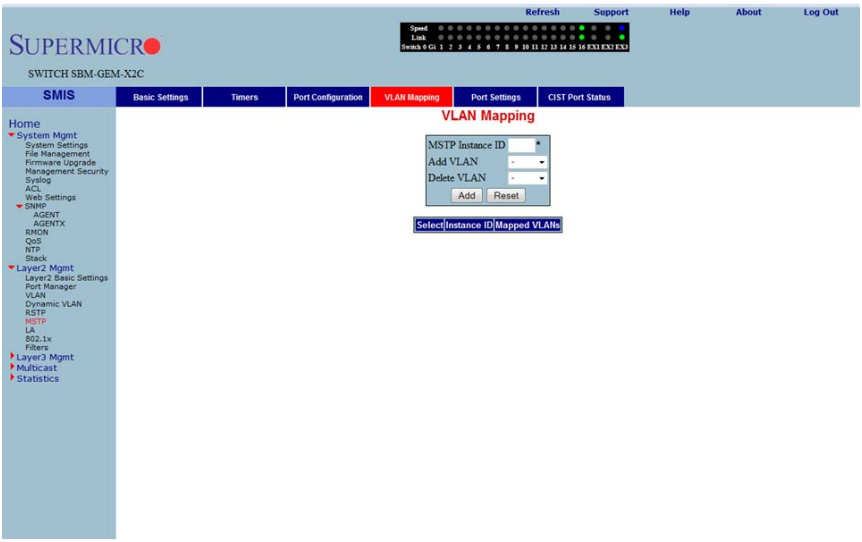
Parameter	Description
Port	This parameter specifies the port identifier.
Admin Status	This parameter specifies the MSTP protocol status that can be enabled/disabled on the particular port.
Priority	This parameter specifies the port priority used in role selection.
Path Cost	This parameter specifies the 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 (*Force* 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 *True*, the edge port status will be dynamically calculated.

Table 5-52. 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 5-75. VLAN Mapping Page



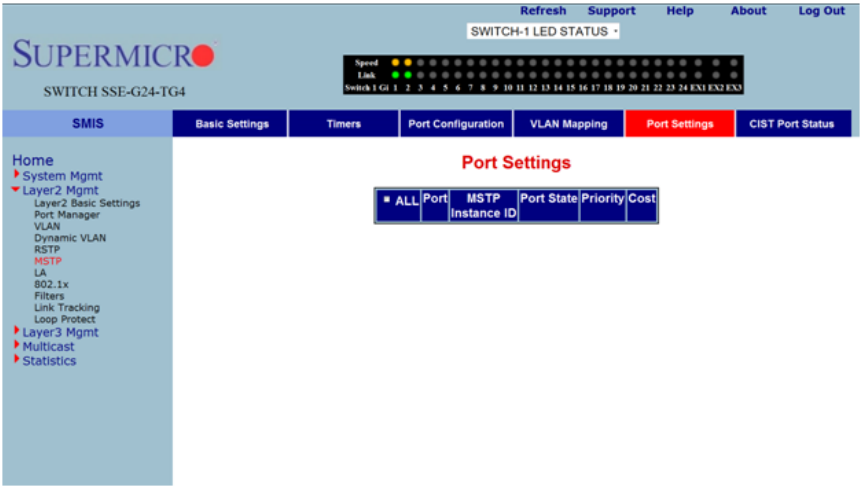
Clicking the VLAN MAPPING tab brings up the VLAN MAPPING page (Figure 5-75), whose table contains one entry for each instance of MSTP. The parameters for this page are shown in Table 5-53.

Table 5-53. VLAN Mapping Page Parameters

Parameter	Description
MSTP Instance ID	This parameter specifies the Instance ID, which is the index of the table.
Map VLAN	This parameter specifies the list of VLANs to be mapped to this instance of the spanning tree.
Unmap VLAN	This parameter specifies the list of VLANs to be unmapped from this instance of the spanning tree.
Select	This control selects the Instance ID from the table.
Instance ID	This shows the Instance ID for each entry in the table.
Mapped VLANs	This shows the Mapped VLANs for each entry in the table.

Port Settings

Figure 5-76. Port Settings Page



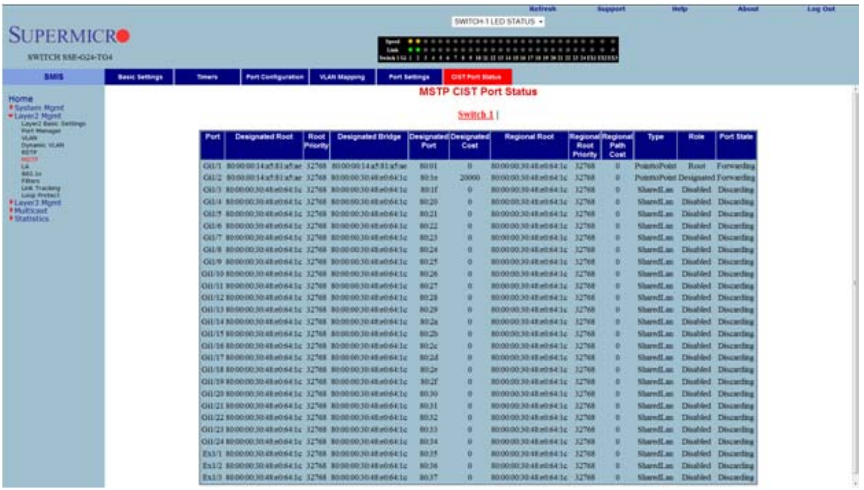
Clicking the PORT SETTINGS tab brings up the PORT SETTINGS page (Figure 5-76), which displays the various parameters for port settings. The parameters for this page are shown in Table 5-54.

Table 5-54. 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 5-77. MSTP CIST Port Status Page



Clicking the CIST PORT STATUS tab brings up the MSTP CIST PORT STATUS page (Figure 5-77), which displays MSTP CIST port specific information. The parameters for this page are shown in Table 5-55.

Table 5-55. MSTP CIST Port Status Page Parameters

Parameter	Description
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 5-55. 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.

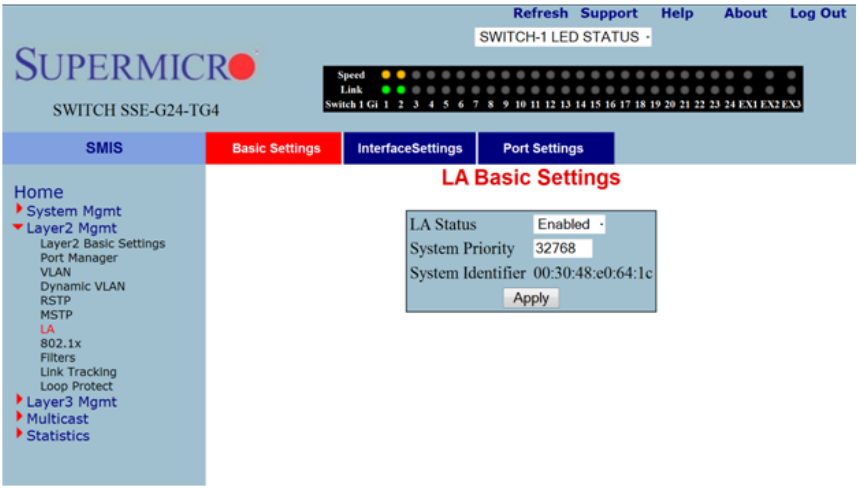
LA

The LA link provides links to the following configuration pages:

- LA Basic Settings
- Interface Settings
- Port Settings

LA Basic Settings

Figure 5-78. LA Basic Settings Page



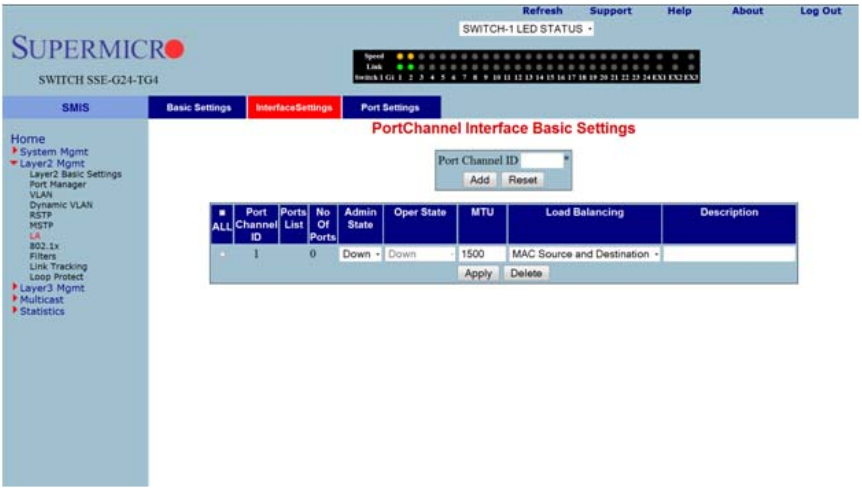
Clicking the BASIC SETTINGS tab brings up the LA BASIC SETTINGS page (Figure 5-78), which displays the various parameters for LA basic settings. The parameters for this page are shown in Table 5-56.

Table 5-56. 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.
System ID	This parameter specifies the Bridge MAC Address that is displayed. This is a read-only parameter.

Interface Settings

Figure 5-79. Port Channel Interface Basic Settings Page



Clicking the INTERFACE SETTINGS tab brings up the PORT CHANNEL INTERFACE BASIC SETTINGS page (Figure 5-79), which allows you to configure port channels. The parameters for this page are shown in Table 5-57.

Table 5-57. Port Channel Interface Basic Settings Page Parameters

Parameter	Description
Port Channel ID	This parameter specifies the identifier of the port channel interface. The valids values are between *1* to *65535*.

Port Settings

Figure 5-80. LA Port Settings Page

Clicking the PORT SETTINGS tab brings up the LA PORT SETTINGS page (Figure 5-80), which configures LA properties at a per-port level. The parameters for this page are shown in Table 5-58.

Table 5-58. LA Port Settings Page Parameters

Parameter	Description
Port	This parameter specifies the Interface Index.
Port Channel	
Mode	This parameter specifies the various port modes, such as *LACP*, *Manual* or *Disable*.
Port Priority	This parameter specifies the priority value of the Port.
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 *Long* timeout is chosen then the ports will time out of the Port Channel in 90-seconds. If a *Short* 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.
Port State	
Aggregation State	

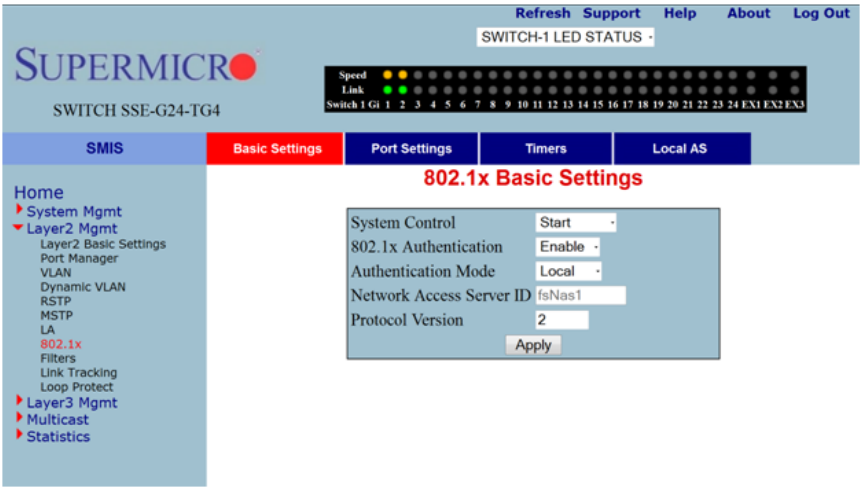
802.1x

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 5-59.

Table 5-59. 802.1x Basic Settings Page Parameters

Parameter	Description
System Control	This parameter starts or shutsdown 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 *Remote* or *Local*.
Network Access Server ID	This parameter specifies the Authenticator ID, which originates the Access-Request Packets.
Protocol Version	

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 5-60.

Table 5-60. 802.1x Port Settings Page Parameters

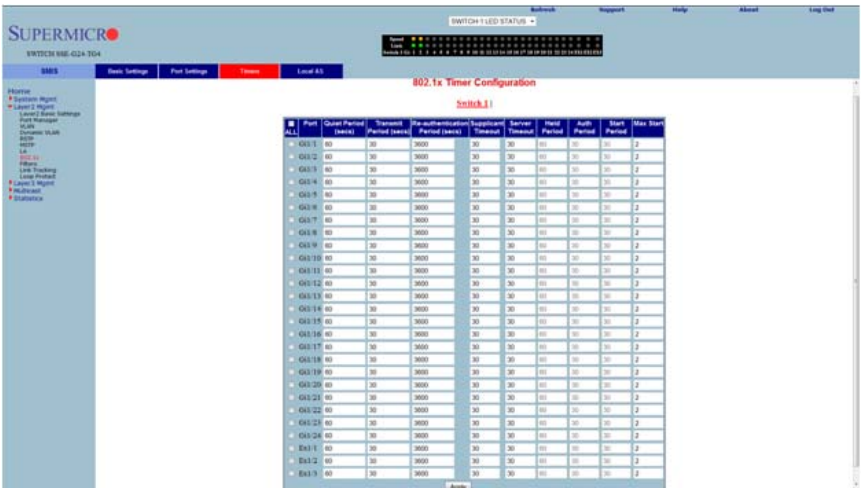
Parameter	Description
Port	This parameter specifies the Index of the port for which its fields (such as PORT CONTROL, PORT AUTHORIZATION STATUS, and so on) are configured.
Port Control	This parameter specifies the control values of the Authenticator Port. The control values can be: • **Force Authorize** - All the traffic through this port will be allowed always. • **Force Unauthorize** - All the traffic through this port will be blocked always. • **Auto** - The 802.1x authentication process will be imposed over this port.
Port Authorization Status	This parameter specifies current status of the port either as *Authorized* or *Un-Authorized*.
Authentication Mode	This parameter specifies the configuration for selecting the AUTHENTICATION MODE to be *Port Based*.
Admin Control Direction	This parameter specifies whether security is to be imposed for • **In** - the incoming traffic • **Both** - both incoming and outgoing traffic
Operational Control Direction	This parameter specifies the current security status.

Table 5-60. 802.1x Port Settings Page Parameters (Continued)

Parameter	Description
Port Initialize	This parameter specifies the initialization control for the port. Setting this value to *True* causes the port to be initialized. The value reverts to *False* once initialization is complete.
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.
Reauthentication	This parameter provides configuration to enable or disable the reauthentication mechanism on the port.

Timers

Figure 5-83. 802.1x Timer Configuration Page



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 5-61. 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.

Table 5-61. 802.1x Timer Configuration Page Parameters (Continued)

Parameter	Description
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.
Re-authentication Period (Seconds)	This parameter specifies the time between periodic re-authentication of the supplicant.

Local AS

Figure 5-84. Local Authentication Server Configuration Page

Clicking the LOCAL AS tab brings up the LOCAL AUTHENTICATION SERVER CONFIGURATION page (Figure 5-21), which configures Local Authentication Server information. The parameters for this page are shown in Table 5-12.

Table 5-62. 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.

Table 5-62. Local Authentication Server Configuration Page Parameters (Continued)

Parameter	Description
Permission	This parameter represents the allowance and denial of access. The values that can be configured are: • **Allow** - When set to *Allow*, the authentication request is allowed over the set of ports in the PORT LIST. • **Deny** - When set to *Deny*, 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.

Table 5-63. MAC Session Info Page Parameters

Parameter	Description
Session Intialize	This parameter is the initialization control for this Supplicant MAC address. Setting this attribute to *True* causes the Supplicant session with this MAC address, to be initialized. The attribute value reverts to *False* once initialization has completed.
Session ReAuthenticate	This parameter is the reauthentication control for this Supplicant MAC address. Setting this attribute to *True* causes the Authenticator PAE state machine for this MAC address to reauthenticate the Supplicant. Setting this attribute to *False* has no effect. This attribute always returns to *False* when it is read.

Filters

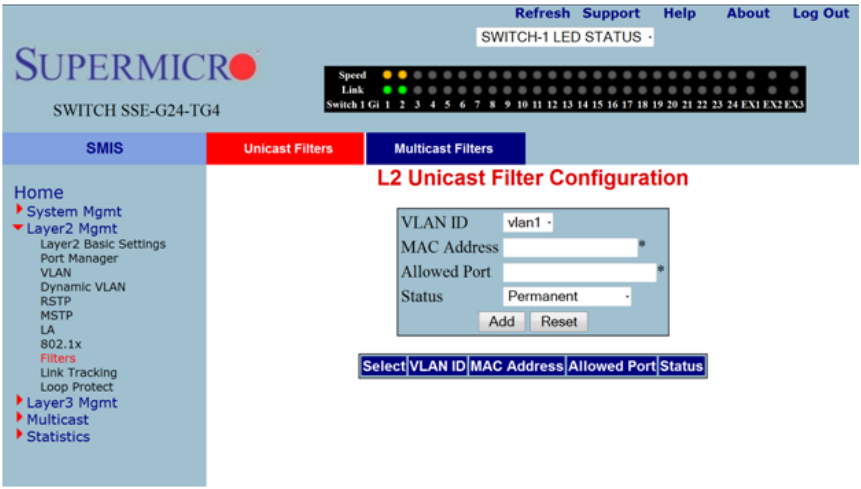
The Filters link allows you to configure Layer 2 packet filtering.

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 5-21), 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 5-64. L2 Unicast Filter Configuration Page Parameters

Parameter	Description
FDB ID	This parameter specifies the forwarding database ID.
MAC Address	This parameter specifies the destination MAC address of the received packet.
Receive Port	This parameter specifies the port on which the packet was received.
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: • **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

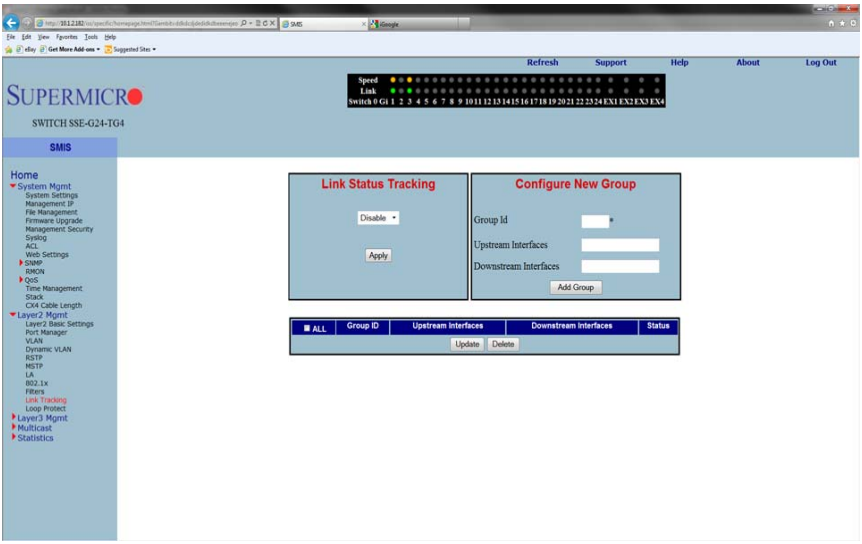
Clicking the MULTICAST FILTERS tab brings up the L2 MULTICAST FILTER CONFIGURATION page (Figure 5-21), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-12.

Table 5-65. 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: • **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.

Line Tracking

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



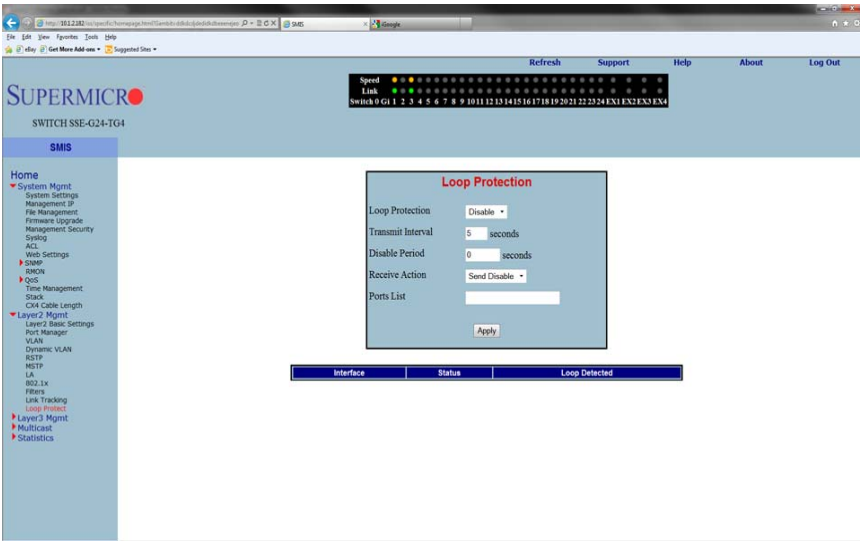
Clicking the LINK TRACKING link brings up the LINK STATUS TRACKING/CONFIGURE NEW GROUP page (Figure 5-87), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-66.

Table 5-66. 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.

Loop Protect

Figure 5-88. Loop Protection Page



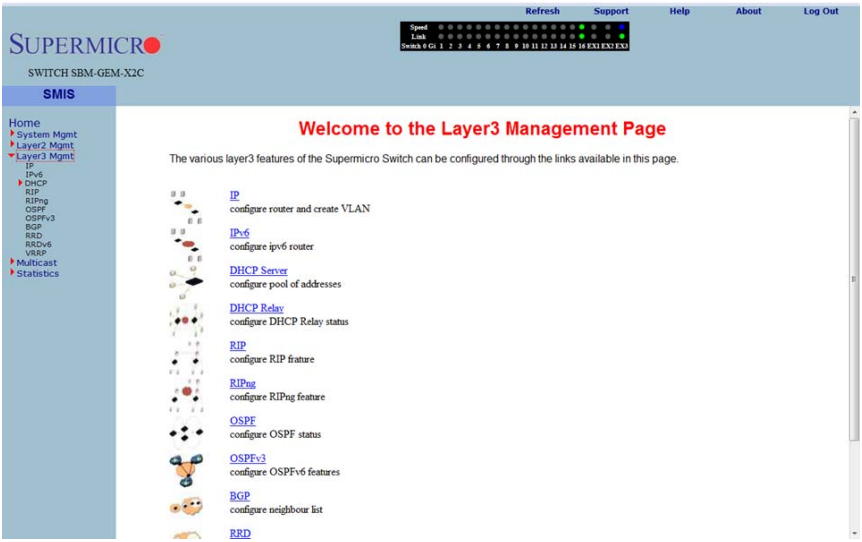
Clicking the LOOP PROTECT link brings up the LOOP PROTECTION page (Figure 5-88), which allows you to set the filter configuration to control the multicast packets that the switch needs to process. The parameters for this page are shown in Table 5-67.

Table 5-67. Loop Protection Page Parameters

Parameter	Description
Loop Protection	This parameter allows you to ENABLE and DISABLE Loop Protection.
Transmit Interval	This parameter allows to set the time interval in seconds.
Disable Period	This Parameter allows to set the disable period in seconds.
Receive Action	This parameter allows to SEND DISABLE or NO DISABLE a received action.
Ports List	This parameter allsows to specify the ports list.

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

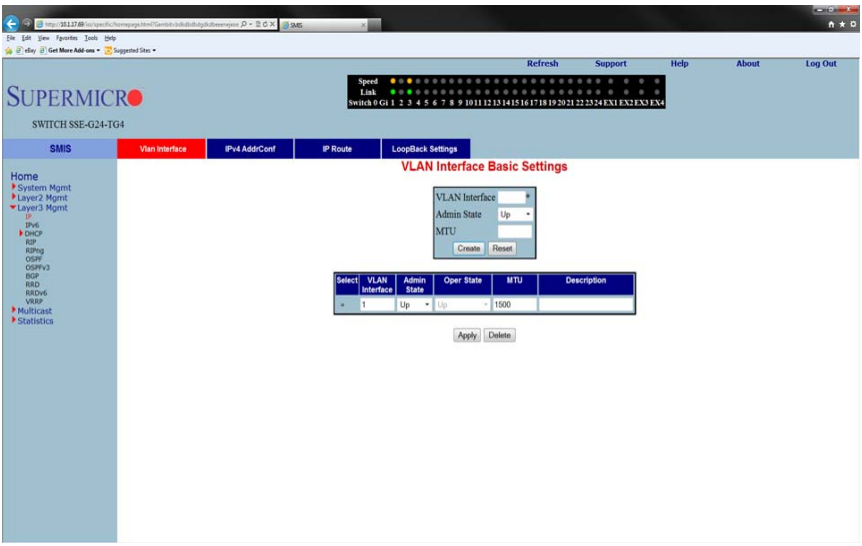
IP

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 Basic 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 5-68.

Table 5-68. VLAN Interface Basic Settings Page Parameters

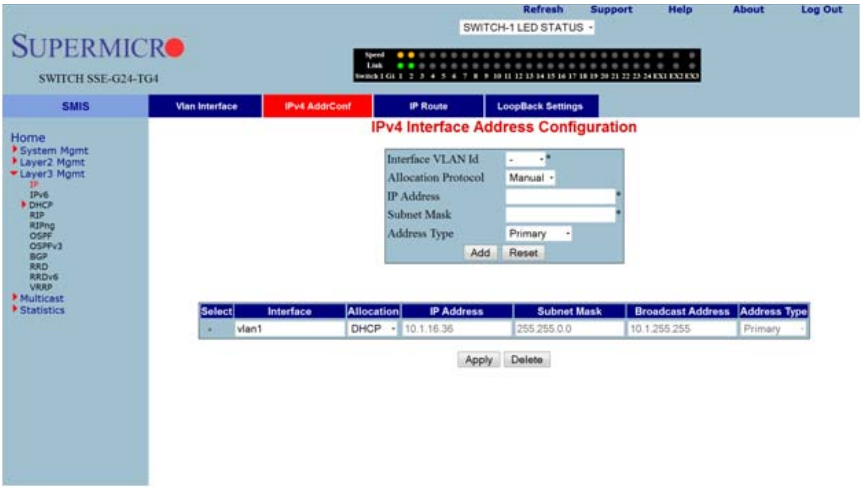
Parameter	Description
VLAN Interface	This parameter specifies the VLAN identifier.
Admin State	This parameter specifies the admin state as either *Up* or *Down*.
MTU	This parameter specifies the maximum transfer unit size in bytes.
Select	

Table 5-68. VLAN Interface Basic Settings Page Parameters (Continued)

Parameter	Description
Oper State	
Description	

IPv4 AddrConf

Figure 5-91. IPv4 Address Configuration Page



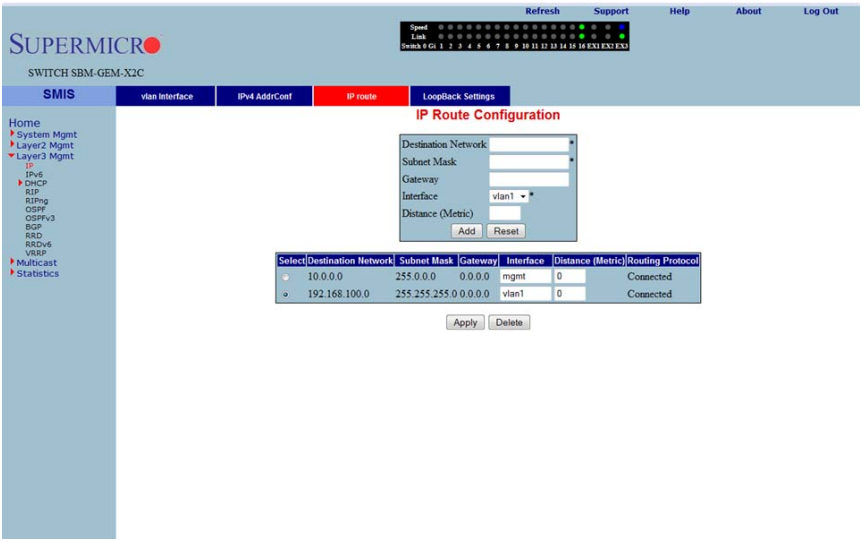
Clicking the IPv4 ADDR CONF tab brings up the IPv4 ADDRESS CONFIGURATION page (Figure 5-91), which allowsyou to configure the IP address for L3 VLANs. The parameters for this page are shown in Table 5-69.

Table 5-69. IPv4 Address Configuration Page Parameters

Parameter	Description
Interface VLAN ID	This parameter specifies the VLAN interface.
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 *Primary* or *Secondary*.

IP Route

Figure 5-92. IP Route Configuration Page



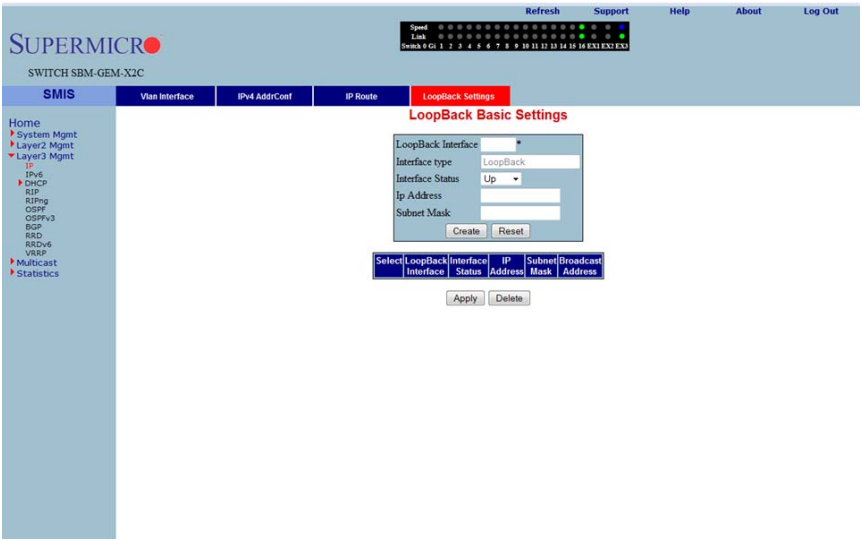
Clicking the IP ROUTE tab brings up the IP ROUTE CONFIGURATION page (Figure 5-92), which allows you to configure the static IP routes. The parameters for this page are shown in Table 5-70.

Table 5-70. 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 Basic Settings

Figure 5-93. LoopBack Basic Settings Page



Clicking the LOOPBACK SETTINGS tab brings up the LOOPBACK BASIC SETTINGS page (Figure 5-93), which allows you to configure loopback IP interfaces. The parameters for this page are shown in Table 5-71.

Table 5-71. 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 *Up* or *Down*.
IP Address	This parameter specifies the IP address for this loopback interface.
Subnet Mask	This parameter specifies the subnet mask for this loopback interface.

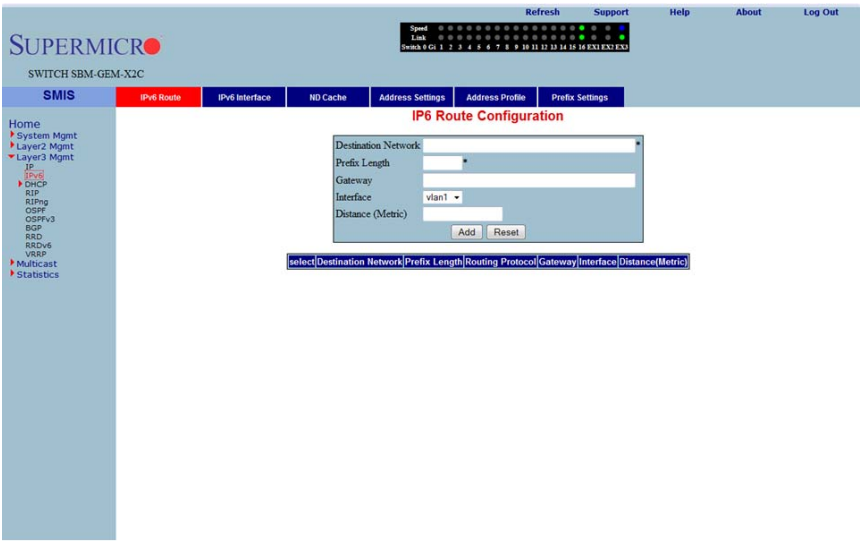
IP V6

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

- IPv6 Route Configuration
- IPv6 Interface
- ND Cache
- Address Settings
- Address Profile
- Prefix Settings

IPv6 Route Configuration

Figure 5-94. IP6 Route Configuration Page



Clicking the IPv6 ROUTE tab brings up the IP6 ROUTE CONFIGURATION page (Figure 5-94), which configures various IP6 Route parameters. The parameters for this page are shown in Table 5-72.

Table 5-72. IP6 Route Configuration Page Parameters

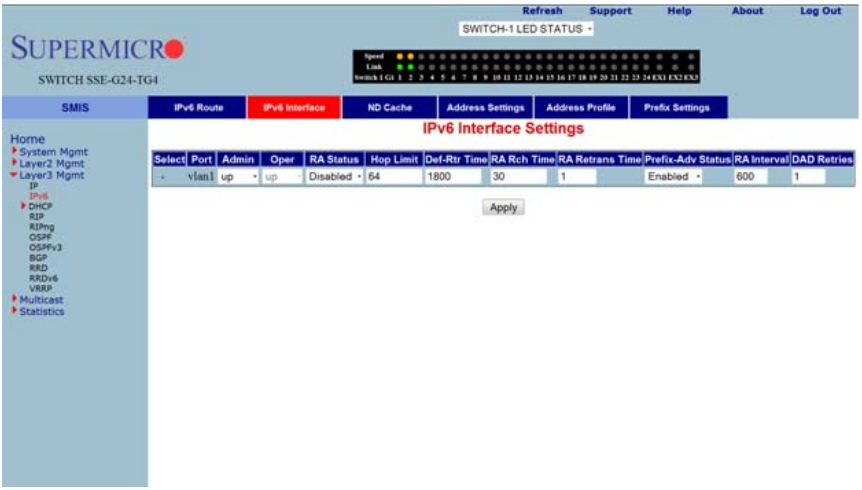
Parameter	Description
Destination Network	This parameter specifies the network address for which the IPv6 route is being added.
Prefix Length	This parameter specifies the subnet mask for the above said address.

Table 5-72. IP6 Route Configuration Page Parameters (Continued)

Parameter	Description
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.

IPv6 Interface

Figure 5-95. IPv6 Interface Settings Page



Clicking the IPv6 INTERFACE tab brings up the IPv6 INTERFACE SETTINGS page (Figure 5-95), which displays the various parameters for the IPv6 Interface. The parameters for this page are shown in Table 5-73.

Table 5-73. IPv6 Interface Settings Page Parameters

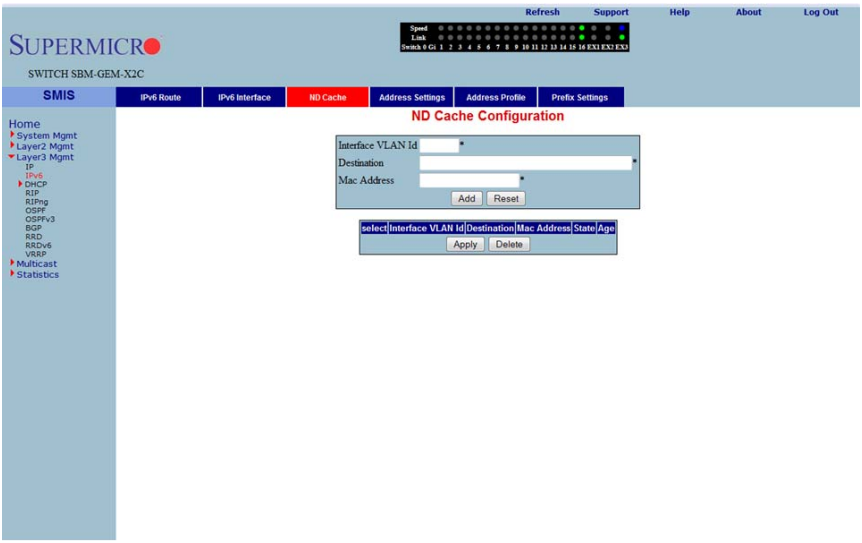
Parameter	Description
Port	This parameter specifies the Index of the VLAN interface.
Admin	This parameter indicates the Administrative Status of IPv6 on the Interface.
Oper	This parameter specifies the Operational Status of IPv6 on the given Interface, which is a read-only field.
RA Status	This parameter indicates the Router Advertisement status on the Interface.
Hop Limit	This parameter denotes the Hop Limit value to be placed in the Router Advertisements sent on the Interface.
Def-Rtr Time	This parameter specifies the Default router lifetime to be placed in the Router Advertisements sent on the interface.

Table 5-73. IPv6 Interface Settings Page Parameters (Continued)

Parameter	Description
RA Rch Time	This parameter indicates the Reachable time to be placed in the Router Advertisements sent on the interface.
RA Retrans Time	This parameter specifies the RA Retransmit time to be placed in the Router Advertisement sent on the interface.
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.
DAD Retries	This parameter specifies the maximum number of Duplicate Address Detection retries.

ND Cache

Figure 5-96. ND Cache Configuration Page



Clicking the ND CACHE tab brings up the ND CACHE CONFIGURATION page (Figure 5-96). The parameters for this page are shown in Table 5-74.

Table 5-74. ND Cache Configuration Page Parameters

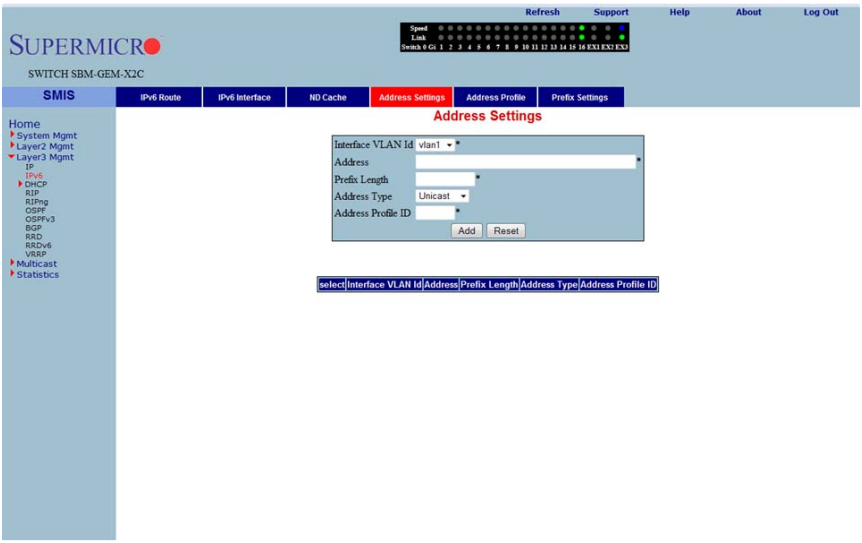
Parameter	Description
Interface VLAN ID	This parameter indicates index of the VLAN interface.
Destination	This parameter specifies Destination IPv6 address.
MAC Address	This parameter denotes the physical address of the Destination address.

Table 5-74. ND Cache Configuration Page Parameters (Continued)

Parameter	Description
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 5-97. Address Settings Page



Clicking the ADDRESS SETTINGS tab brings up the ADDRESS SETTINGS page (Figure 5-97), which allows you to configure address settings for IPv6. The parameters for this page are shown in Table 5-75.

Table 5-75. 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.
Prefix Length	This parameter indicates the length of the prefix (in bits) associated with this entry's IPv6 address.
Address Type	This parameter specifies that the type of address can be Link-*Local*, Global-*Unicast* or *Anycast*.
Address Profile ID	This parameter indicates the index to the IPv6 address Profile table.

Address Profile

Figure 5-98. Address Profile Settings Page

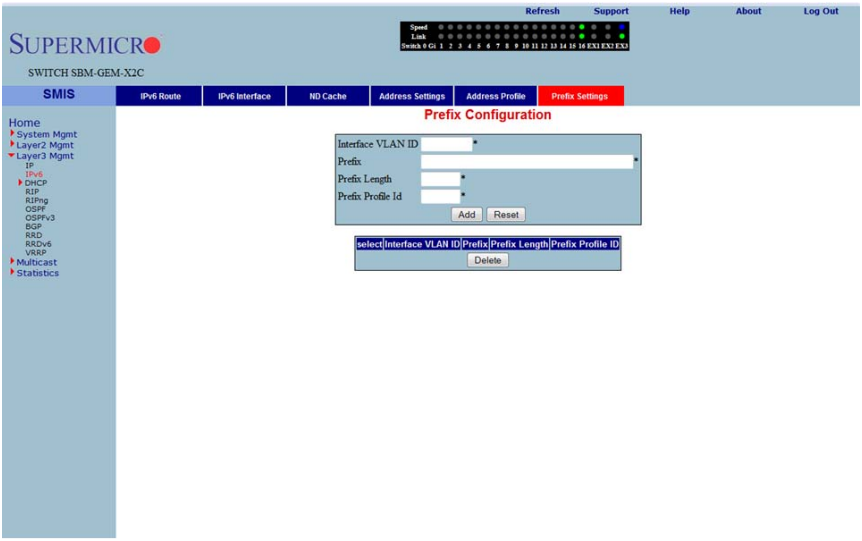
Clicking the ADDRESS PROFILE tab brings up the ADDRESS PROFILE SETTINGS page (Figure 5-98). The parameters for this page are shown in Table 5-76.

Table 5-76. 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.
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.
Valid Time	This parameter indicates the Valid Lifetime of the prefix address that uses this profile.
Valid Flag	This parameter specifies if the Valid Lifetime Flag is *Variable* or *Fixed*.
Preferred Flag	This parameter specifies if the Preferred Lifetime Flag is *Variable* or *Fixed*.

Prefix Settings

Figure 5-99. Prefix Configuration Page



Clicking the PREFIX SETTINGS tab brings up the PREFIX CONFIGURATION page (Figure 5-99). The parameters for this page are shown in Table 5-77.

Table 5-77. Prefix Configuration Page Parameters

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

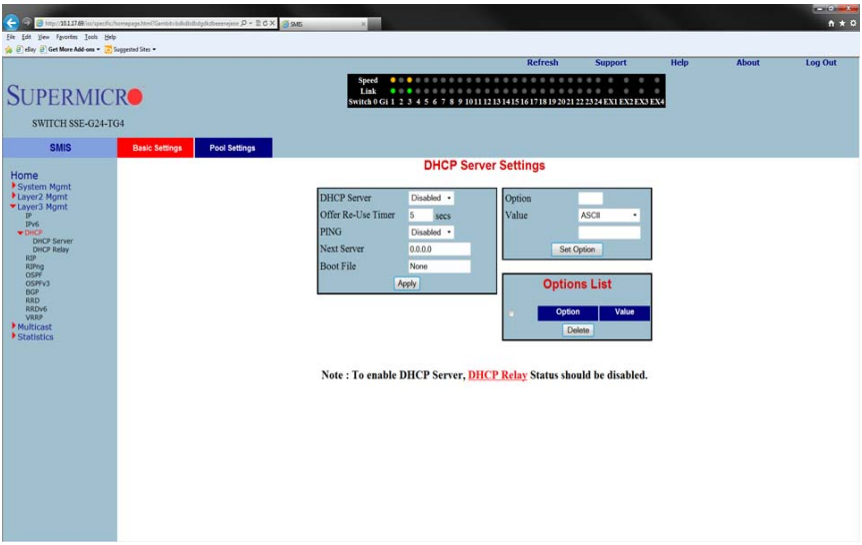
DHCP Server

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

- DHCP Basic Settings
- Pool Settings

DHCP Basic Settings

Figure 5-100. DHCP Server Settings Page



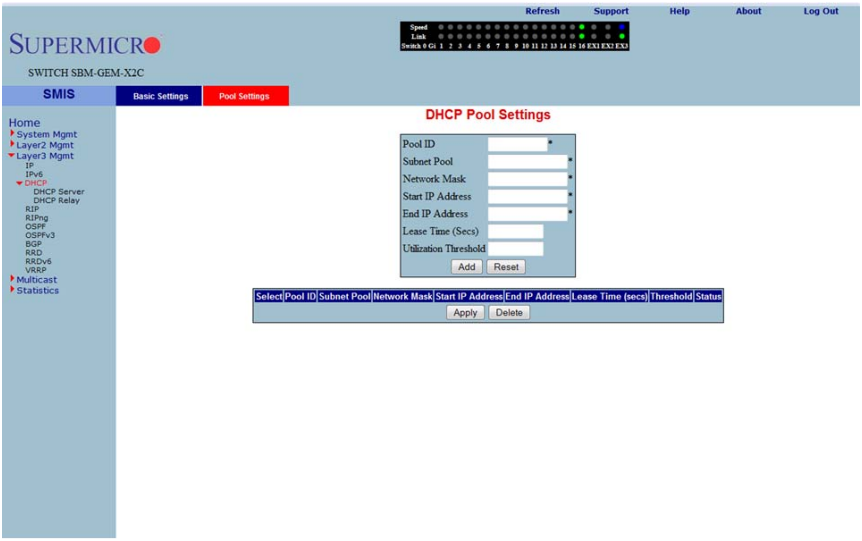
Clicking the DHCP SETTINGS tab brings up the DHCP SERVER SETTINGS page (Figure 5-100). The parameters for this page are shown in Table 5-78.

Table 5-78. 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.
ICMP Echo	This parameter enables or disables the ICMP Echo feature.

Pool Settings

Figure 5-101. DHCP Pool Settings Page



Clicking the POOL SETTINS link brings up the DHCP POOL SETTINGS page (Figure 5-101), 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 5-79.

Table 5-79. DHCP Pool Settings Page Parameters

Parameter	Description
Pool ID	This parameter specifies the pool ID to index among the different subnet pools configured.
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.
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.
Status	This parameter specifies the status of the entry.

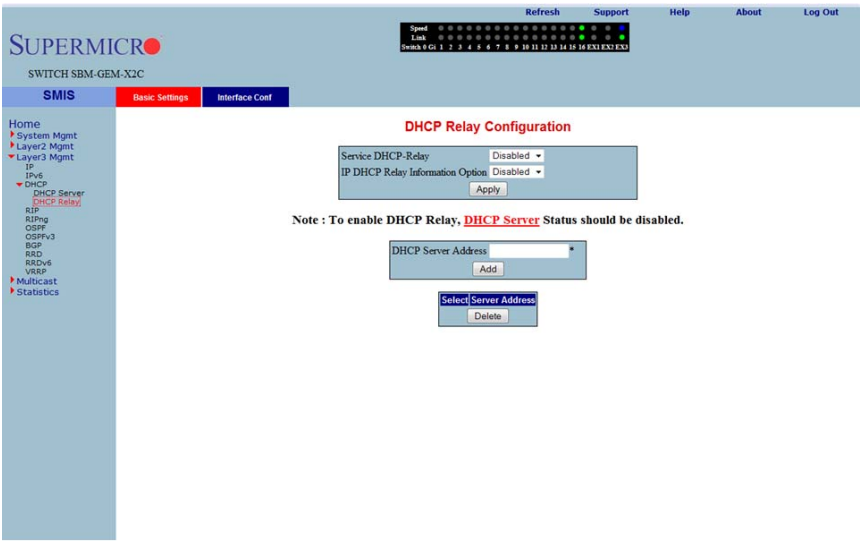
DHCP Relay

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

- DHCP Relay Basic Settings
- Interface Settings

DHCP Relay Basic Settings

Figure 5-102. DHCP Relay Configuration Page



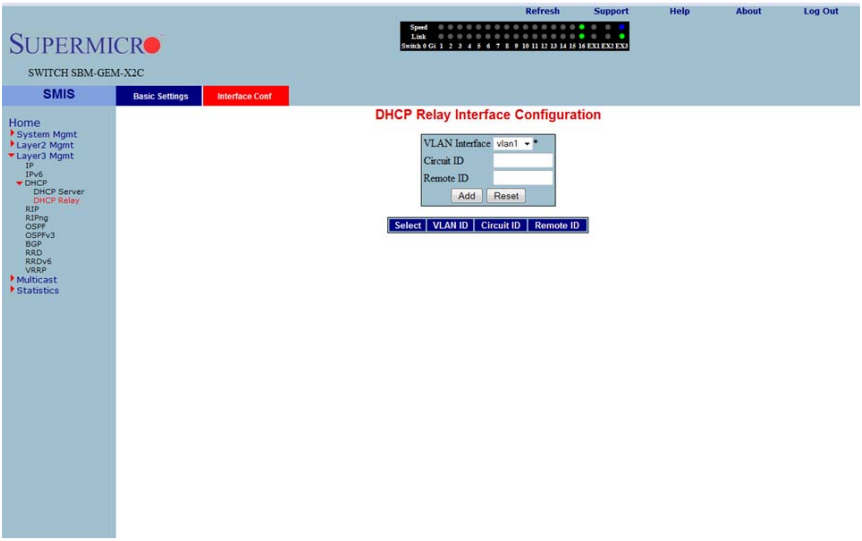
Clicking the BASIC SETTINGS tab brings up the DHCP RELAY CONFIGURATION page (Figure 5-102), which displays the various parameters for configuring the DHCP relay. The parameters for this page are shown in Table 5-80.

Table 5-80. 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 Settings

Figure 5-103. DHCP Relay Interface Configuration Page



Clicking the INTERFACE CONF tab brings up the DHCP RELAY INTERFACE CONFIGURATION page (Figure 5-103), which allows you to configure the DHCP relay for VLANs. The parameters for this page are shown in Table 5-81.

Table 5-81. 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 identifer.
Remote ID	This parameter specifies the Remote identifer.

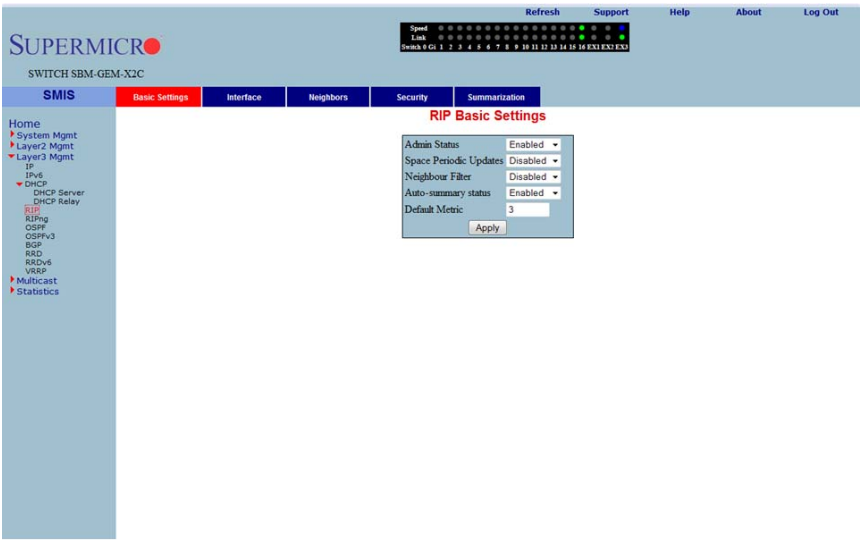
RIP

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

- RIP Basic Settings
- Interfaces
- Neighbors List
- Security Settings
- Address Summarization

RIP Basic Settings

Figure 5-104. RIP Basic Settings Page



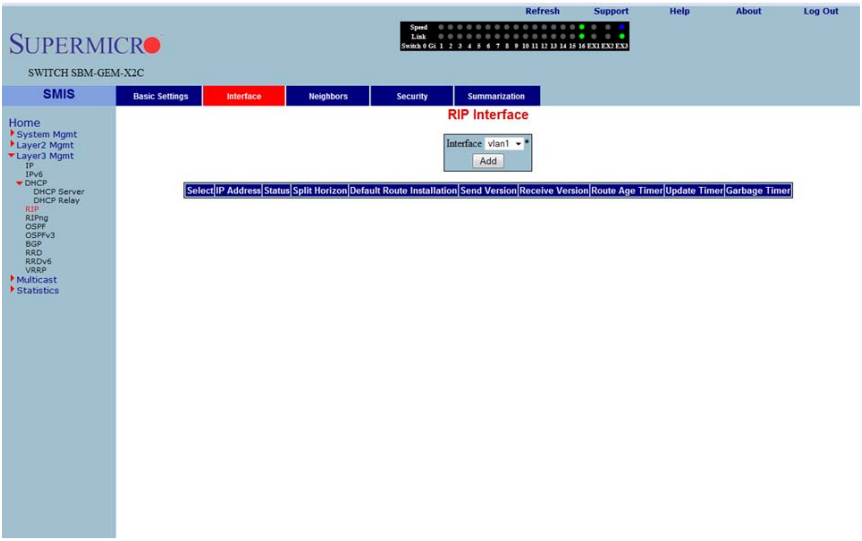
Clicking the BASIC SETTINGS tab brings up the RIP BASIC SETTINGS page (Figure 5-104). The parameters for this page are shown in Table 5-82.

Table 5-82. RIP Basic Settings Page Parameters

Parameter	Description
Output-delay	This parameter specifies the delay that needs to be enabled for RIP to split the periodic update packets before they are sent out.
Neighbor Filter	This parameter enables or disables neighbor filtering. Neighbor filtering helps you to filter routes from specific neighbors.
Auto-summary status	This parameter enables or disables the Auto-summary feature.

Interfaces

Figure 5-105. RIP Interface Page



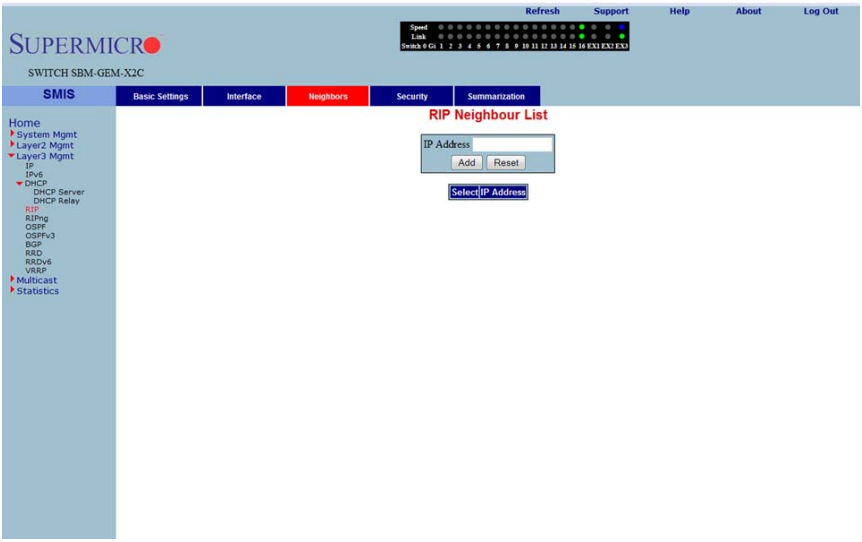
Clicking the INTERFACE tab brings up the RIP INTERFACE page (Figure 5-105). The parameters for this page are shown in Table 5-83.

Table 5-83. 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 *RIPV1*, *RIP1 Compatible* or *RIPv2*.
Receive Version	This parameter is similar to SEND VERSION, but it allows you to choose the RIP packets to be received as either *RIPV1, RIPV2*, both *RIPv1 and RIPv2* or *None*.
Route Age Timer	This parameter specifies the time interval after which the routes will be flushed.
Update Timer	This parameter specifies the time interval between successive RIP updates.
Garbage Timer	This parameter specifies the time interval after which the invalid routes will be removed from the routing table.

Neighbors List

Figure 5-106. RIP Neighbor List Page

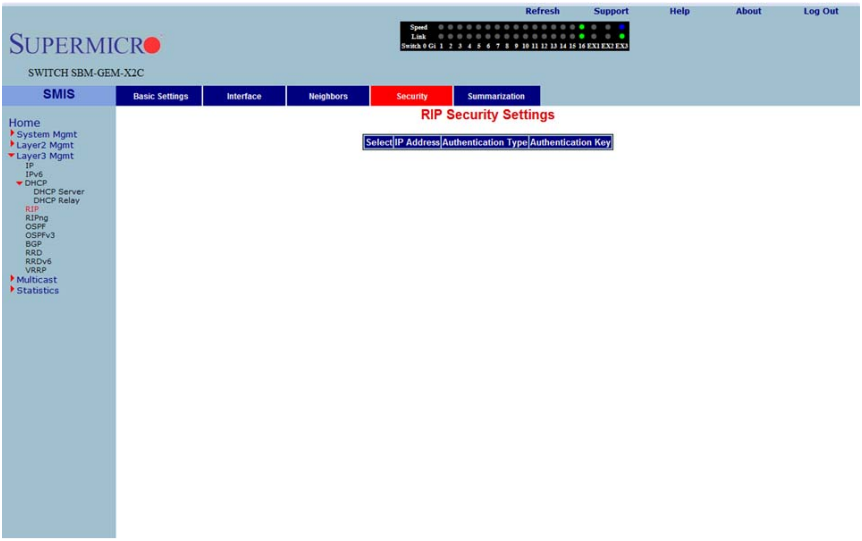


Clicking the NEIGHBORS tab brings up the RIP NEIGHBOR LIST page (Figure 5-106), which is used to configure the RIP neighbors, by configuring their IP address.

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 Settings

Figure 5-107. RIP Security Settings Page



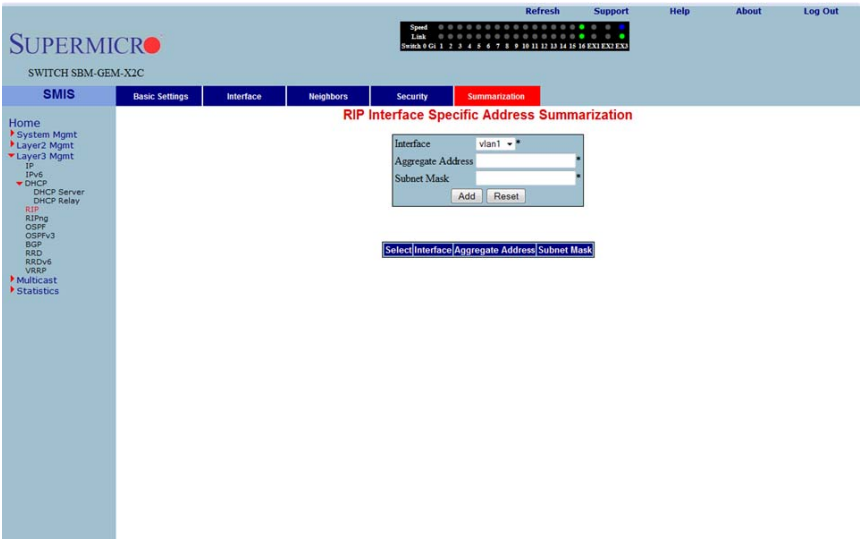
Clicking the SECURITY tab brings up the RIP SECURITY SETTING page (Figure 5-107). The parameters for this page are shown in Table 5-12.

Table 5-84. 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 *No Authentication*, or *Simple Password*, or the *md5* authentication type.
Authentication Key	This parameter specifies the key used for authentication if the authentication type is other than *No Authentication*.

Address Summarization

Figure 5-108. RIP Interface Specific Address Summarization Page



Clicking the SUMMARIZATION tab brings up the RIP INTERFACE SPECIFIC ADDRESS SUMMARIZATION page (Figure 5-108). The parameters for this page are shown in Table 5-85.

Table 5-85. 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.

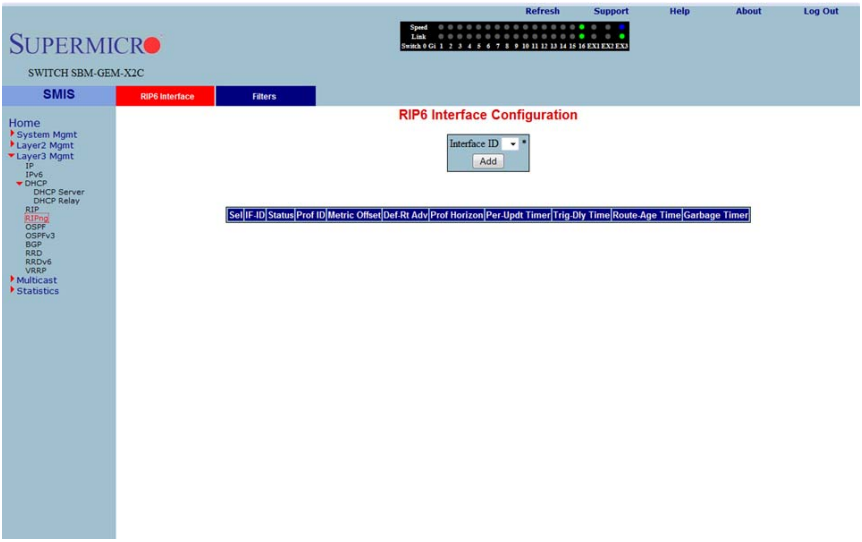
RIPng

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 5-109. RIP6 Interface Configuration Page



Clicking the RIP6 INTERFACE tab brings up the RIP6 INTERFACE CONFIGURATION page (Figure 5-109). The parameters for this page are shown in Table 5-86.

Table 5-86. RIP6 Interface Configuration Page Parameters

Parameter	Description
Interface ID	Specifies the Interface Id for which RIPv6 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 RIP6 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 5-110. RIP6 Filter Configuration Page

Clicking the FILTERS tab brings up the RIP6 FILTER CONFIGURATION page (Figure 5-110). The parameters for this page are shown in Table 5-87.

Table 5-87. 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.

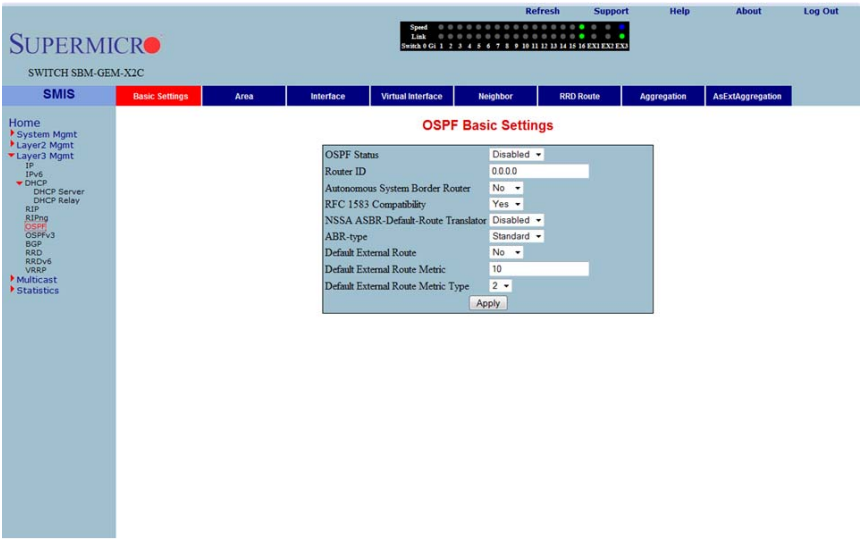
OSPF

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

- OSPF Basic Settings
- Area
- Interface
- Virtual Interface
- OSPF Neighbor
- OSPF RRD Route Configuration
- OSPF Area Aggregation
- External Aggregation

OSPF Basic Settings

Figure 5-111. OSPF Basic Settings Page



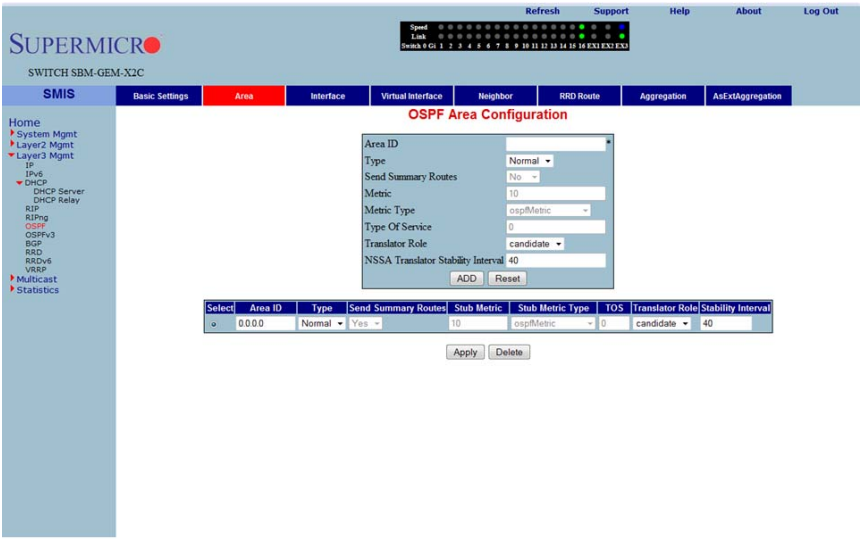
Clicking the BASIC SETTINGS tab brings up the OSPF BASIC SETTINGS page (Figure 5-111). The parameters for this page are shown in Table 5-88.

Table 5-88. 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.
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 5-112. OSPF Area Configuration Page



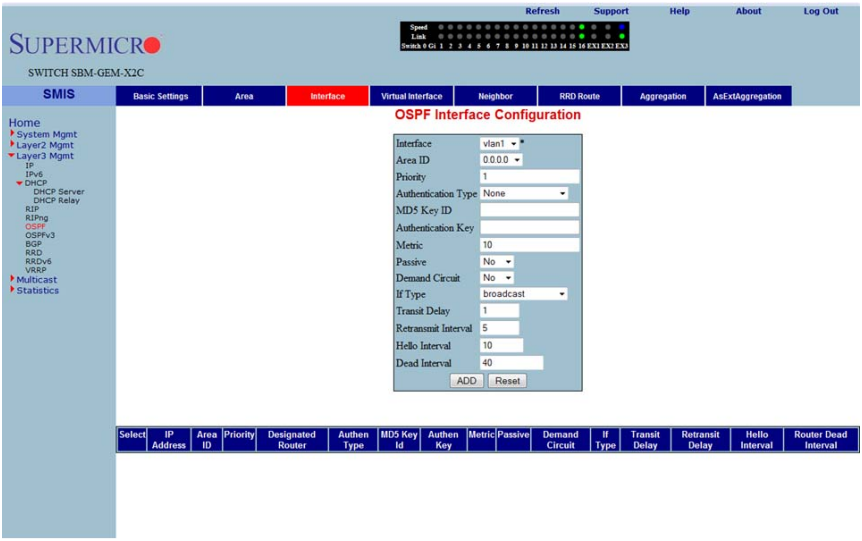
Clicking the AREA tab brings up the OSPF AREA CONFIGURATION page (Figure 5-112). The parameters for this page are shown in Table 5-89.

Table 5-89. 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 *Stub* area, a *Normal* area or *NSSA*.
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.
Default Cost	This parameter specifies the metric/cost associated with the routes.

Interface

Figure 5-113. OSPF Interface Configuration Page



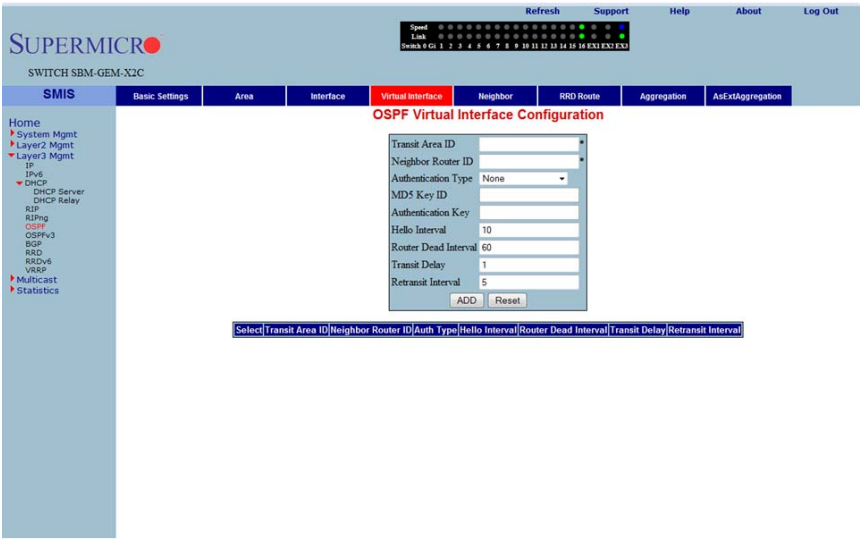
Clicking the INTERFACE tab brings up the OSPF INTERFACE CONFIGURATION page (Figure 5-113). The parameters for this page are shown in Table 5-90.

Table 5-90. 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.
Authentication Type	This parameter allows you to choose *MD5*, *Simple Password* or *None* 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 *MD5*.
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.
Status	When this parameter is enabled, the interface is advertised as an internal route to some area. When disabled it denotes that the interface is external to OSPF.

Virtual Interface

Figure 5-114. OSPF Virtual Interface Configuration Page



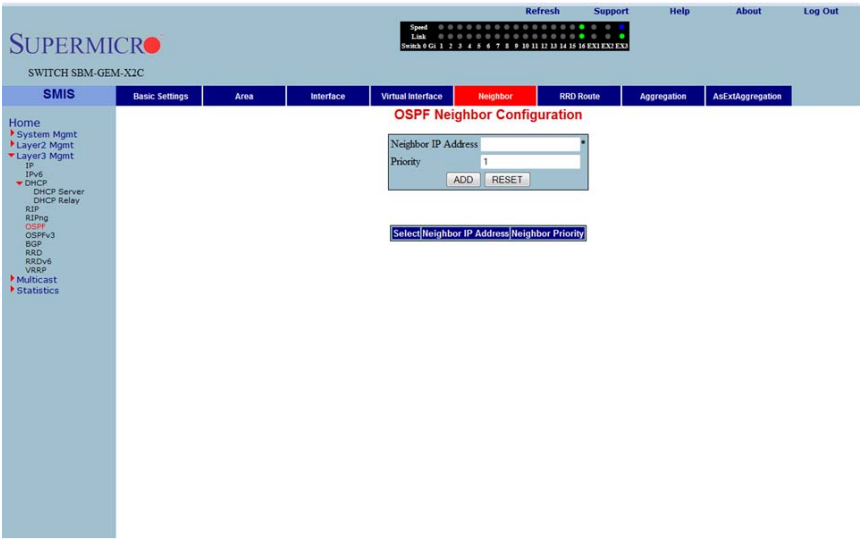
Clicking the VIRTUAL INTERFACE tab brings up the OSPF VIRTUAL INTERFACE CONFIGURATION page (Figure 5-114). The parameters for this page are shown in Table 5-91.

Table 5-91. 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 *MD5*, *Simple Password* or *None* 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 *MD5*.
Authentication Key	This parameter specifies the key required for authentication, if authentication is enabled on this interface.

OSPF Neighbor

Figure 5-115. OSPF Neighbor Configuration Page



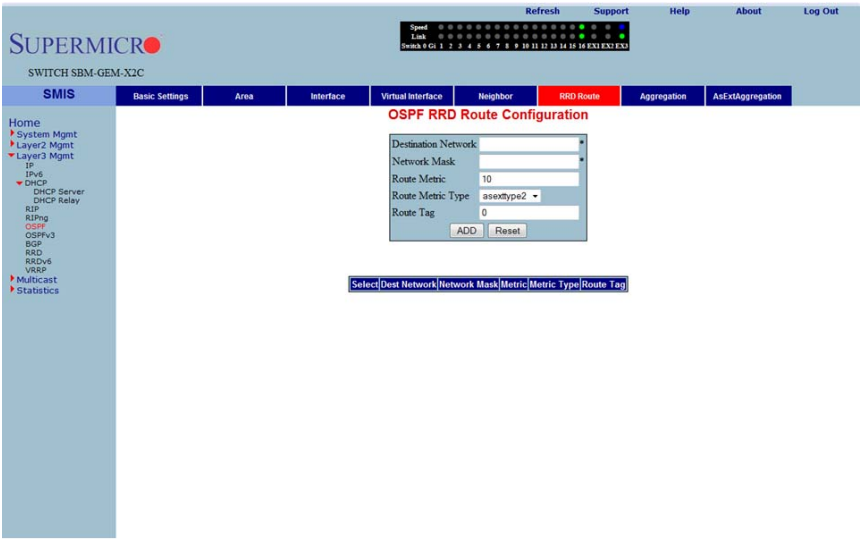
Clicking the NEIGHBOR tab brings up the OSPF NEIGHBOR CONFIGURATION page (Figure 5-115), which allows you to configure OSPF neighbors. The parameters for this page are shown in Table 5-92.

Table 5-92. 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.

OSPF RRD Route Configuration

Figure 5-116. OSPF RRD Route Configuration Page



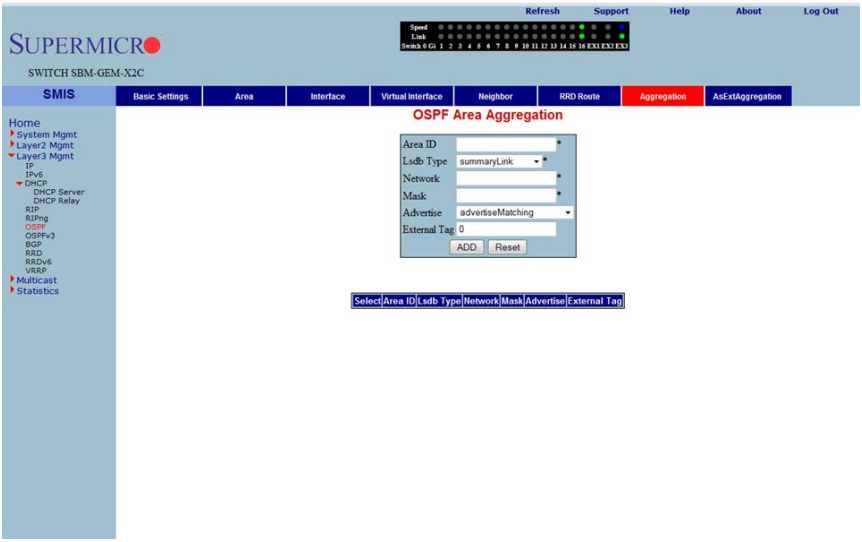
Clicking the RRD ROUTE tab brings up the OSPF RRD ROUTE CONFIGURATION page (Figure 5-116), which displays the various parameters for RRD Route configuration. The parameters for this page are shown in Table 5-93.

Table 5-93. 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.

OSPF Area Aggregation

Figure 5-117. OSPF Area Aggregation Page



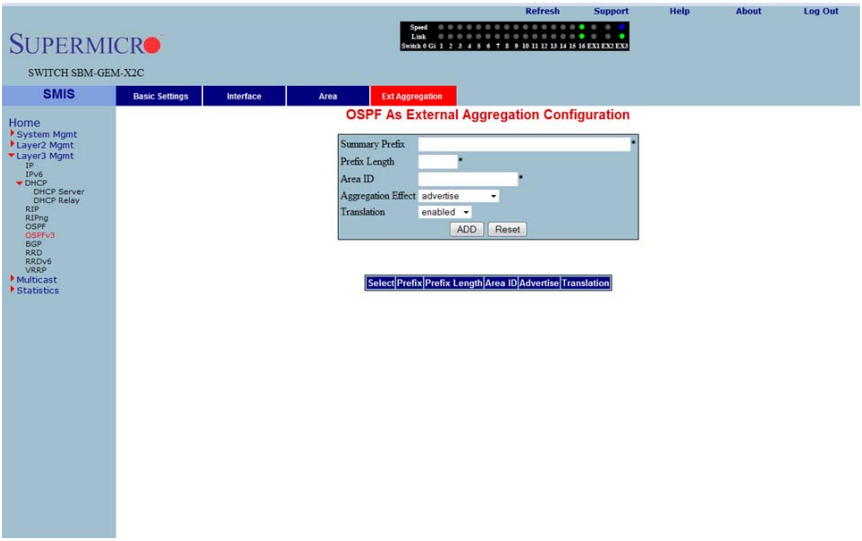
Clicking the AGGREGATION tab brings up the OSPF AREA AGGREGATION page (Figure 5-117). The parameters for this page are shown in Table 5-94.

Table 5-94. 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 *Summary Link* or as a *NSSA External Link*.
Network	This parameter specifies the network address.
Mask	This parameter specifies the network mask.
Advertise	This parameter specifies the advertise option as *Advertise Matching* or *Do Not Advertise Matching*.
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.

External Aggregation

Figure 5-118. OSPF As External Aggregation Configuration Page



Clicking the EXT AGGREGATION tab brings up the OSPF AS EXTERNAL AGGREGATION CONFIGURATION page (Figure 5-118), which allows you to configure OSPF external aggregation parameters. The parameters for this page are shown in Table 5-95.

Table 5-95. 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 5-95. OSPF As External Aggregation Configuration Page Parameters

Parameter	Description
Aggregation Effect	This parameter specifies the Aggreation option as one of the following: • **Advertise** – When set to *advertise* 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 *doNotAdvertise* (2) 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 *allowAll* 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 *denyAll* neither Type-5 nor Type-7 will be generated for the specified range.
Translation	This parameter enables or disables the translation.

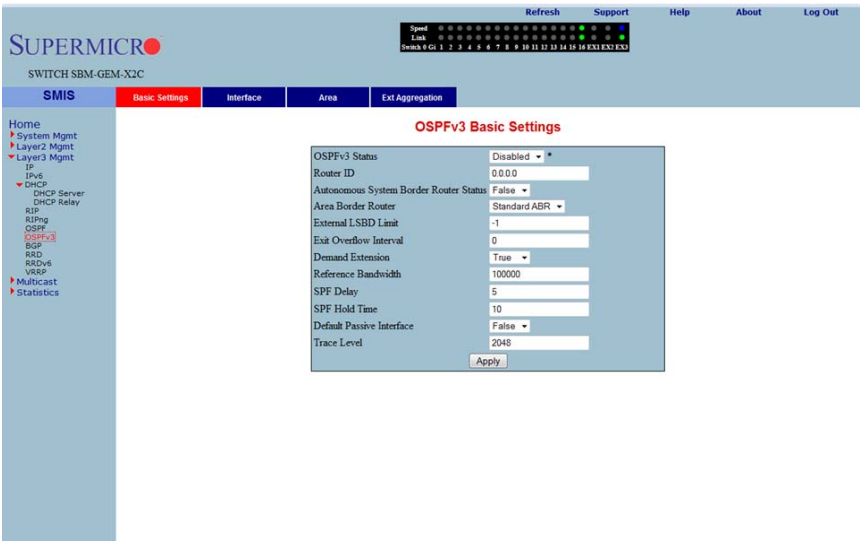
OSPF V3

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

- OSPFv3 Basic Settings
- Interface
- Area
- OSPF V3 External Aggregation

OSPFv3 Basic Settings

Figure 5-119. OSPFv3 Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the OSPFv3 BASIC SETTINGS page (Figure 5-119). The parameters for this page are shown in Table 5-96.

Table 5-96. OSPFv3 Basic Settings Page Parameters

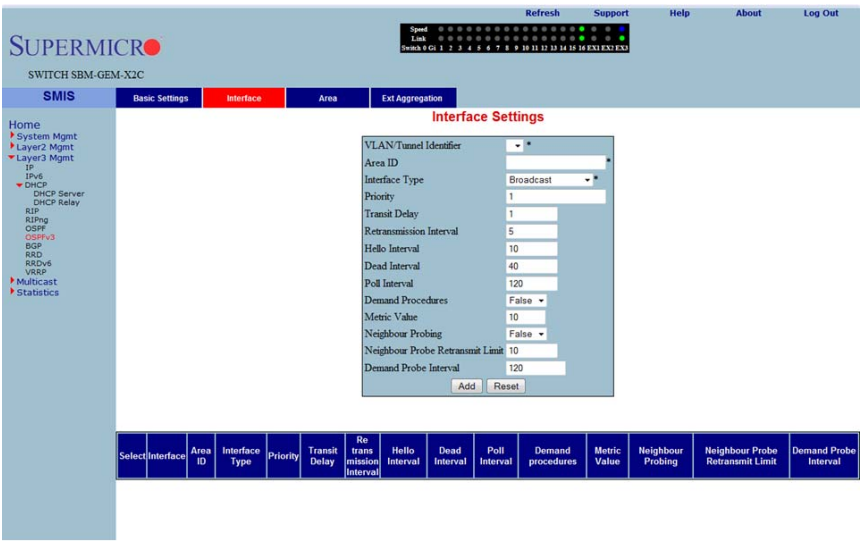
Parameter	Description
OSPFv3 Status	This parameter enables or disables OSPFv3 administratively.
Router ID	This parameter uniquely identifies the router in the Autonomous System.
Autonomous System Border Router Status	This parameter specifies the router as Autonomous System border router.
Area Border Router	This parameter specifies the router as an area border router.

Table 5-96. OSPFv3 Basic Settings Page Parameters (Continued)

Parameter	Description
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 OverflowState.
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.
SPF Delay	This parameter indicates the delay in routing calculation after a topology change.
SPF Hold Time	This parameter specifies the minimum time between two consecutive SPF calculations.
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 5-120. Interface Settings Page



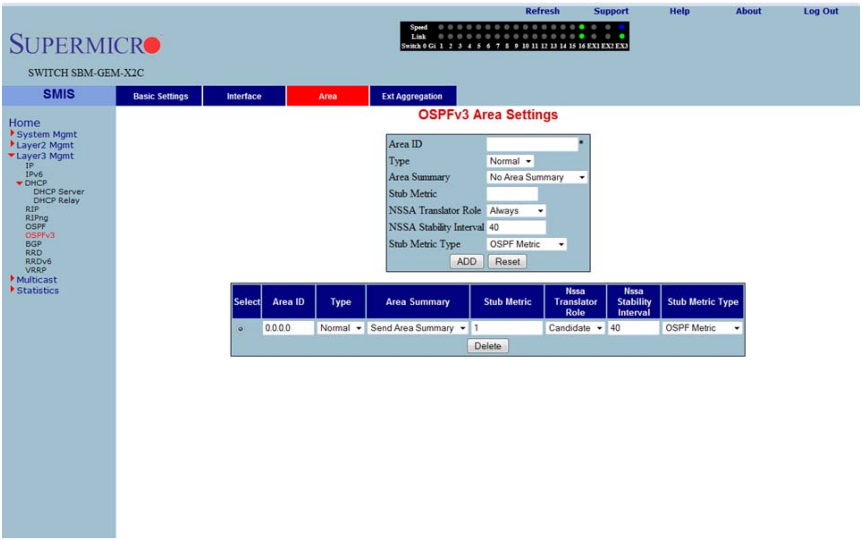
Clicking the INTERFACE tab brings up the INTERFACE SETTINGS page (Figure 5-120). The parameters for this page are shown in Table 5-97.

Table 5-97. 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.
Transit Delay	This parameter indicates the estimated number of seconds to transmit a link state update packet over the interface.
Retransmission Interval	This parameter indicates the number of seconds between the link-state advertisement retransmissions, for adjacencies belonging to the interface.
Hello Interval	This parameter indicates the length of time, in seconds, between the Hello packets that the router sends on the interface.
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.
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.
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.
Demand Probe Interval	This parameter defines how often the neighbor is probed.

Area

Figure 5-121. OSPFv3 Area Settings Page



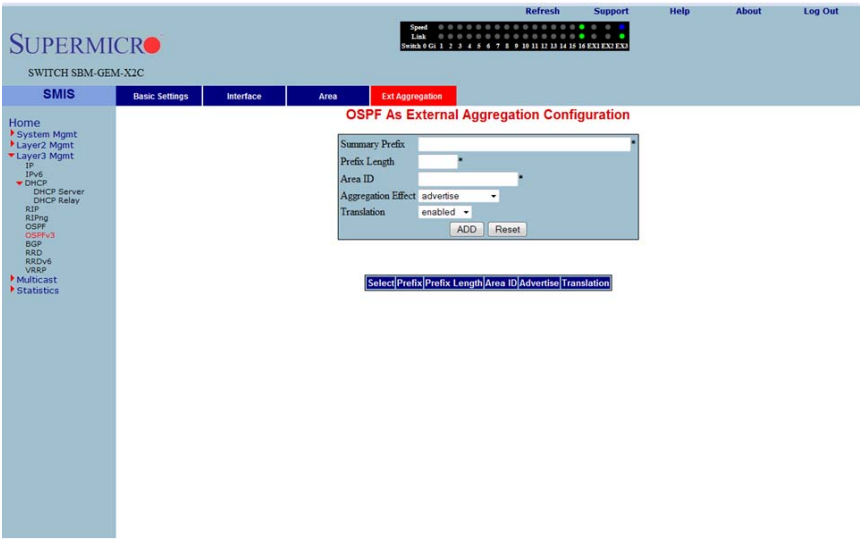
Clicking the AREA tab brings up the OSPFv3 AREA SETTINGS page (Figure 5-121). The parameters for this page are shown in Table 5-98.

Table 5-98. OSPFv3 Area Settings Page Parameters

Parameter	Description
Area ID	This parameter uniquely identifies an area.
Type	This parameter indicates whether an area is a *Stub* area, *NSSA*, or *Standard* (normal) area.
Area Summary	This parameter controls the import of Inter-Area LSAs into stub areas. This can be *noAreaSummary* or *sendAreaSummary*.
Stub Metric	This parameter indicates the metric value advertised for the default route into *Stub* area and *NSSA*.
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 (*OSPFv3 Metric, External Type 1, External Type 2*) advertised as a default route.

OSPF V3 External Aggregation

Figure 5-122. OSPF AS External Aggregation Configuration Page



Clicking the EXT AGGREGATION tab brings up the OSPF AS EXTERNAL AGGREGATION CONFIGURATION page (Figure 5-122), which allows you to configure OSPF external aggregation parameters. The parameters for this page are shown in Table 5-99.

Table 5-99. 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 5-99. OSPF AS External Aggregation Configuration Page Parameters

Parameter	Description
Aggregation Effect	This parameter specifies the Aggreation option as one of the following: • **Advertise** – When set to *advertise* 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 *doNotAdvertise (2)* 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 *allowAll* 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 *denyAll* neither Type-5 nor Type-7 will be generated for the specified range.
Translation	This parameter enables or disables the translation.

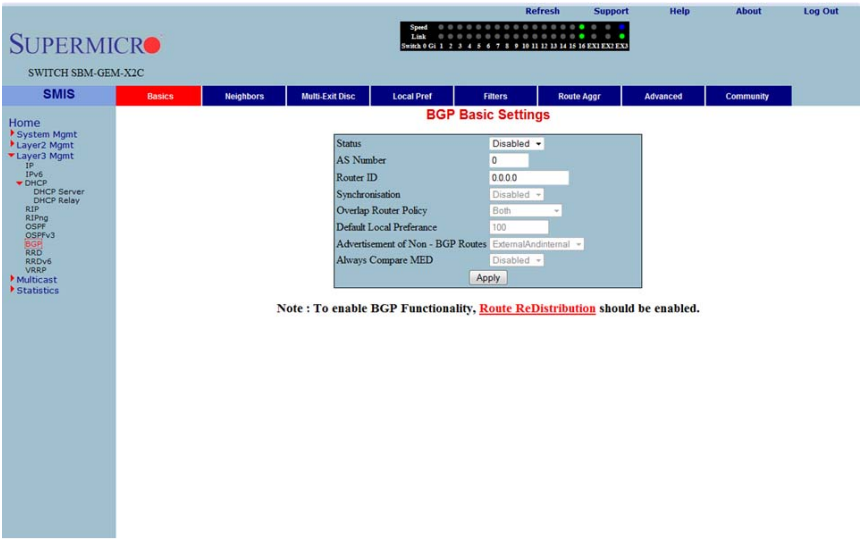
BGP

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

- BGP Basic Settings
- BGP Peer Configuration
- BGP MED Configuration
- Local Preference
- BGP Filter
- Route Aggregations
- Advanced BGP Configuration
- BGP Community Management

BGP Basic Settings

Figure 5-123. BGP Basic Settings Page



Clicking the BASICS tab brings up the BGP BASIC SETTINGS page (Figure 5-123). The parameters for this page are shown in Table 5-100.

Table 5-100. BGP Basic Settings Page Parameters

Parameter	Description
Status	This parameter specifies the BGP admin 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.
Synchronization	The synchronization between IGP and BGP can be ensured by enabling this field.
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.

BGP Peer Configuration

Figure 5-124. BGP Peer Configuration Page

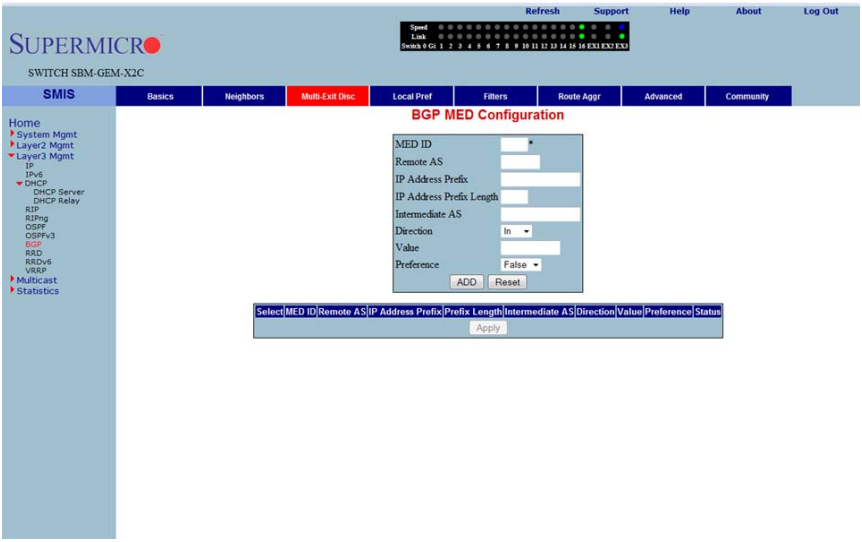
Clicking the NEIGHBORS tab brings up the BGP PEER CONFIGURATION page (Figure 5-124), which allows you to configre BGP Neighbors. The parameters for this page are shown in Table 5-101.

Table 5-101. 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 *Self* or *Automatic*. By setting this field to *Self*, 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.
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.
Remote AS	This parameter represents the remote autonomous system number.
Advertisement Interval (seconds)	This parameter specifies the interval in seconds for the Minimum Route advertisement interval timer.
Status	This parameter specifies the status of the entry.

BGP MED Configuration

Figure 5-125. BGP MED Configuration Page



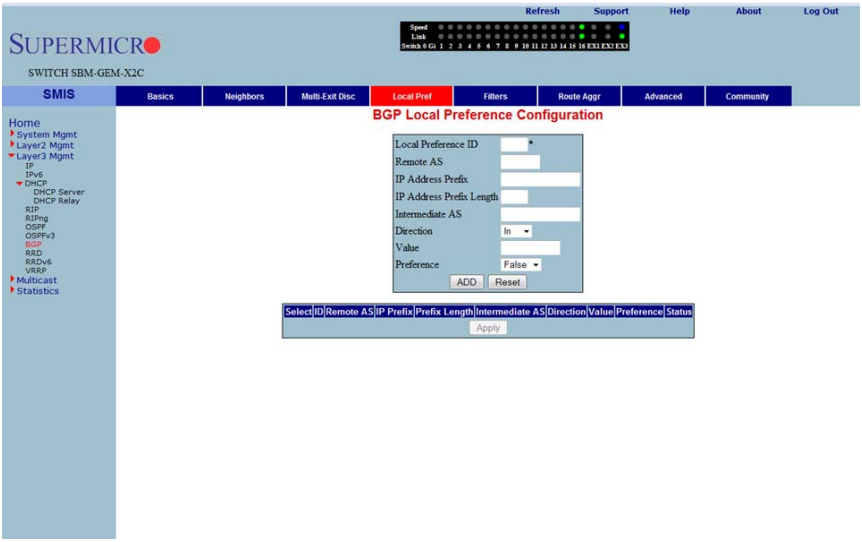
Clicking the MULTI-EXIT DISC tab brings up the BGP MED CONFIGURATION page (Figure 5-125), which allows you to configure the MED value for routes learnt from BGP peers. The parameters for this page are shown in Table 5-102.

Table 5-102. BGP MED Configuration Page Parameters

Parameter	Description
MED ID	This parameter specifies the index for this table.
Remote AS	This parameter specifies the AS number from which the route update is received.
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.
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 *In* and *Out* values.
Value	This parameter specifies the MED value to be associated with this path learnt.
Preference	This parameter is used to enable/disable filtering.
Status	This parameter indicates the status of the entry.

Local Preference

Figure 5-126. BGP Local Preference Configuration Page



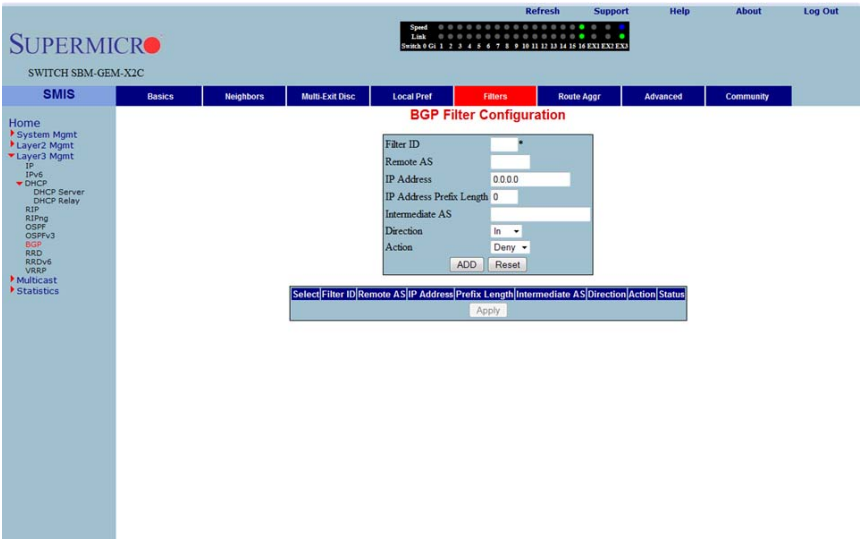
Clicking the LOCAL PREF tab brings up the BGP LOCAL PREFERENCE CONFIGURATION page (Figure 5-126), which allows you to configure the Local Preference value for routes. The parameters for this page are shown in Table 5-103.

Table 5-103. 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.
Remote AS	This parameter specifies the AS number from which the route update is received.
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.
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 *In* and *Out* values.
Value	This parameter specifies the Local preference value to be associated with this learnt path.
Preference	This parameter is used to enable/disable filtering.
Status	This parameter specifies the status of the entry.

BGP Filter

Figure 5-127. BGP Filter Configuration Page



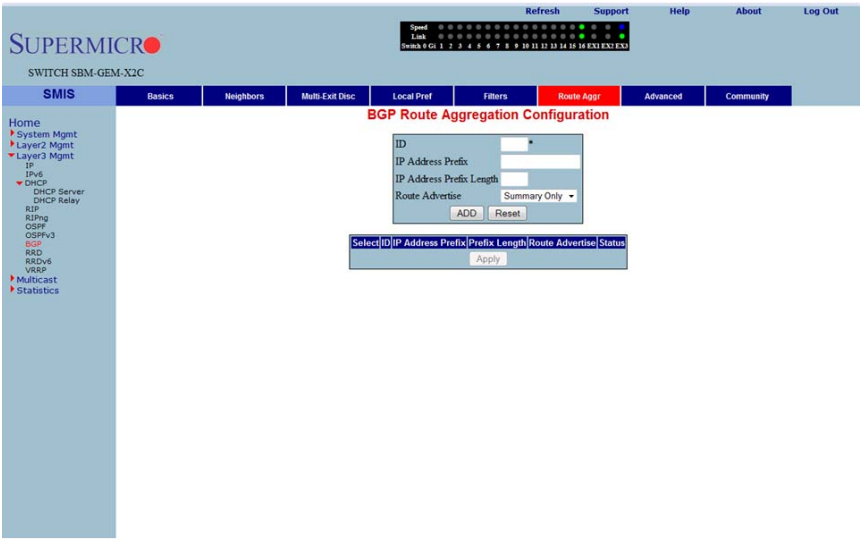
Clicking the FILTERS tab brings up the BGP FILTER CONFIGURATION page (Figure 5-127), which is used to set the filters on the routes being learnt. The parameters for this page are shown in Table 5-104.

Table 5-104. BGP Filter Configuration Page Parameters

Parameter	Description
Filter ID	This parameter specifies the filter index.
Remote AS	This parameter specifies the remote AS associated with the BGP peer from which the router is being distributed.
IP Address	This parameter specifies the IP address for which the route is being learnt.
IP Address Prefix Length	This parameter specifies the prefix length to calculate the Subnet.
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 *Allow* (not to filter) or *Deny* (Filter) for the above configuration set.
Status	This parameter specifies the status of the entry.

Route Aggregations

Figure 5-128. BGP Route Aggregation Configuration Page



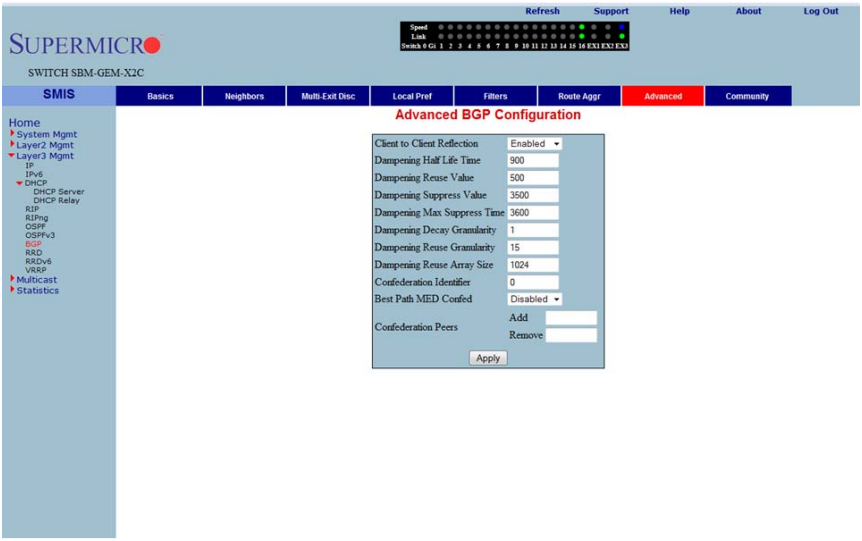
Clicking the ROUTE AGGR tab brings up the BGP ROUTE AGGREGATION CONFIGURATION page (Figure 5-128), which is used to aggregate and configure the routes advertised by BGP. The parameters for this page are shown in Table 5-105.

Table 5-105. BGP Route Aggregation Configuration Page Parameters

Parameter	Description
ID	This parameter specifies the index to this table.
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.
Route Advertise	With this parameter you can either choose to advertise only the aggregated routes by setting *Summary only,* or choose to advertise all routes by setting *All*.
Status	This parameter specifies the status of the entry.

Advanced BGP Configuration

Figure 5-129. Advanced BGP Configuration Page



Clicking the ADVANCED tab brings up the ADVANCED BGP CONFIGURATION page (Figure 5-129), which configures dampening and confederation parameters. The parameters for this page are shown in Table 5-106.

Table 5-106. Advanced BGP Configuration Page Parameters

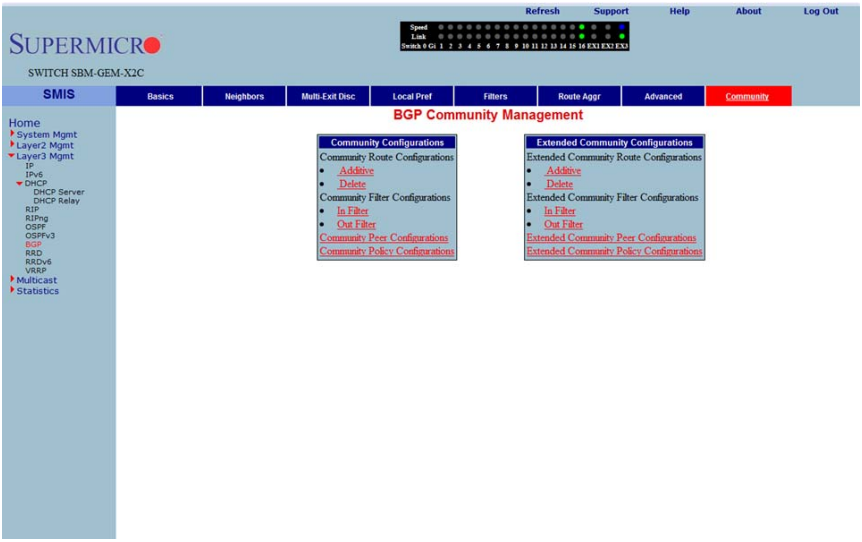
Parameter	Description
Client to Client Reflection	This parameter configures the Route Reflector to support route reflection to client peers. By default, the Route Reflector will reflect routes learnt from a client peer to all other client peers. If required, the administrator can disable this feature by disabling client-to-client reflection. 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.
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.
Dampening Reuse Value	If the penalty associated with a suppressed route falls below this value, the route is re-used.
Dampening Suppress Value	A route is suppressed when the penalty associated with the route exceeds this value.

Table 5-106. Advanced BGP Configuration Page Parameters (Continued)

Parameter	Description
Dampening Max Suppress Time	This parameter specifies the maximum time (in seconds) a route can be suppressed.
Dampening Decay Granularity	This parameter specifies the time granularity in seconds used to perform all decay computations.
Dampening Reuse Granularity	This parameter specifies the time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment.
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.
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.

BGP Community Management

Figure 5-130. BGP Community Management Page



Clicking the COMMUNITY tab brings up the BGP COMMUNITY MANAGEMENT page (Figure 5-130), which configures BGP community and extended community parameters. The parameters for this page are shown in Table 5-107.

Table 5-107. 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.

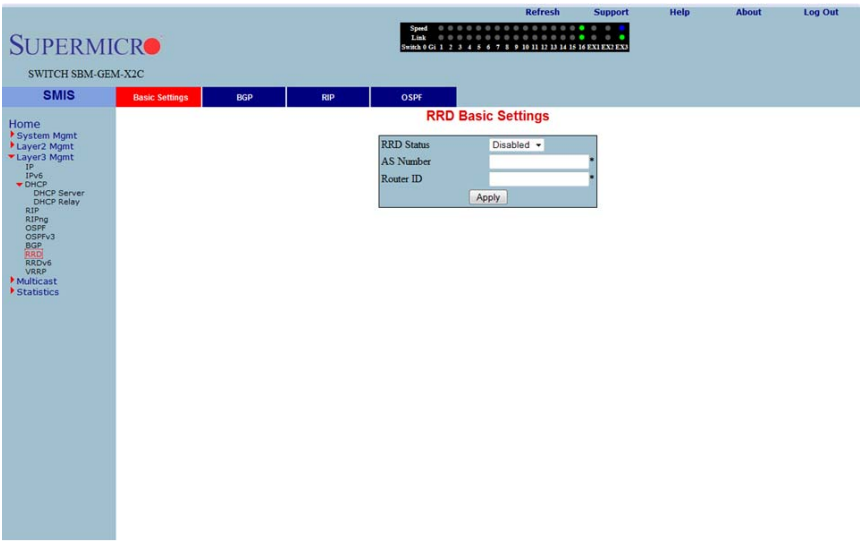
RRD

The RRD link allows you to manage the Route Redistribution with the help of the following pages:

- RRD Basic Settings
- BGP
- RIP
- OSPF

RRD Basic Settings

Figure 5-131. RRD Basic Settings Page



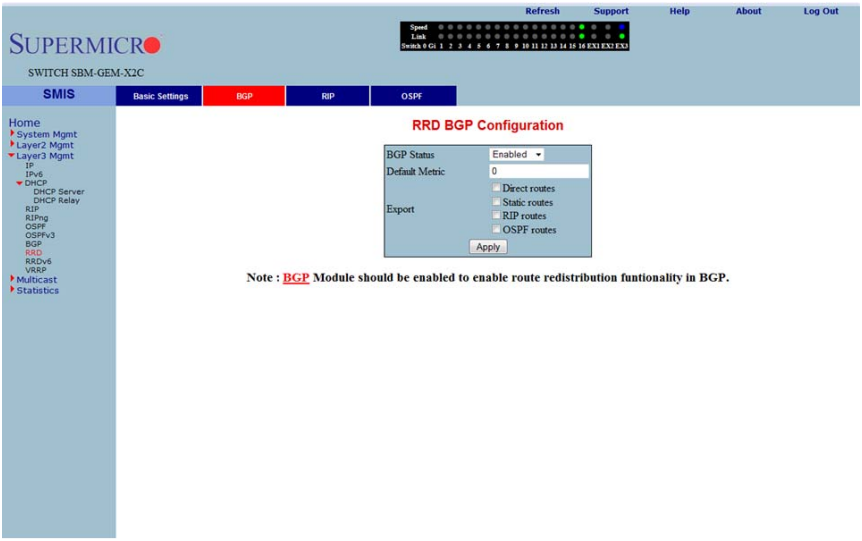
Clicking the BASIC SETTINGS tab brings up the RRD BASIC SETTINGS page (Figure 5-131). The parameters for this page are shown in Table 5-108.

Table 5-108. RRD Basic Settings Page Parameters

Parameter	Description
RRD Status	By enabling this parameter, Route Re-distribution can be enabled in the switch.
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 5-132. RRD BGP Configuration Page



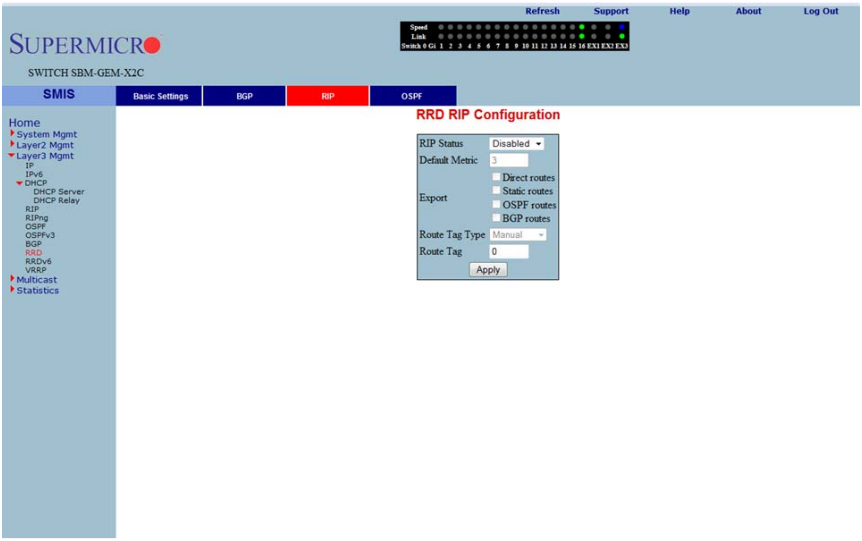
Clicking the BGP tab brings up the RRD BGP CONFIGURATION page (Figure 5-132), which allows you to re-distribute the routes that are learnt through other routing protocols to BGP. The parameters for this page are shown in Table 5-109.

Table 5-109. 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.
Import	With this parameter you can choose to import *Direct routes*, *Static routes*, *RIP routes* and/or *OSPF routes* to BGP.

RIP

Figure 5-133. RRD RIP Configuration Page



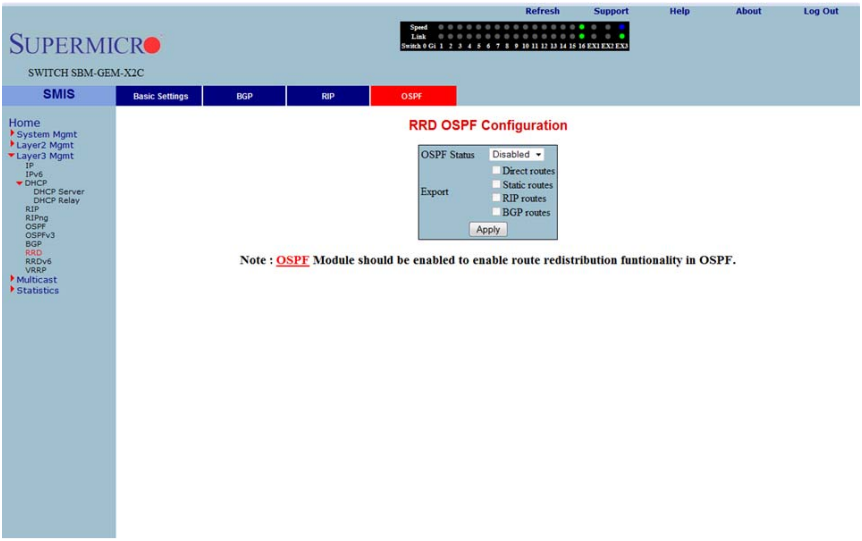
Clicking the RIP tab brings up the RRD RIP CONFIGURATION page (Figure 5-133), which allows you to re-distribute the routes that are learnt through other routing protocols to RIP. The parameters for this page are shown in Table 5-110.

Table 5-110. 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.
Import	You can use this parameter to choose to import *Direct routes, Static routes, OSPF routes* and *BGP routes* to RIP.
Route Tag Type	This parameter describes whether a tag is *manually* configured or *automatically* generated.
Route Tag	This parameter indicates the route tag in case you configure a manual option for the tag type.

OSPF

Figure 5-134. RRD OSPF Configuration Page



Clicking the OSPF tab brings up the RRD OSPF CONFIGURATION page (Figure 5-134), which allows you to e-distribute the routes that are learnt through other routing protocols to OSPF. The parameters for this page are shown in Table 5-111.

Table 5-111. 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 *Direct routes, Static routes, RIP routes* and *BGP routes* to OSPF.

RRD6

The RRD6 link allows you to perform RRD6 related configuration through the following pages.

- RRD6 Basic Settings
- Filters
- RRD V6 OSPF
- RRD RIP

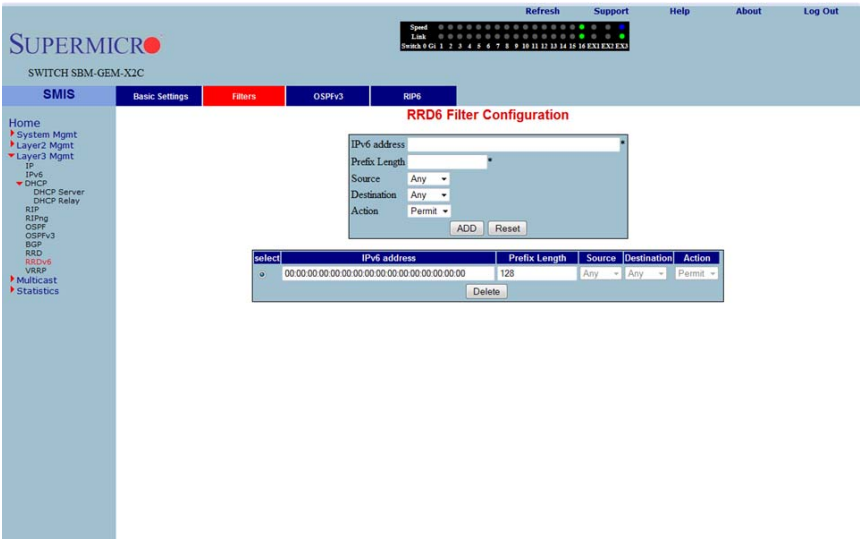
RRD6 Basic Settings

Figure 5-135. RRD6 Basic Settings Page

Clicking the BASIC SETTINGS tab brings up the RRD6 BASIC SETTINGS page (Figure 5-135), which has the single parameter option of changing the throat limit for RRD6.

Filters

Figure 5-136. RRD6 Filter Configuration Page



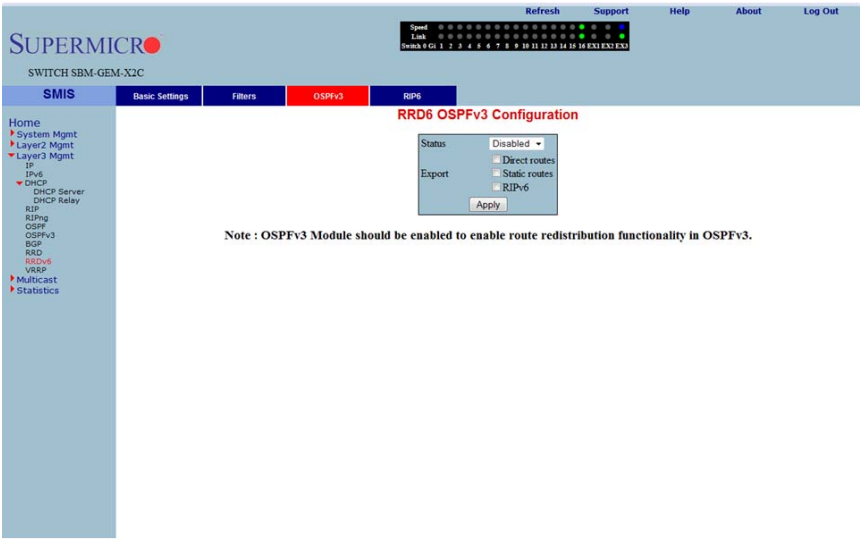
Clicking the FILTERS tab brings up the RRD6 FILTER CONFIGURATION page (Figure 5-136). The parameters for this page are shown in Table 5-112.

Table 5-112. 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 *Permit* (not to filter) or *Deny* (Filter) for the above configuration set.

RRD V6 OSPF

Figure 5-137. RRD6 OSPFv3 Configuration Page



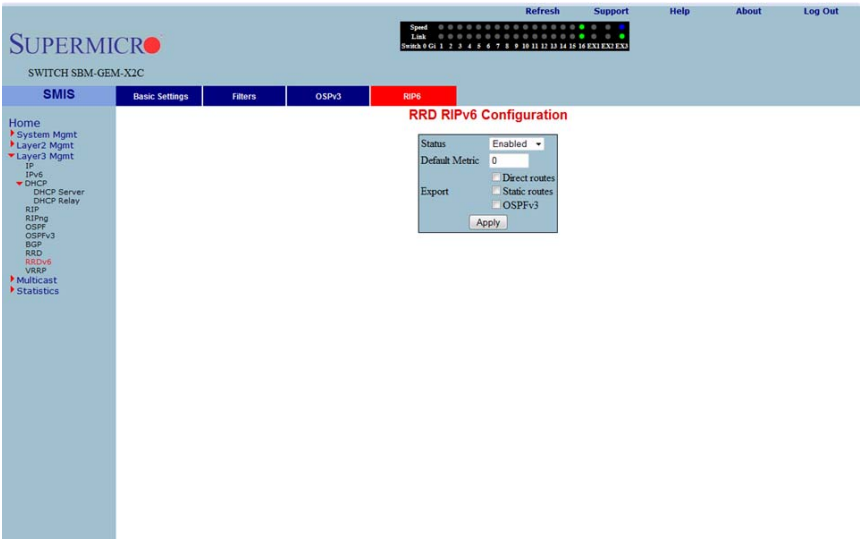
Clicking the OSPFv3 tab brings up the RRD6 OSPFv3 CONFIGURATION page (Figure 5-137). The parameters for this page are shown in Table 5-113.

Table 5-113. RRD6 OSPFv3 Configuration Page Parameters

Parameter	Description
Status	This parameter enables or disables redistribution for OSPFv3.
Import	With this parameter you can choose to import *Direct routes*, *Static routes* or *RIPv6 routes*.

RRD RIP

Figure 5-138. RRD RIPv6 Configuration Page



Clicking the RP6 tab brings up the RRD RIPv6 CONFIGURATION page (Figure 5-138). The parameters for this page are shown in Table 5-114.

Table 5-114. 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.
Import	With this parameter you can choose to import *Direct routes, Static routes* or *OSPFv3 routes*.

VRRP

The VRRP link allows you to configure VRRP through the following two pages:

- VRRP Basic Settings
- VRRP Settings

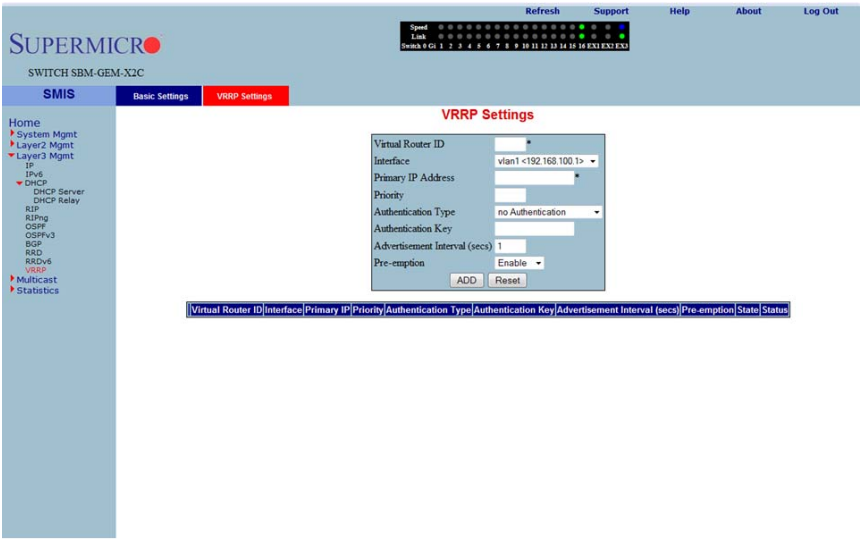
VRRP Basic Settings

Figure 5-139. VRRP Basic Settings Page

Clicking the BASIC SETTINGS tab brings up the VRRP BASIC SETTINGS page (Figure 5-139), whose single parameter allows you to specify the status of VRRP in the switch.

VRRP Settings

Figure 5-140. VRRP Settings Page



Clicking the VRRP SETTINGS link brings up the VRRP SETTINGS page (Figure 5-140). The parameters for this page are shown in Table 5-115.

Table 5-115. VRRP Settings Page Parameters

Parameter	Description
Virtual Router ID	This parameter indicates the Virtual ID associated with each Virtual Router.
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 enablesor 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 5-141. Multicast Home Page

MULTICAST HOME page (Figure 5-141) 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:

- IGMP Snooping Configuration
- IGMP Snooping Timer
- IGMP Snooping Interface
- IGMP Snooping VLAN Router
- IGMP MAC Forwarding

IGMP Snooping Configuration

Figure 5-142. IGMP Snooping Configuration Page

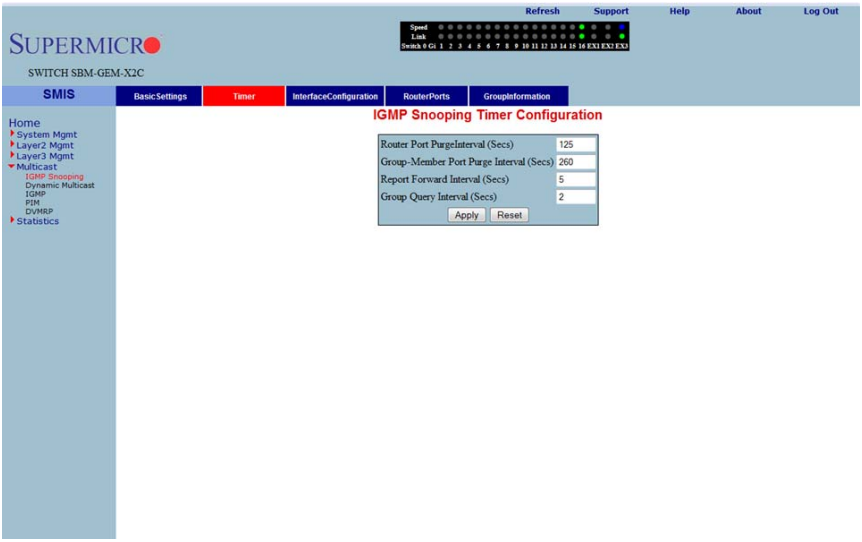
Clicking the BASIC SETTINGS tab brings up the IGMP SNOOPING CONFIGURATION page (Figure 5-142), which allows you to configure IGMP snooping parameters. The parameters for this page are shown in Table 5-116.

Table 5-116. IGMP Snooping Configuration Page Parameters

Parameter	Description
System Control	This parameter *Starts* or *Shutsdown* 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 *Disabled*.
Operational Status	This parameter enables or disables IGMP snooping operationally in the switch. To enable IGS, GMRP status must be *Disabled*.
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.
Query Transmit On TC	This parameter allows you to enable or disable query transmit when topology changes.

IGMP Snooping Timer

Figure 5-143. IGMP Snooping Timer Configuration Page



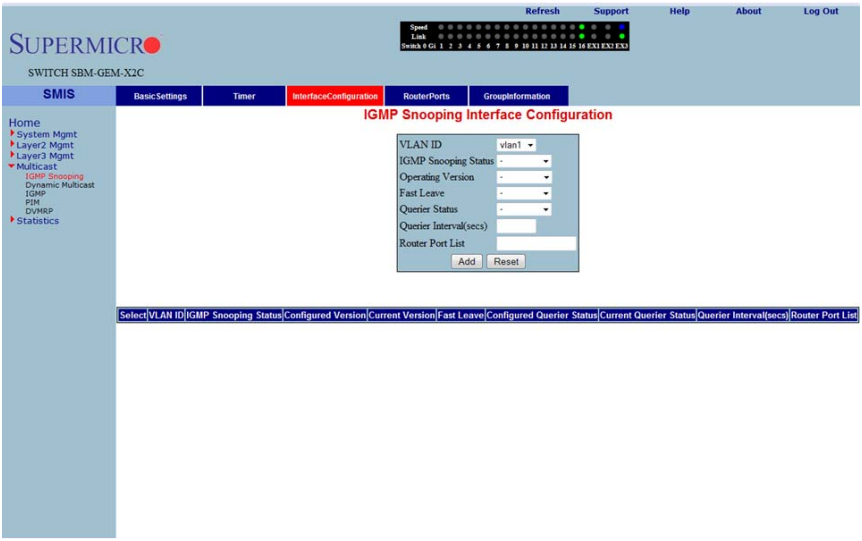
Clicking the TIMER tab brings up the IGMP SNOOPING TIMER CONFIGURATION page (Figure 5-143), which configures IGMP snooping timers. The parameters for this page are shown in Table 5-117.

Table 5-117. 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-second**s.

IGMP Snooping Interface

Figure 5-144. IGMP Snooping Interface Configuration Page



Clicking the INTERFACE CONFIGURATION tab brings up the IGMP SNOOPING INTERFACE CONFIGURATION page (Figure 5-144), which configures IGMP snooping interface specific parameters. The parameters for this page are shown in Table 5-118.

Table 5-118. 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.
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.
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.

Table 5-118. IGMP Snooping Interface Configuration Page Parameters (Continued)

Parameter	Description
Current Version	This parameter specifies the working IGMP Version on the given VLAN.
Current Querier Status	This parameter specifies the current status of the Querier.

IGMP Snooping VLAN Router

Figure 5-145. IGMP Snooping VLAN Router Ports Page

Clicking the ROUTE PORTS tab brings up the IGMP SNOOPING VLAN ROUTER PORTS page (Figure 5-145). The parameters for this page are shown in Table 5-119.

Table 5-119. 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.

IGMP MAC Forwarding

Figure 5-146. MAC Based Multicast Forwarding Table Page

Clicking the GROUP INFORMATION tab brings up the MAC BASED MULTICAST FORWARDING TABLE page (Figure 5-146), 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 5-120.

Table 5-120. 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.

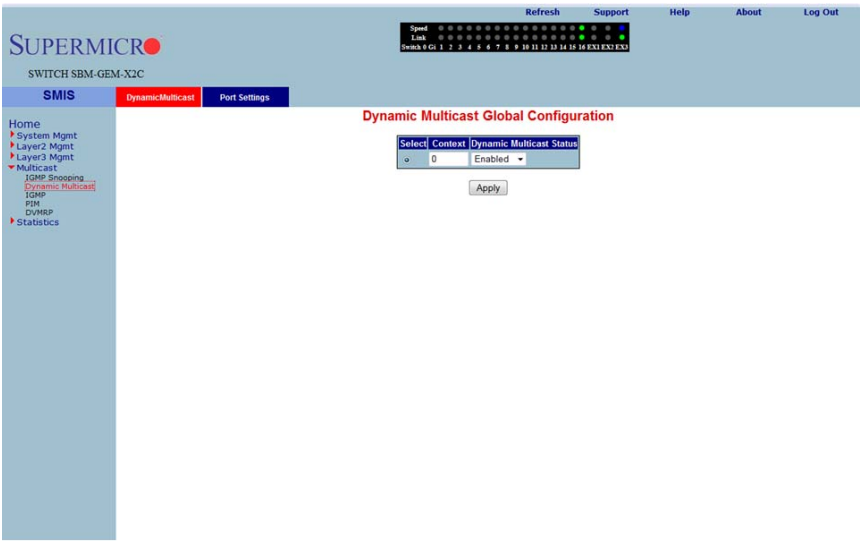
Dynamic Multicast

The Dynamic Multicast link allows you to configure Dynamic Multicast through the following pages:

- Global Configuration
- Dynamic Multicast Port Configuration

Global Configuration

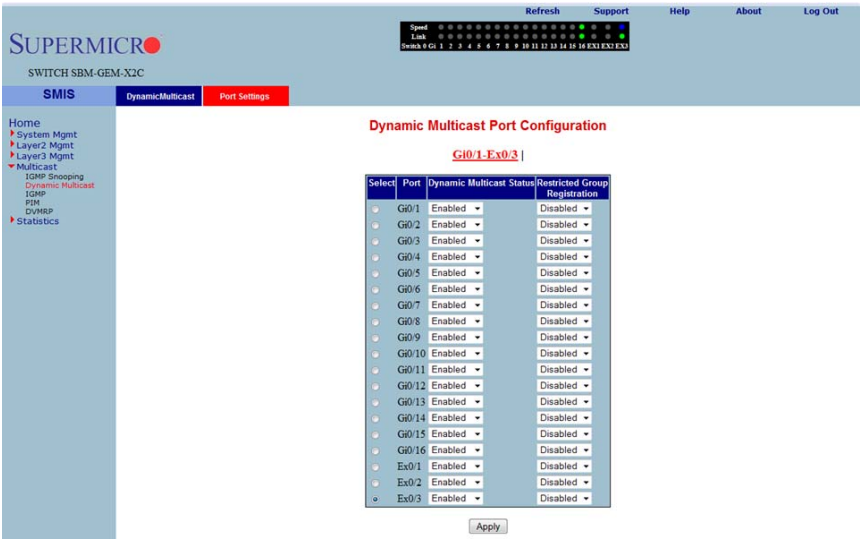
Figure 5-147. Dynamic Multicast Global Configuration Page



Clicking the DYNAMIC MULTICAST tab brings up the DYNAMIC MULTICAST GLOBAL CONFIGURATION page (Figure 5-147), which allows you to enable or disable the dynamic multicast feature.

Dynamic Multicast Port Configuration

Figure 5-148. Dynamic Multicast Port Configuration Page



Clicking the PORT SETTINGS tab brings up the DYNAMIC MULTICAST PORT CONFIGURATION page (Figure 5-148), which configures dynamic multicast at the port level. The parameters for this page are shown in Table 5-121.

Table 5-121. 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.

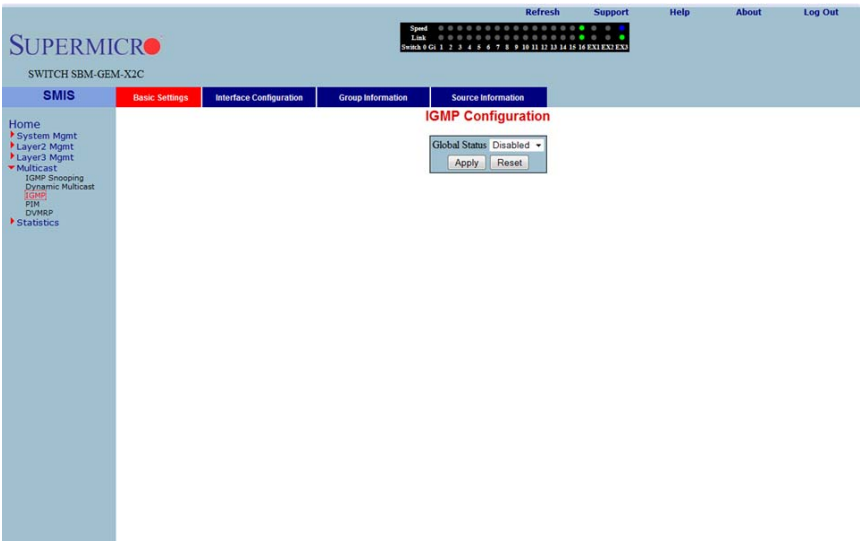
IGMP

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

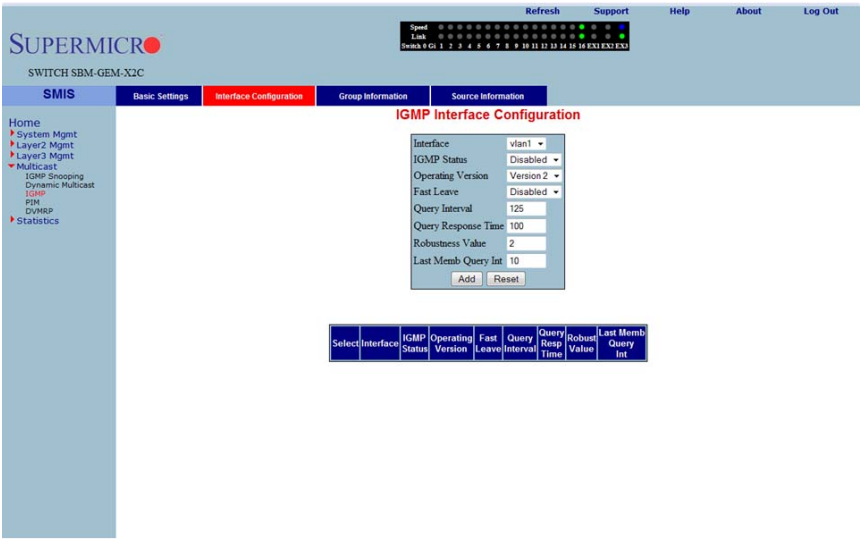
Figure 5-149. IGMP Configuration Page



Clicking the IGMP CONFIGURATION tab brings up the IGMP CONFIGURATION page (Figure 5-149), whose single parameter allows you to enable or disable IGMP in the switch.

Interface Configuration

Figure 5-150. IGMP Interface Configuration Page



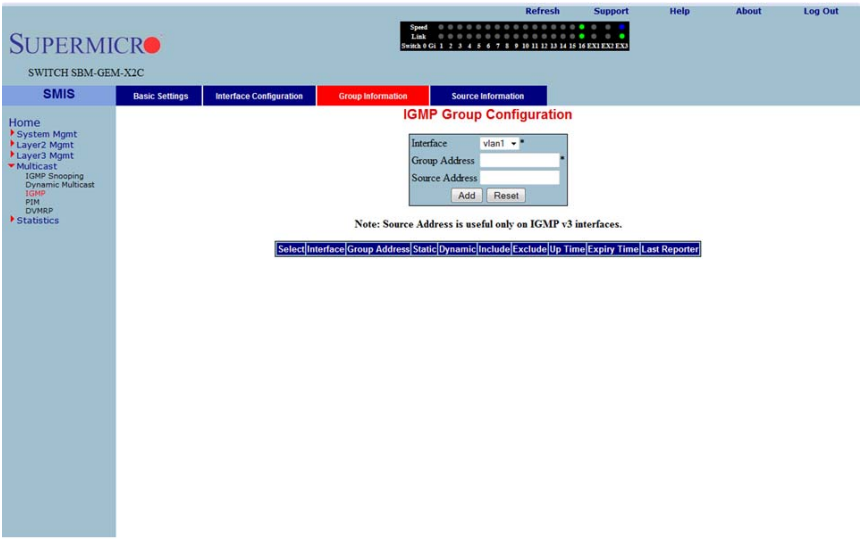
Clicking the INTERFACE CONFIGURATION tab brings up the IGMP INTERFACE CONFIGURATION page (Figure 5-150). The parameters for this page are shown in Table 5-122.

Table 5-122. 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 *IGMP Version 1*, *IGMP Version 2* or *IGMP Version 3*. 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.
Query Response Time	This parameter specifies the response time for IGMP queries.
Robustness Value	This parameter specifies the ROBUSTNESS VALUE on this interface.

Group Information

Figure 5-151. IGMP Group Configuration Page



Clicking the GROUP INFORMATION tab brings up the IGMP GROUP CONFIGURATION page (Figure 5-151). The parameters for this page are shown in Table 5-123.

Table 5-123. 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.
Filter Mode	This parameter specifies the FILTER MODE.

Source Information

Figure 5-152. IGMP Source Information Page

Clicking the SOURCE INFORMATION tab brings up the IGMP SOURCE INFORMATION page (Figure 5-152). The parameters for this page are shown in Table 5-124.

Table 5-124. 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.

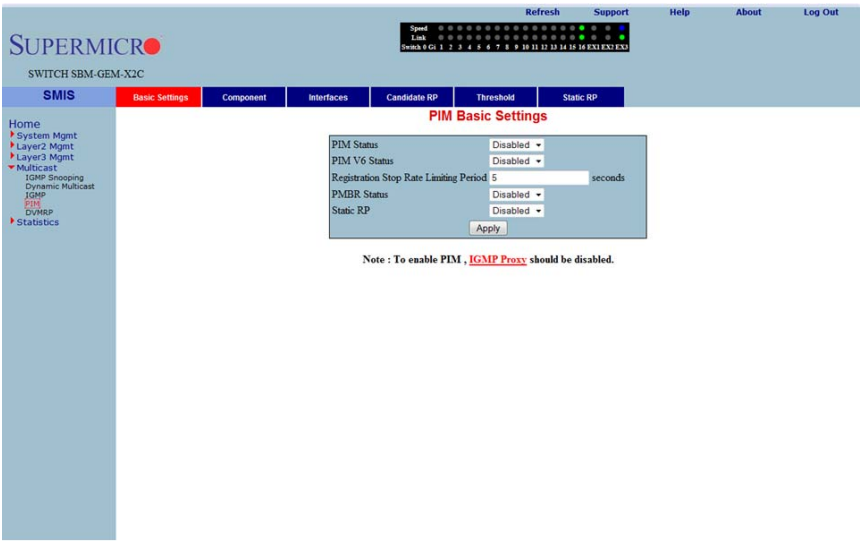
PIM

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 5-153. PIM Basic Settings Page



Clicking the BASIC SETTINGS tab brings up the PIM BASIC SETTINGS page (Figure 5-153), which specifies the PIM status in the switch. The parameters for this page are shown in Table 5-125.

Table 5-125. PIM Basic Settings Page Parameters

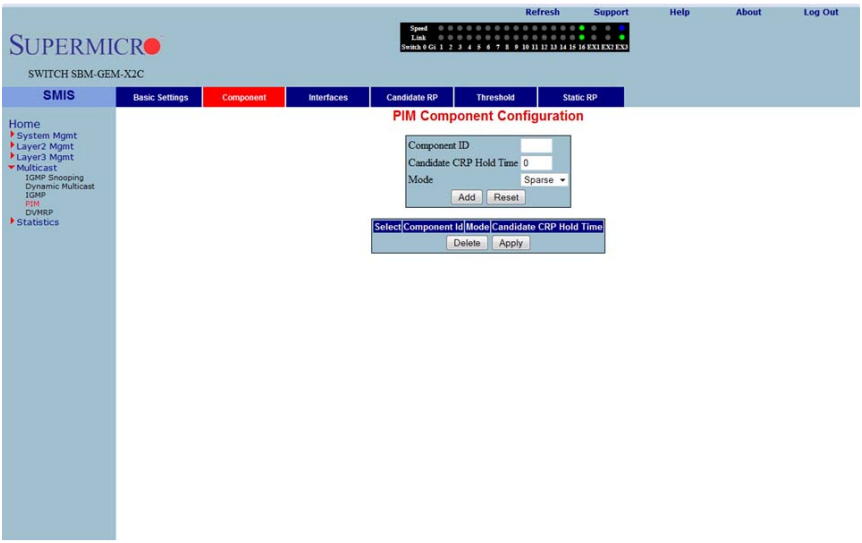
Parameter	Description
PIM Status	This parameter allows you to enable or disable the PIM status in the switch.
PIM V6 Status	This parameter allows you to enable or disable the PIM V6 status in the switch.

Table 5-125. PIM Basic Settings Page Parameters (Continued)

Parameter	Description
Registration Stop Rate Limiting Period	This parameter specifies the registration stop rate limiting period in 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 5-154. PIM Component Configuration Page



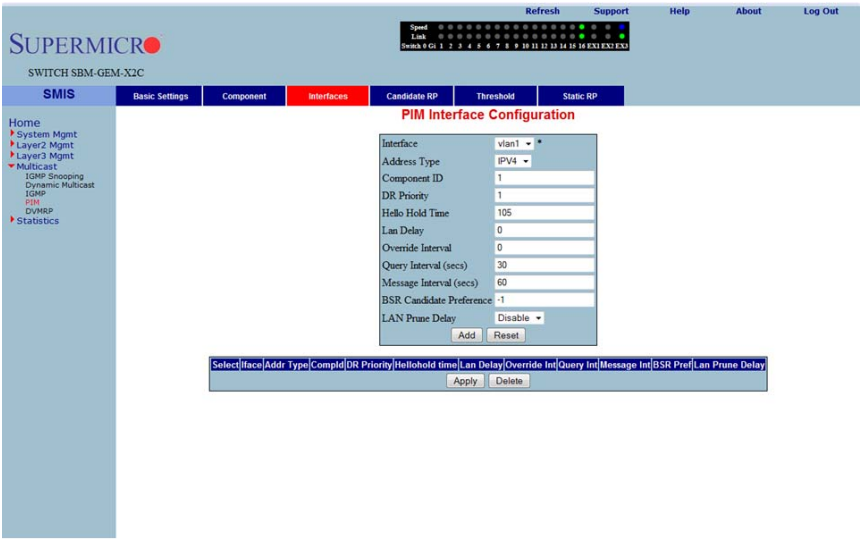
Clicking the COMPONENT tab brings up the PIM COMPONENT CONFIGURATION page (Figure 5-154). The parameters for this page are shown in Table 5-126.

Table 5-126. PIM Component Configuration Page Parameters

Parameter	Description
Component ID	This parameter specifies a number uniquely identifying the component.
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 *Sparse* or *Dense*.
BSR Address	This parameter specifies the IP address of the bootstrap router for the local PIM region, which is a read-only field.
BSR Expiry Time	This parameter indicates the minimum time remaining before the bootstrap router in the local domain is declared down, which is a read-only field.

Interfaces

Figure 5-155. PIM Interface Configuration Page



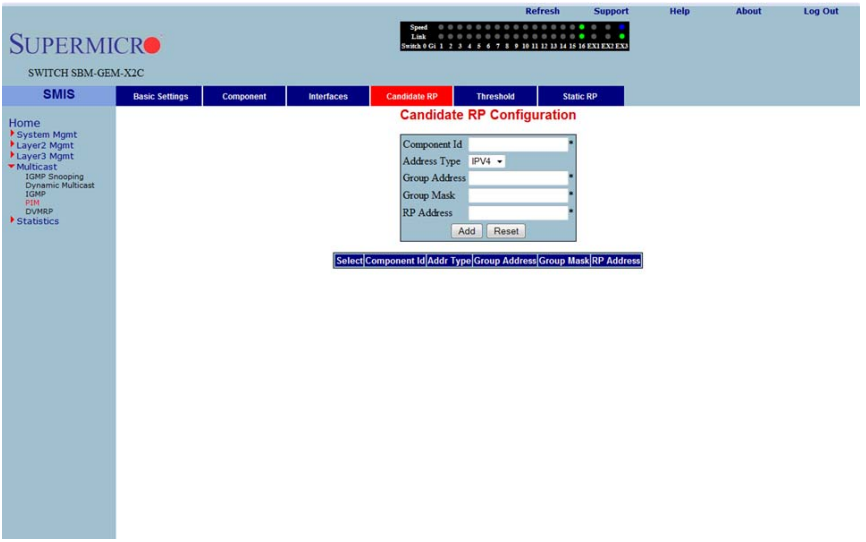
Clicking the INTERFACES tab brings up the PIM INTERFACE CONFIGURATION page (Figure 5-155). The parameters for this page are shown in Table 5-127.

Table 5-127. PIM Interface Configuration Page Parameters

Parameter	Description
Interface	This parameter specifies the interface index.
Component ID	This parameter specifies a number uniquely identifying the component.
Hello Interval (Seconds)	This parameter specifies the time interval between two successive Hello messages being sent by PIM on this interface.
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 5-156. Candidate RP Configuration Page



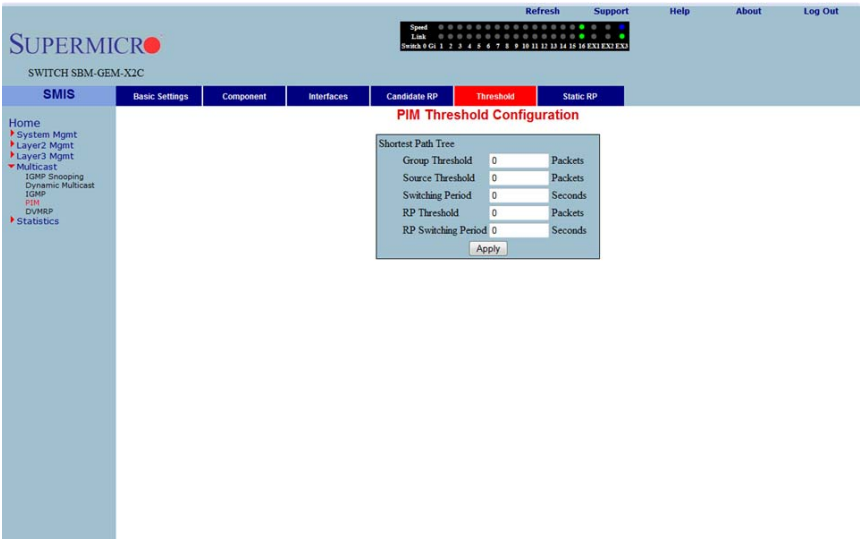
Clicking the CANDIDATE RPS tab brings up the CANDIDATE RP CONFIGURATION page (Figure 5-156). The parameters for this page are shown in Table 5-128.

Table 5-128. 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.
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 5-157. PIM Threshold Configuration Page



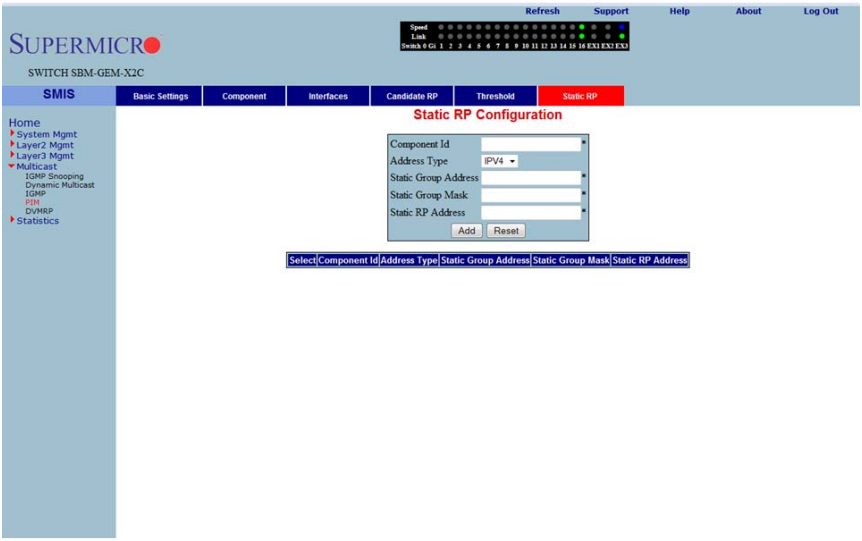
Clicking the THRESHOLD tab brings up the PIM THRESHOLD CONFIGURATION page (Figure 5-157). The parameters for this page are shown in Table 5-129.

Table 5-129. 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.
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 5-158. Static RP Configuration Page



Clicking the STATIC RP tab brings up the STATIC RP CONFIGURATION page (Figure 5-158), which configure static PIM RPs (Rendezvous Points). The parameters for this page are shown in Table 5-130.

Table 5-130. 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.

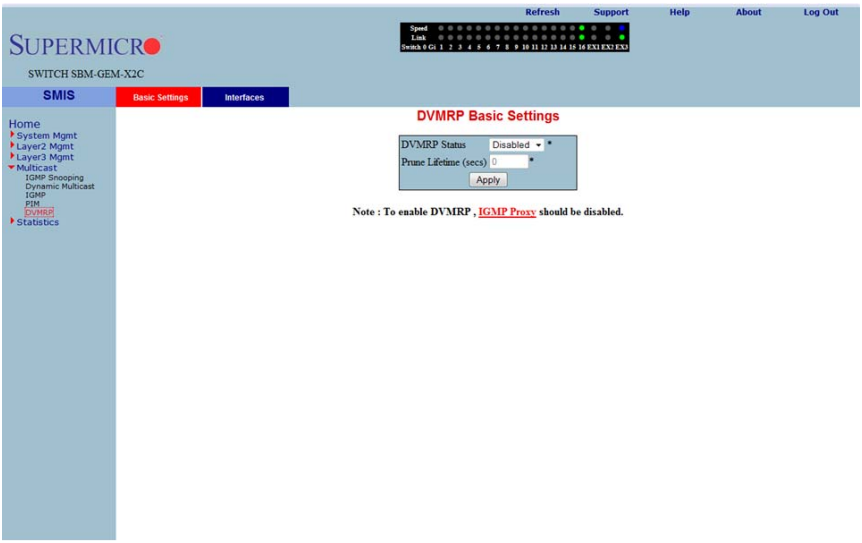
DVMRP

The DVMRP page allows you to configure the DVMRP protocol using the following pages:

- DVMRP Basic Settings
- Interfaces

DVMRP Basic Settings

Figure 5-159. DVMRP Basic Settings Page



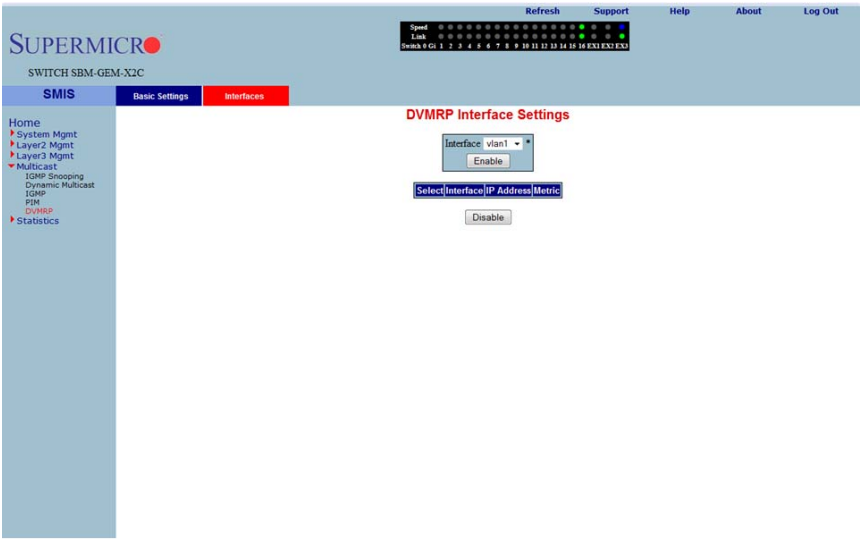
Clicking the BASIC SETTINGS tab brings up the DVMRP BASIC SETTINGS page (Figure 5-159). The parameters for this page are shown in Table 5-131.

Table 5-131. 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.

Interfaces

Figure 5-160. DVMRP Interface Settings Page



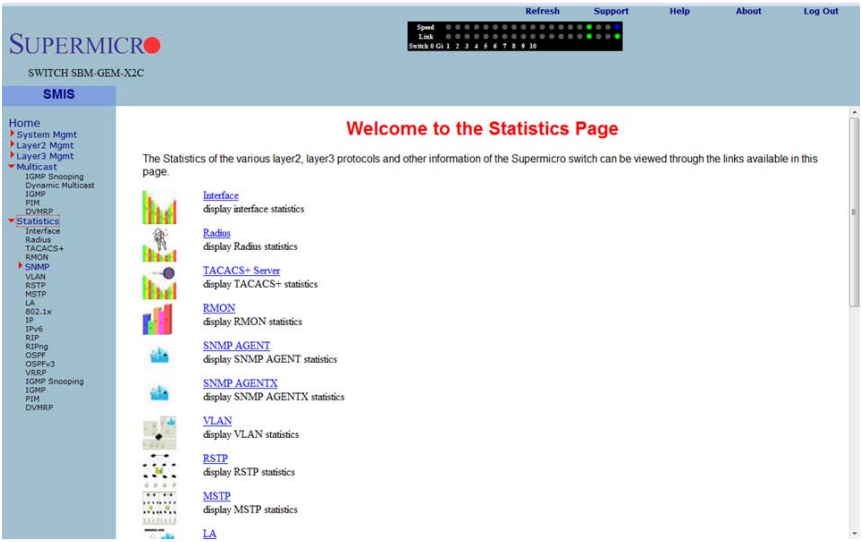
Clicking the INTERFACES tab brings up the DVMRP INTERFACE SETTINGS page (Figure 5-160), which displays the various parameters XXXXXX. The parameters for this page are shown in Table 5-132.

Table 5-132. DVMRP Interface Settings Page Parameters

Parameter	Description
Interface	This parameter specifies the Interface Index.
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 5-161. Statistics Home Page



The STATISTICS HOME page (Figure 5-161) 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 Statistics
- RIP6
- OSPF
- OSPFv3
- VRRP Statistics
- IGMP Snooping

- IGMP Statistics
- PIM
- DVMRP

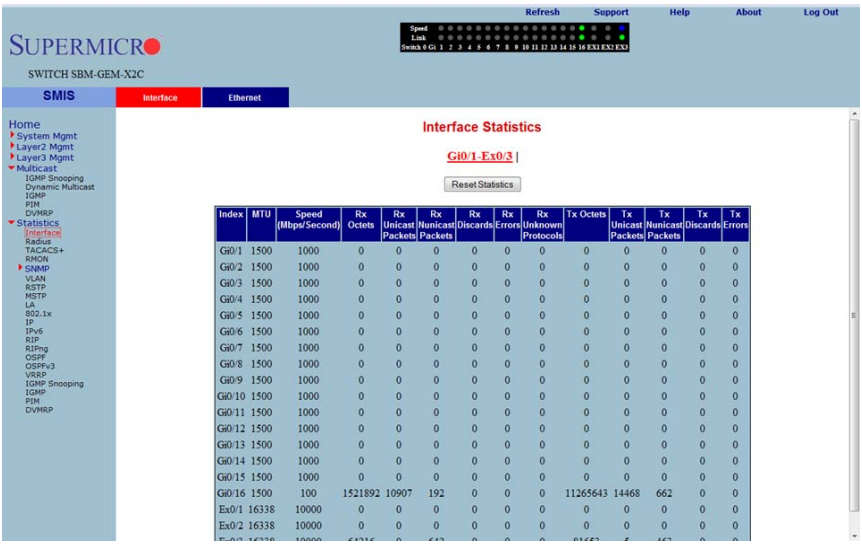
Interface

The Interface link allows you to configure the following pages:

- Interface Statistics
- Ethernet Statistics

Interface Statistics

Figure 5-162. Interface Statistics Page



Clicking the INTERFACE tab brings up the INTERFACE STATISTICS page (Figure 5-162). The parameters for this page are shown in Table 5-133.

Table 5-133. Interface Statistics Page Parameters

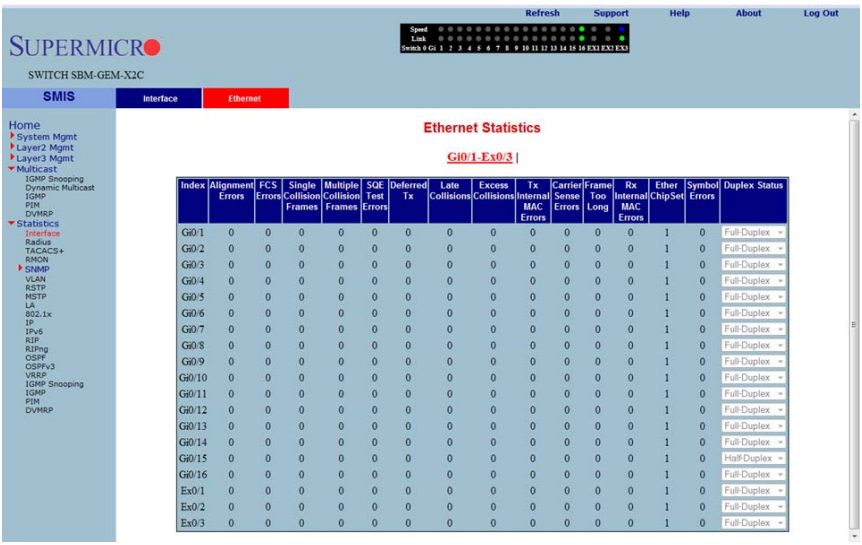
Parameter	Description
Index	This parameter specifies the Port index.
MTU	This parameter specifies the Max Transfer Unit bytes.
Speed (Bits Per Second)	This parameter specifies the port speed in bits per second.
Received Octets	This parameter specifies the number of bytes received.

Table 5-133. Interface Statistics Page Parameters (Continued)

Parameter	Description
Received Unicast Packets	This parameter specifies the number of unicast packets received.
Received Nunicast Packets	This parameter specifies the number of non-unicast packets received.
Received Discards	This parameter specifies the number of packets discared 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 Discards	This parameter specifies the number of packets discarded due to transmit errors.
Transmitted Errors	This parameter specifies the number of transmit errors.

Ethernet Statistics

Figure 5-163. Ethernet Statistics Page



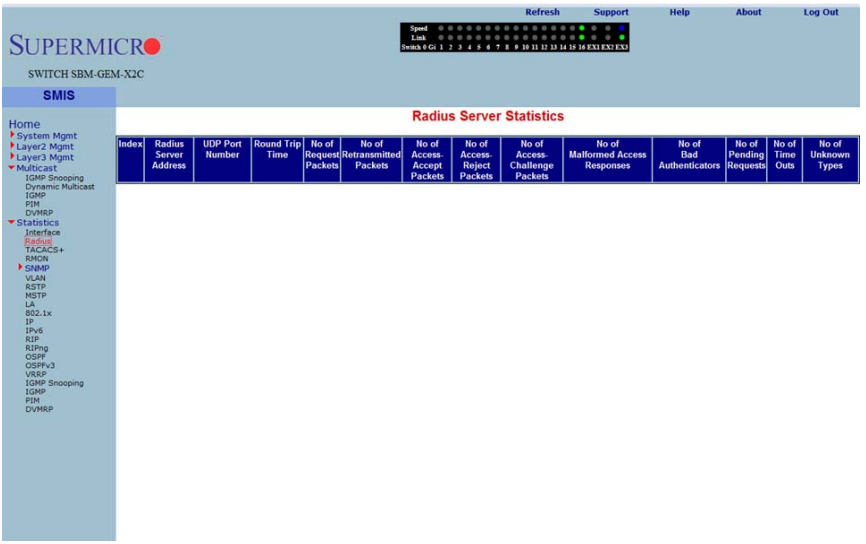
Clicking the ETHERNET tab brings up the ETHERNET STATISTICS page (Figure 5-163). The parameters for this page are shown in Table 5-134.

Table 5-134. Ethernet Statistics Page Parameters

Parameter	Description
Index	This parameter specifies the port index.
Alignment Errors	This parameter specifies the number of alignment errors. Alighment 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.
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.
Symbol Errors	This parameter specifies the number of symbol errors.
Duplex Status	This parameter specifies the current status of duplex.

Radius

Figure 5-164. Radius Server Statistics Page



Clicking the RADIUS link brings up the RADIUS SERVER STATISTICS page (Figure 5-164). The parameters for this page are shown in Table 5-135.

Table 5-135. Radius Server Statistics Page Parameters

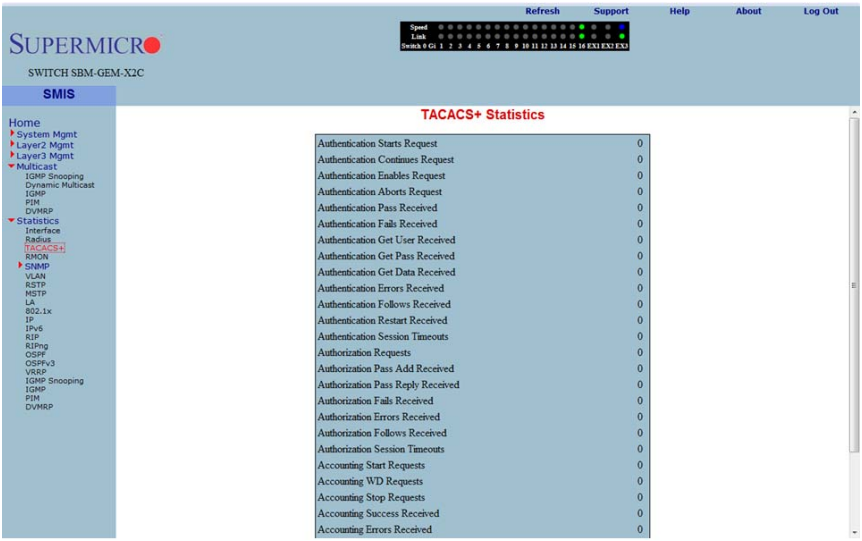
Parameter	Description
Index	This parameter specifies the port index.
Radius Server Address	This parameter specifies the RADIUS SERVER ADDRESS.
UDP Port Number	This parameter specifies the UDP PORT NUMBER.
Round Trip Time	This parameter displays the ROUND TRIP TIME in seconds.
No of Request Packets	This 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 5-135. 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 5-165. TACACS+ Statistics Page



Clicking the TACACS+ link brings up the TACACS+ STATISTICS page (Figure 5-165). The parameters for this page are shown in Table 5-136.

Table 5-136. TACACS+ Statistics Page Parameters

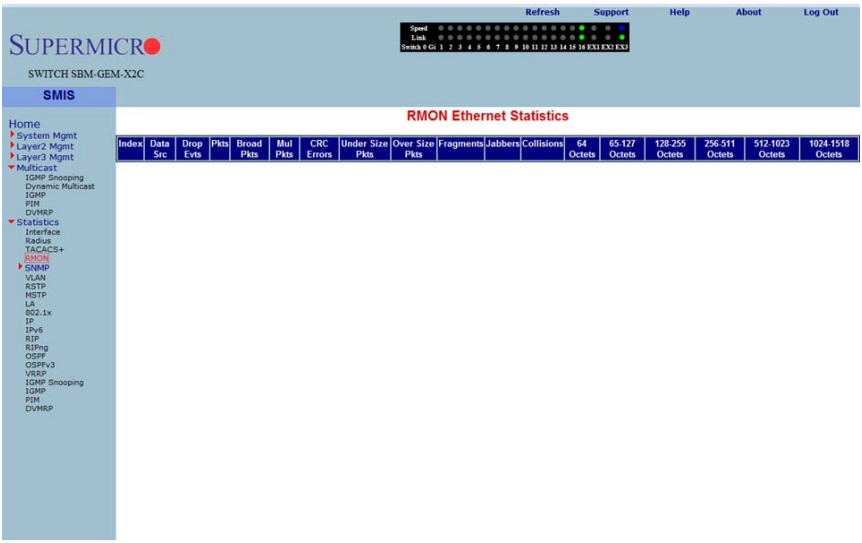
Parameter	Description
Authentication Starts Request	This parameter specifies the number of authentication starts requested.
Authentication Continues Request	This parameter specifies the number of authentication continues requested.
Authentication Enables Request	This parameter specifies the number of 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 5-136. 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.

RMON Ethernet Statistics

Figure 5-166. RMON Ethernet Statistics Page



Clicking the RMON link brings up the RMON ETHERNET STATISTICS page (Figure 5-166), which displays RMON Ethernet statistics information. The parameters for this page are shown in Table 5-137.

Table 5-137. 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 Packtes	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 5-137. 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.

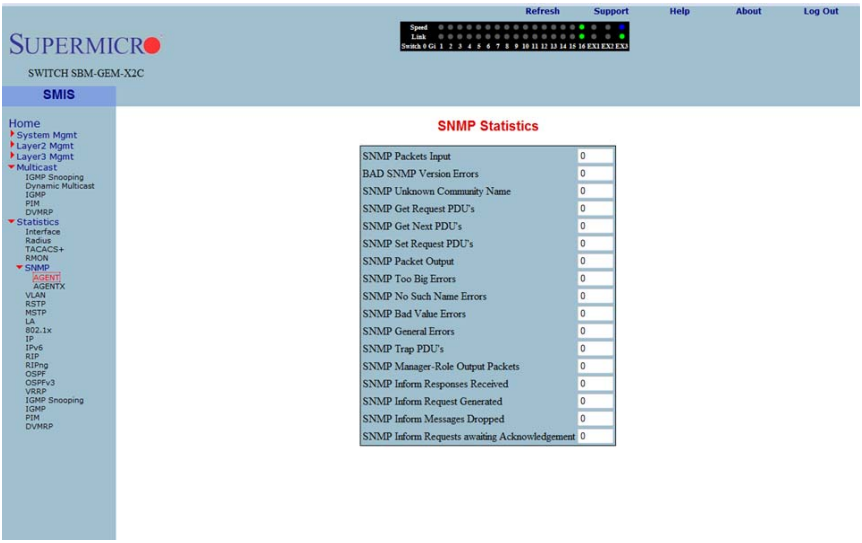
SNMP Statistics

The SNMP Statistics link allows you to configure SNMP Statistics through the following pages:

- Agent
- SNMP AgentX

Agent

Figure 5-167. SNMP Statistics Page



Clicking the SNMP AGENT link brings up the SNMP STATISTICS page (Figure 5-167), which displays SNMP statistics. The parameters for this page are shown in Table 5-138.

Table 5-138. 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 5-138. 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.

SNMP AgentX

Clicking the AGENTX link brings up the AGENTX SUBAGENT STATISTICS page (not shown), which displays Agentx Subagent information. The parameters for this page are shown in Table 5-139.

Table 5-139. 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.

Table 5-139. Agentx Subagent Statistics Page Parameters (Continued)

Parameter	Description
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.

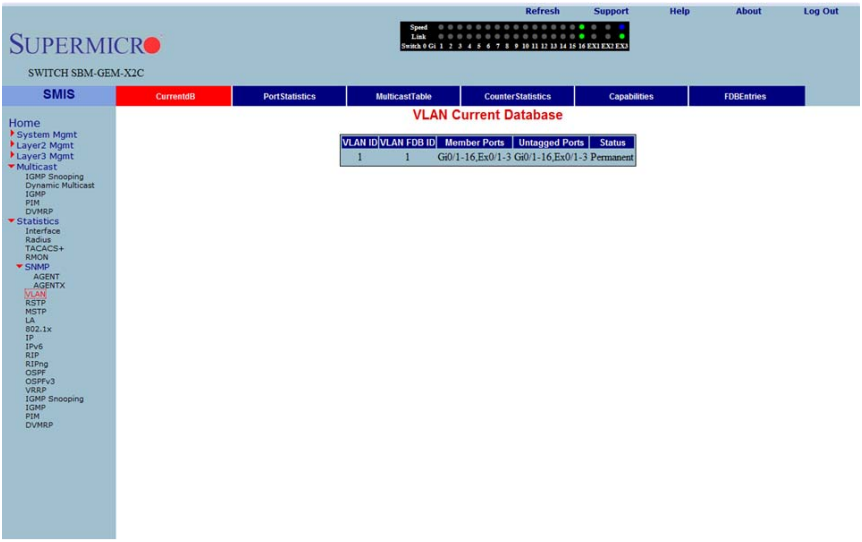
VLAN

The VLAN link allows you to view VLAN statistics through the following pages:

- Current DB
- VLAN Port Statistics
- VLAN Multicast Table
- VLAN Counter Statistics
- VLAN Capabilities
- VLAN FDB Entries

Current DB

Figure 5-168. VLAN Current Database Page



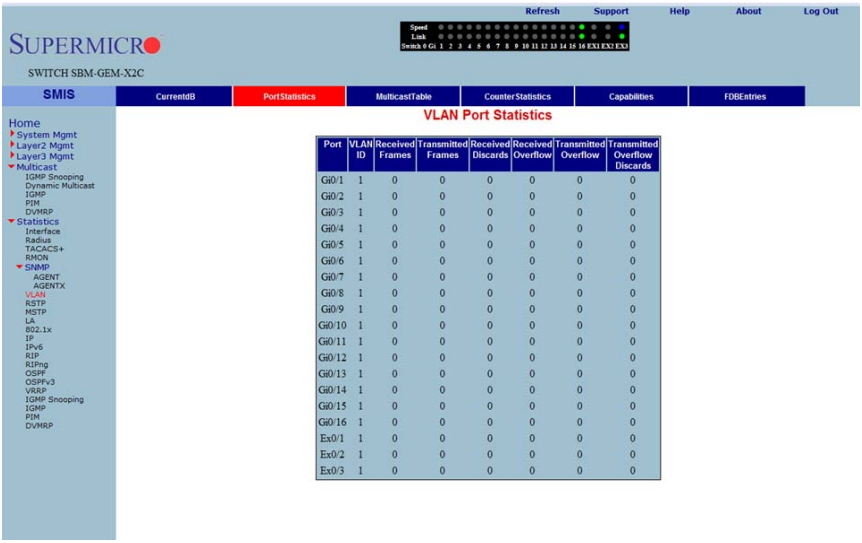
Clicking the CURRENT DB tab brings up the VLAN CURRENT DATABASE page (Figure 5-168), which displays VLAN database entries. The parameters for this page are shown in Table 5-140.

Table 5-140. VLAN Current Database Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifer.
VLAN FDB ID	This parameter specifies the VLAN filter database identifer.
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 VALN status.

VLAN Port Statistics

Figure 5-169. VLAN Port Statistics Page



Clicking the PORT STATISTICS tab brings up the VLAN PORT STATISTICS page (Figure 5-169), which displays the various parameters XXXXXX. The parameters for this page are shown in Table 5-141.

Table 5-141. VLAN Port Statistics Page Parameters

Parameter	Description
Port	This parameter specifies the port index.
VLAN ID	This parameter specifies the VLAN identifer.
Received Frames	This parameter specifies the number of packets received in this VLAN.
Transmitted Frames	This parameter specifies the number of packets transmitted in this VLAN.
Received Discards	This parameter specifies the number of received packets discarded.
Received Overflow	This parameter specifies the number of received overflow packets.
Transmitted Overflow	This parameter specifies the number of transmit overflows.
Transmitted Overflow Discards	This parameter specifies the number of transmit overflow discards.

VLAN Multicast Table

Figure 5-170. VLAN Multicast Table Page

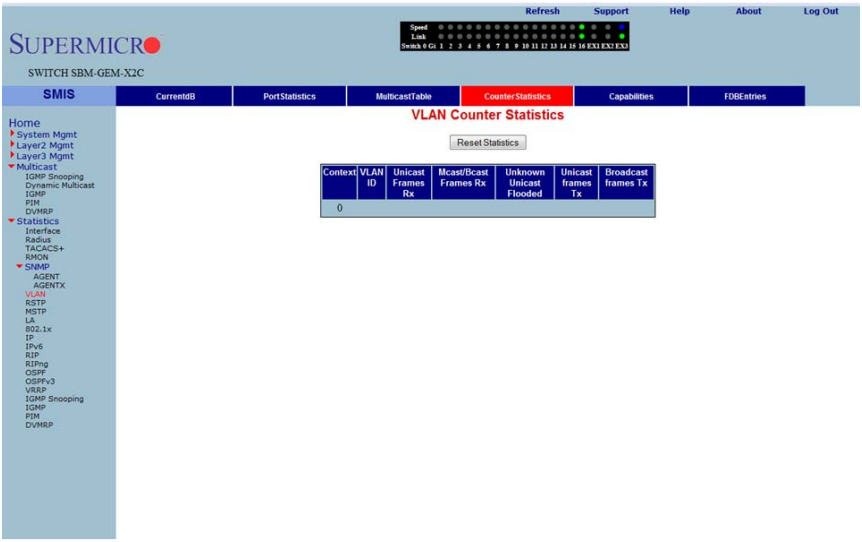
Clicking the MULTICAST TABLE tab brings up the VLAN MULTICAST TABLE page (Figure 5-170), which displays multicast VLAN information. The parameters for this page are shown in Table 5-142.

Table 5-142. VLAN Multicast Table Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifer.
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.

VLAN Counter Statistics

Figure 5-171. VLAN Counter Statistics Page



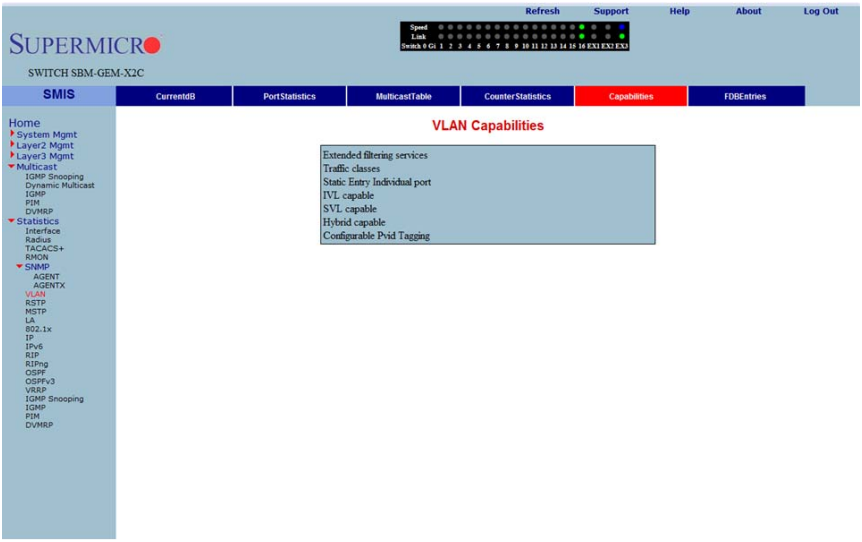
Clicking the COUNTER STATISTICS link brings up the VLAN COUNTER STATISTICS page (Figure 5-171), which displays VLAN counters. The parameters for this page are shown in Table 5-143.

Table 5-143. VLAN Counter Statistics Page Parameters

Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
Unicast Frames Rx	This parameter specifies the number of unicast packets received.
Mcast/Bcast Frames Rx	This parameter specifies the number of non-unicast packets received.
Unknown Unicast Flooded	This parameter specifies the number of packets flooded due to unknown unicast.
Unicast frames Tx	This parameter specifies the number of unicast packets transmitted.
Broadcast frames Tx	This parameter specifies the number of broadcast packets transmitted.

VLAN Capabilities

Figure 5-172. VLAN Capabilities Page



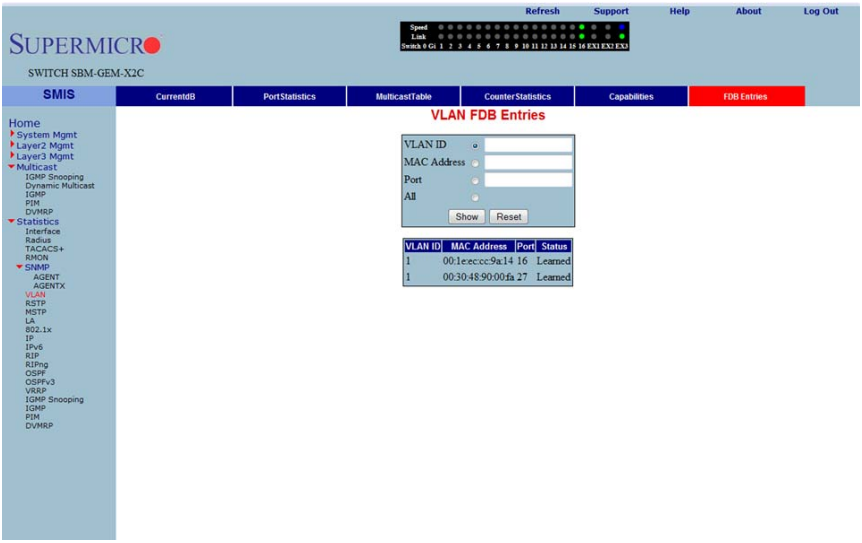
Clicking the CAPABILITIES tab brings up the VLAN CAPABILITIES page (Figure 5-172), which displays the VLAN capabilities of the switch. The parameters for this page are shown in Table 5-144.

Table 5-144. 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.

VLAN FDB Entries

Figure 5-173. VLAN FDB Entries Page



Clicking the FDB ENTRIES tab brings up the VLAN FDB ENTRIES page (Figure 5-173), which displays VLAN filter database entries. The parameters for this page are shown in Table 5-145.

Table 5-145. VLAN FDB 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.

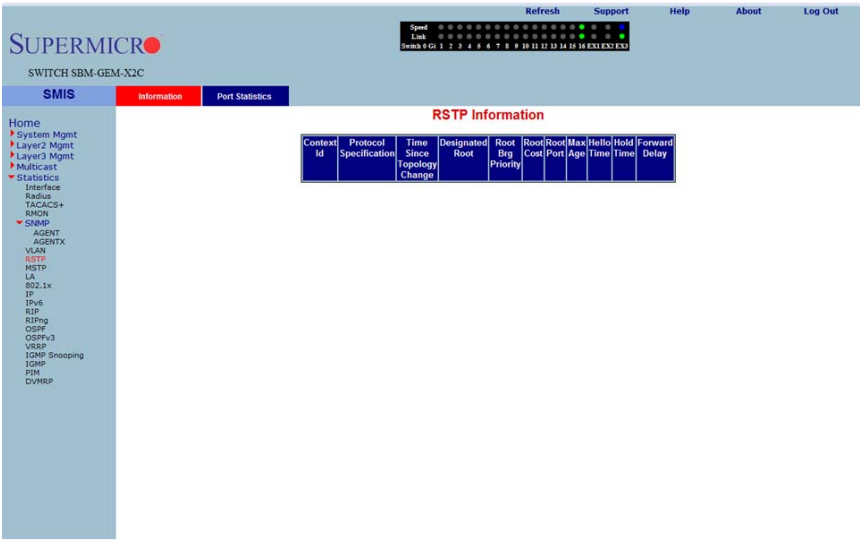
RSTP Statistics

The RSTP STATISTICS link allows you to view RSTP statistics through the following pages:

- RSTP Information
- RSTP Port Statistics

RSTP Information

Figure 5-174. RSTP Information Page



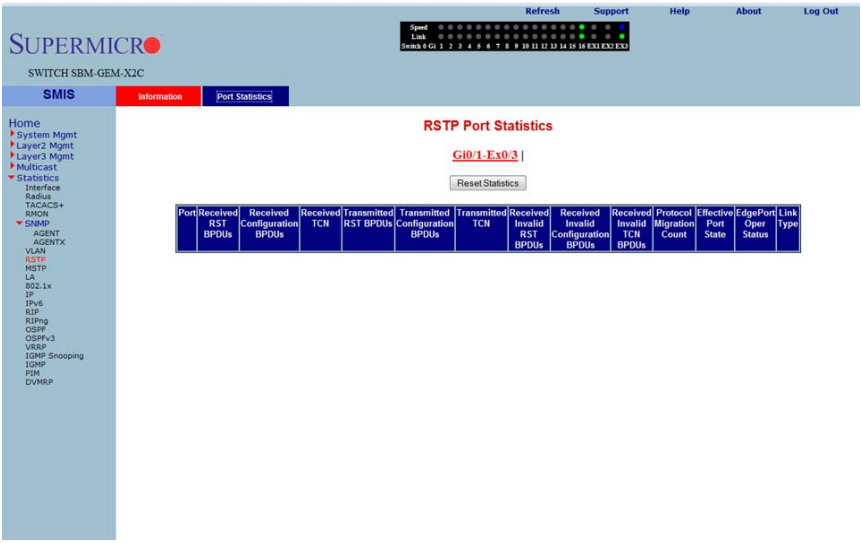
Clicking the INFORMATION tab brings up the RSTP INFORMATION page (Figure 5-174), which displays RSTP statistics. The parameters for this page are shown in Table 5-146.

Table 5-146. RSTP Information Page Parameters

Parameter	Description
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.

RSTP Port Statistics

Figure 5-175. RSTP Port Statistics Page



Clicking the PORT STATISTICS tab brings up the RSTP PORT STATISTICS page (Figure 5-175), which displays RSTP port level statistics. The parameters for this page are shown in Table 5-147.

Table 5-147. 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 5-147. 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.

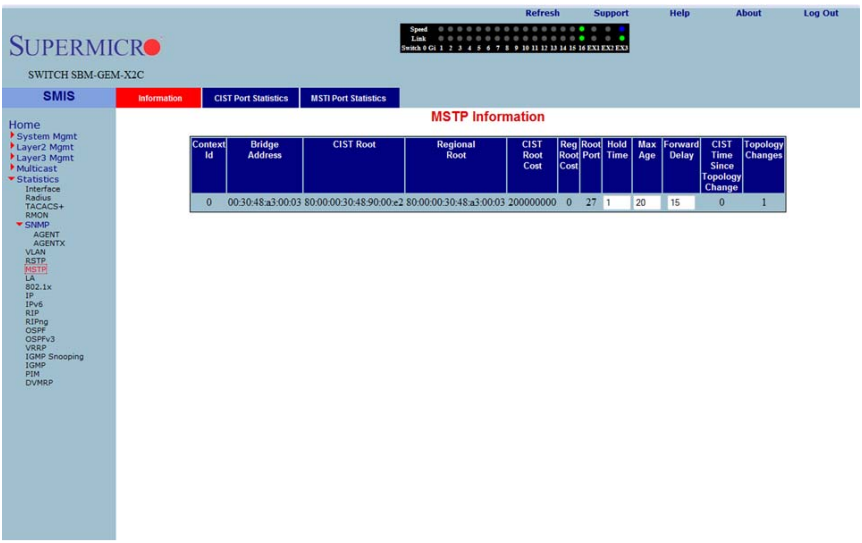
MSTP Statistics

The MSTP Statistics link allows you to view MSTP statistics through the following pages:

- MSTP Information
- MSTP CIST Statistics
- MSTP MSTI Port Statistics

MSTP Information

Figure 5-176. MSTP Information Page



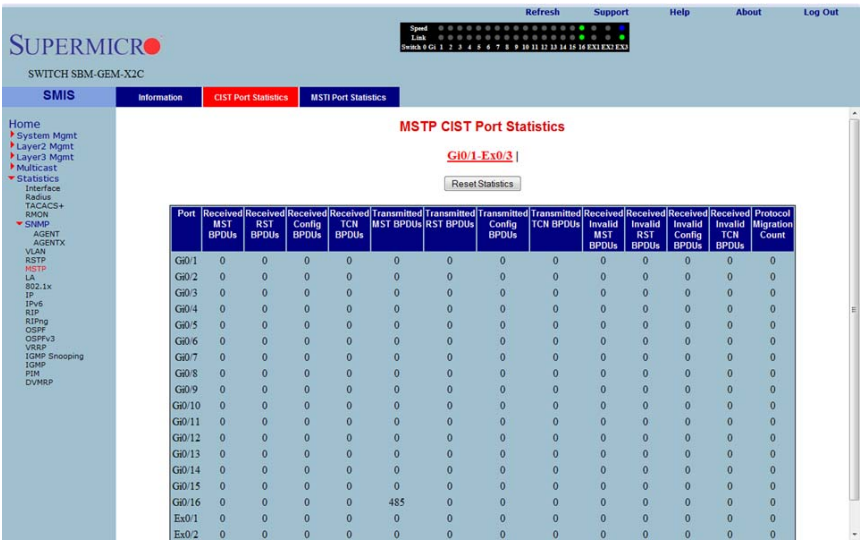
Clicking the INFORMATION tab brings up the MSTP INFORMATION page (Figure 5-132), which displays MSTP statistics. The parameters for this page are shown in Table 5-12.

Table 5-148. MSTP Information Page Parameters

Parameter	Description
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.

MSTP CIST Statistics

Figure 5-177. MSTP CIST Port Statistics Page



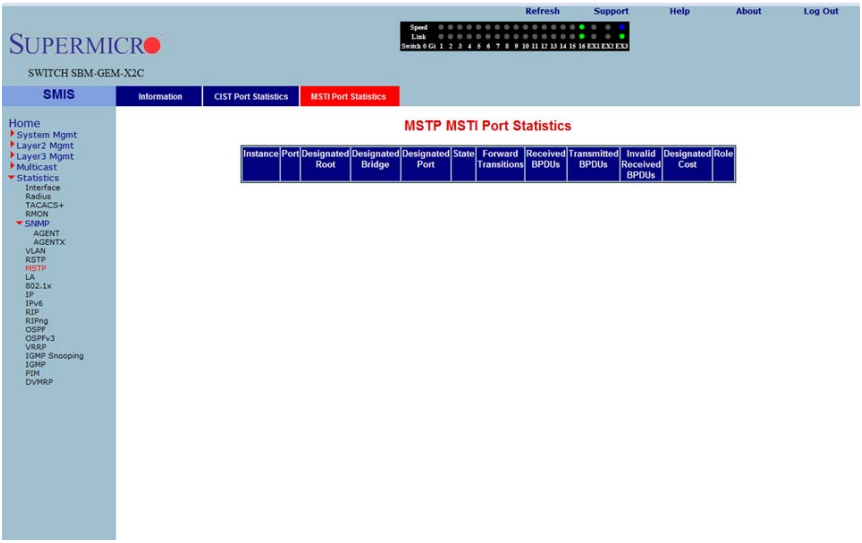
Clicking the CIST PORT STATISTICS tab brings up the MSTP CIST PORT STATISTICS page (Figure 5-177), which displays STP CIST port level statistics. The parameters for this page are shown in Table 5-149.

Table 5-149. 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.

MSTP MSTI Port Statistics

Figure 5-178. MSTP MSTI Port Statistics Page



Clicking the MSTI PORT STATISTICS tab brings up the MSTP MSTI PORT STATISTICS page (Figure 5-178), which displays MSTP MSTI port level statistics. The parameters for this page are shown in Table 5-150.

Table 5-150. MSTP MSTI Port Statistics Page Parameters

Parameter	Description
Instance	This parameter specifies the MSTP instance Identifer.
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.

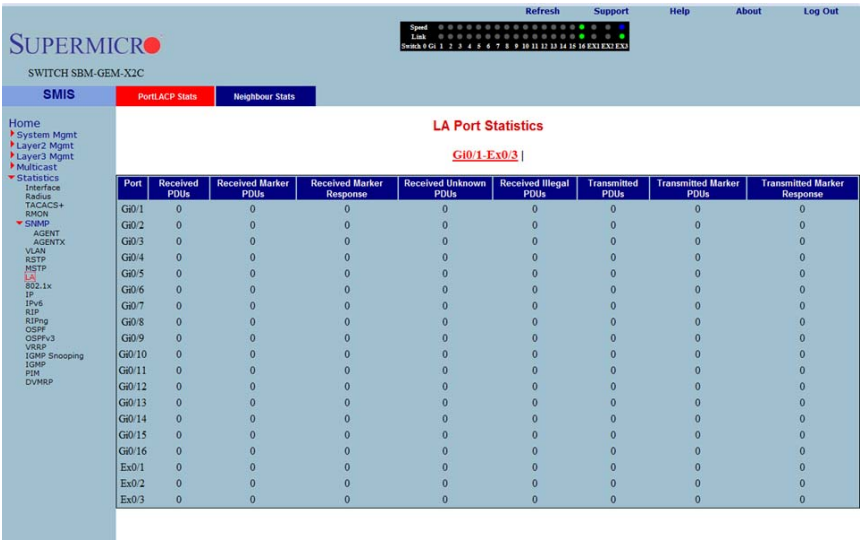
Link Aggregation (LA)

The Link Aggregation link allows you to view Link Aggregation (LA) statistics through the following pages:

- LA Port Statistics
- LA Neighbor Statistics

LA Port Statistics

Figure 5-179. LA Port Statistics Page



Clicking the PORT LACP STATS tab brings up the LA PORT STATISTICS page (Figure 5-179), which displays LACP port level statistics. The parameters for this page are shown in Table 5-151.

Table 5-151. LA Port Statistics Page Parameters

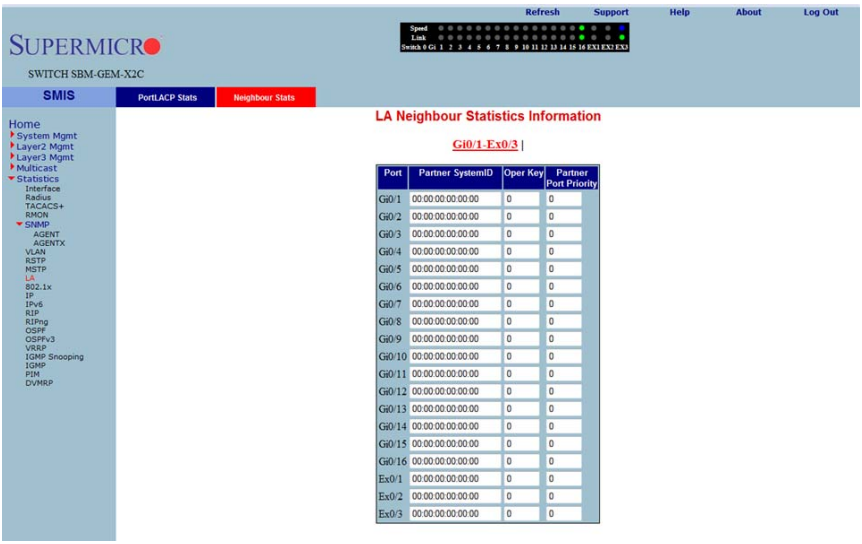
Parameter	Description
Port	This parameter specifies the port index.
Received PDUs	This parameter specifies the number of LACP PDUs received.
Received Marker PDUs	This parameter specifies the number of Marker PDUs received.
Received Marker Response	This parameter specifies the number of Marker response PDUs received.
Received Unknown PDUs	This parameter specifies the number of unknown PDUs received.

Table 5-151. 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.

LA Neighbor Statistics

Figure 5-180. LA Neighbor Statistics Information Page



Clicking the NEIGHBOR STATS tab brings up the LA NEIGHBOR STATISTICS INFORMATION page (Figure 5-180), which displays LACP neighbor statistics. The parameters for this page are shown in Table 5-152.

Table 5-152. 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.

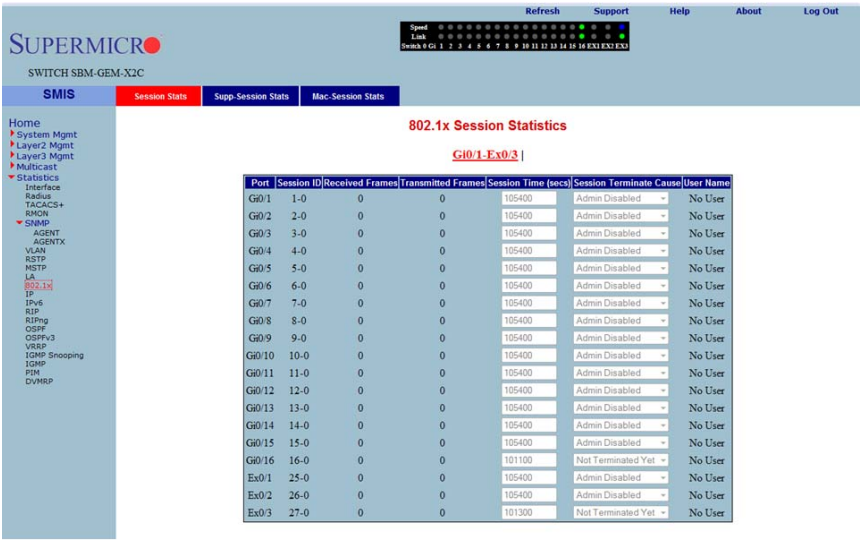
802.1X

The 802.1x link allows you to view 802.1x statistics through the following pages:

- 802.1X Session Statistics
- 802.1X Supplicant Statistics
- Mac Session Statistics

802.1X Session Statistics

Figure 5-181. 802.1x Session Statistics Page



Clicking the SESSION STATS tab brings up the 802.1X SESSION STATISTICS page (Figure 5-181), which displays 802.1x statistics information. The parameters for this page are shown in Table 5-153.

Table 5-153. 802.1x Session Statistics Page Parameters

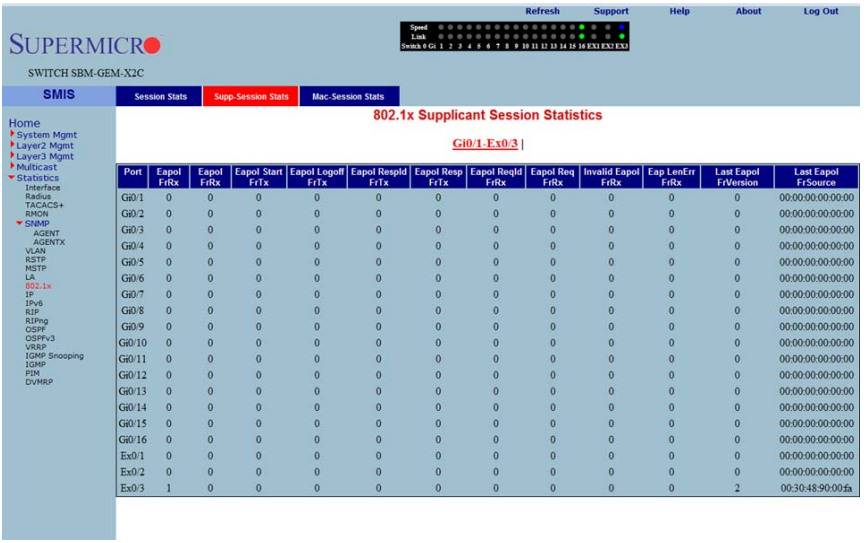
Parameter	Description
Port	This parameter specifies the port index.
Session ID	This parameter specifies the session identifier.
Received Frames	This parameter specifies the number of packets received.
Transmitted Frames	This parameter specifies the number of packets transmitted.
Session Time (secs)	This parameter specifies the session time in seconds.

Table 5-153. 802.1x Session Statistics Page Parameters (Continued)

Parameter	Description
Session Terminate Cause	This parameter specifies the reason for session termination.
User Name	This parameter specifies the name of the user authenticated.

802.1X Supplicant Statistics

Figure 5-182. 802.1x Supplicant Session Statistics Page



Clicking the SUPP SESSION STATS tab brings up the 802.1X SUPPLICANT SESSION STATISTICS page (Figure 5-182), which displays information about the 802.1x supplicant session. The parameters for this page are shown in Table 5-154.

Table 5-154. 802.1x Supplicant Session Statistics Page Parameters

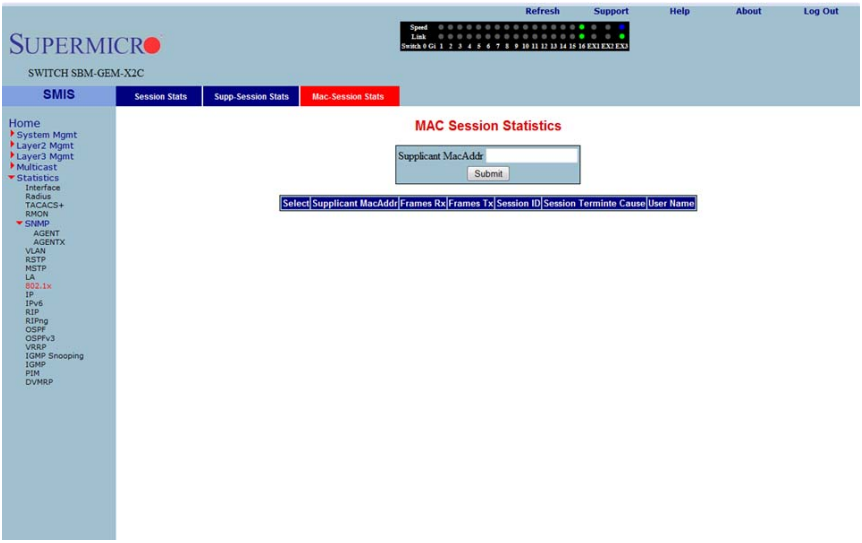
Parameter	Description
Port	This parameter specifies the port index.
Eapol FrRx	This parameter specifies the number of the EAPOL packets received.
Eapol FrTx	This parameter specifies the number of the EAPOL packets transmitted.
Eapol Start FrTx	This parameter specifies the number of the EAPOL start packet transmitted.
Eapol Logoff FrTx	This parameter specifies the number of the EAPOL logoff packet transmitted.
Eapol RespId FrTx	This parameter specifies the number of the EAPOL response identifier packet transmitted.

Table 5-154. 802.1x Supplicant Session Statistics Page Parameters (Continued)

Parameter	Description
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 receieved.
Invalid Eapol FrRx	This parameter specifies the number of the invalid EAPOL frame received.
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 Statistics

Figure 5-183. MAC Session Statistics Page



Clicking the MAC SESSION STATS tab brings up the MAC SESSION STATISTICS page (Figure 5-183), which displays statistics information about 802.1x MAC sessions. The parameters for this page are shown in Table 5-155.

Table 5-155. 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 Terminte Cause	This parameter specifies the reason for session termination.
User Name	This parameter specifies the name of user authenticated.

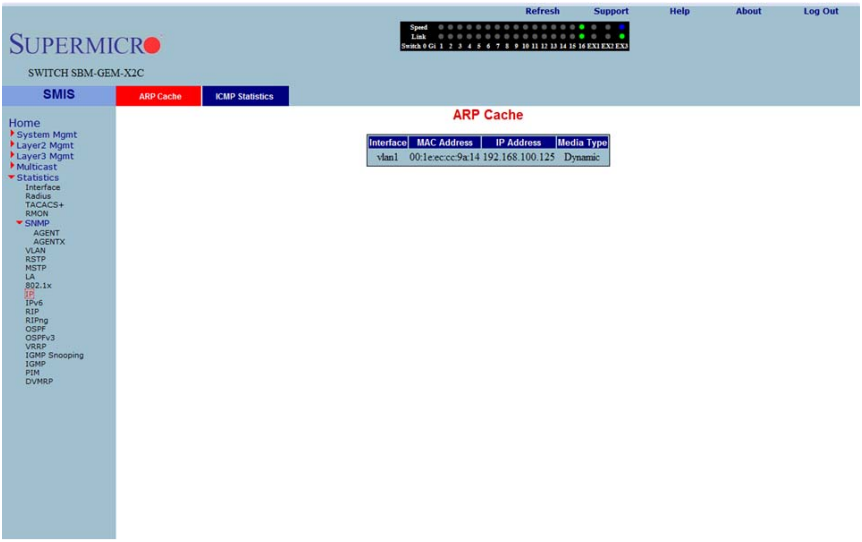
IP

The IP link allows you to view IP statistics through the following pages:

- ARP Cache
- ICMP Statistics

ARP Cache

Figure 5-184. ARP Cache Page



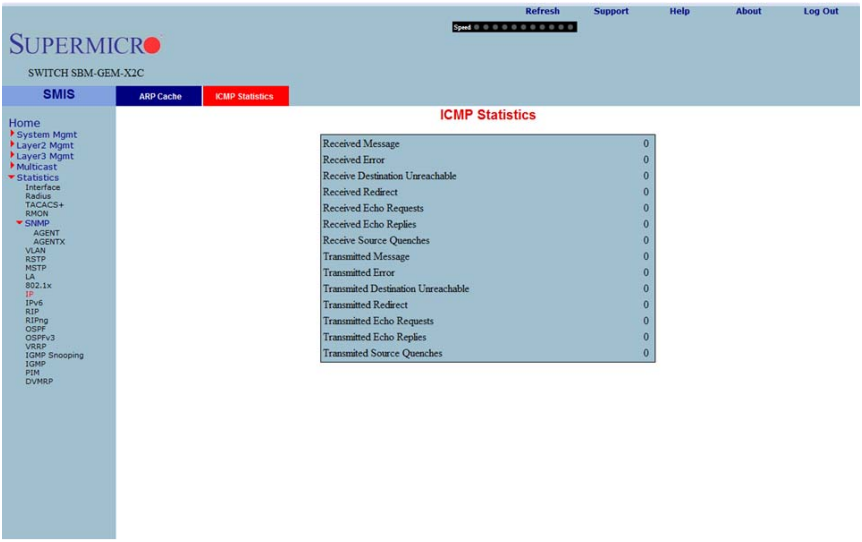
Clicking the ARP CACHE tab brings up the ARP CACHE page (Figure 5-184), which displays ARP entries. The parameters for this page are shown in Table 5-156.

Table 5-156. 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 5-185. ICMP Statistics Page



Clicking the ICMP STATISTICS tab brings up the ICMP STATISTICS page (Figure 5-185), which displays ICMP statistics information. The parameters for this page are shown in Table 5-157.

Table 5-157. 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 transmited messages.
Transmitted Error	This parameter specifies the number of transmitted errors.

Table 5-157. ICMP Statistics Page Parameters (Continued)

Parameter	Description
Transmitted Destination Unreachable	This parameter specifies the number of transmitted destination unreachables.
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.
Transmited Source Quenches	This parameter specifies the number of transmitted source quenches.

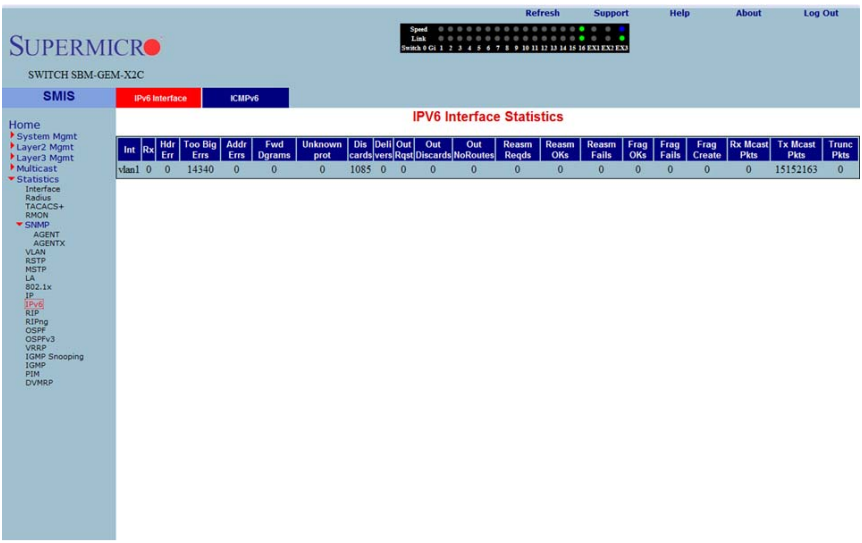
IPv6

The IPv6 link allows you to view IPv6 statistics through the following pages:

- IP V6 Interface Statistics
- ICMP V6 Statistics

IP V6 Interface Statistics

Figure 5-186. IPV6 Interface Statistics Page



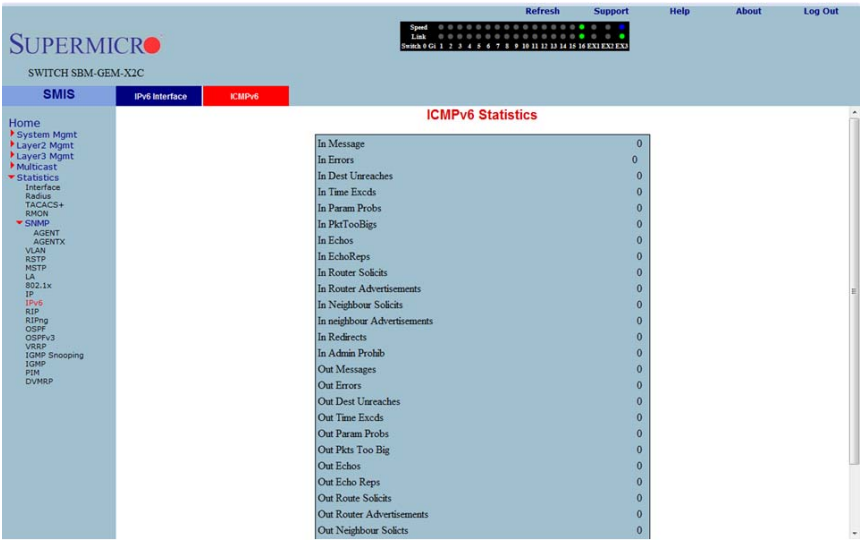
Clicking the IPV6 INTERFACE tab brings up the IPV6 INTERFACE STATISTICS page (Figure 5-186), which displays IPv6 port statistics. The parameters for this page are shown in Table 5-158.

Table 5-158. 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.
Discdrs	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 or 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.

ICMP V6 Statistics

Figure 5-187. ICMPv6 Statistics Page



Clicking the ICMPv6 tab brings up the ICMPv6 STATISTICS page (Figure 5-187), which displays ICMPv6 statistics. The parameters for this page are shown in Table 5-159.

Table 5-159. 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 solicits.
In Router Advertisements	This parameter specifies the number of routers advertisement received.
In Neighbor Solicits	This parameter specifies the number of received neighbor solicits.
In Neighbor Advertisements	This parameter specifies the number of received neighbor solicits.

Table 5-159. 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 prohibted.
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 Solicts	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 prohibted.
In Bad Code	This parameter specifies the number of bad code packets.

RIP Statistics

Figure 5-188. RIP Interface Statistics Page

Clicking the RIP link brings up the RIP INTERFACE STATISTICS page (Figure 5-188), which displays RIP statistics. The parameters for this page are shown in Table 5-160.

Table 5-160. 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.

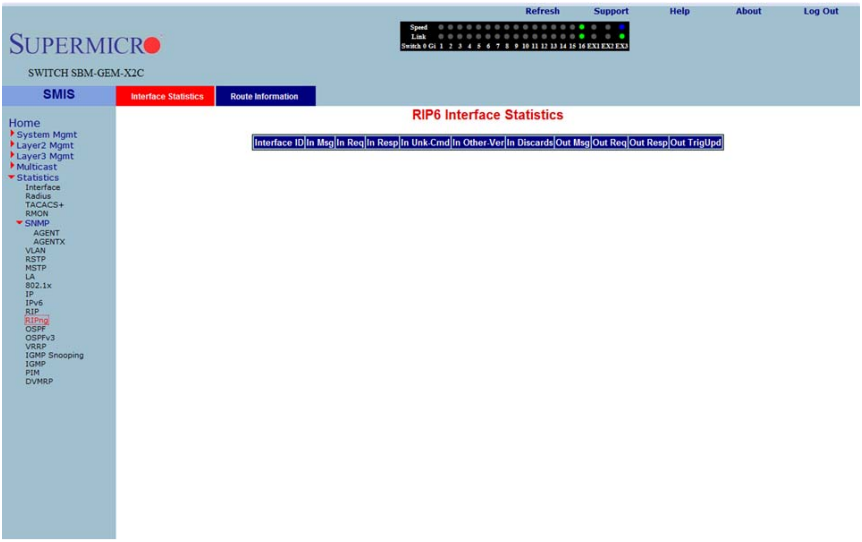
RIP6

The RIP6 link allows you to view RIP6 statistics through the following pages:

- RIP6 Interface Statistics
- RIP6 Route Information

RIP6 Interface Statistics

Figure 5-189. RIP6 Interface Statistics Page



Clicking the INTERFACE STATISTICS tab brings up the RIP6 INTERFACE STATISTICS page (Figure 5-189), which displays RIPng statistics. The parameters for this page are shown in Table 5-161.

Table 5-161. 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 resonse 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.

RIP6 Route Information

Figure 5-190. RIP6 Route Information Page

Clicking the ROUTE INFORMATION tab brings up the RIP6 ROUTE INFORMATION page (Figure 5-190), which displays information about RIPng routes. The parameters for this page are shown in Table 5-162.

Table 5-162. 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:

- OSPF Route Information
- OSPF Link State DB

OSPF Route Information

Figure 5-191. OSPF Route Information Page

Clicking the ROUTE INFORMATION tab brings up the OSPF ROUTE INFORMATION page (Figure 5-191), which displays information about OSPF routes. The parameters for this page are shown in Table 5-163.

Table 5-163. 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.

OSPF Link State DB

Figure 5-192. OSPF Link State Database Page

Clicking the LINK STATE DATABASE tab brings up the OSPF LINK STATE DATABASE page (Figure 5-192), which displays information about OSPF link state database. The parameters for this page are shown in Table 5-164.

Table 5-164. 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 identifer.
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 DB

OSPFV3 Route Information

Figure 5-193. OSPFV3 Route Information Page

Clicking the OSPFV3 ROUTE INFORMATION tab brings up the OSPFV3 ROUTE INFORMATION page (Figure 5-193), which displays information about OSPFV3 routes. The parameters for this page are shown in Table 5-165.

Table 5-165. 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 DB

Figure 5-194. OSPFV3 Link State Database Page

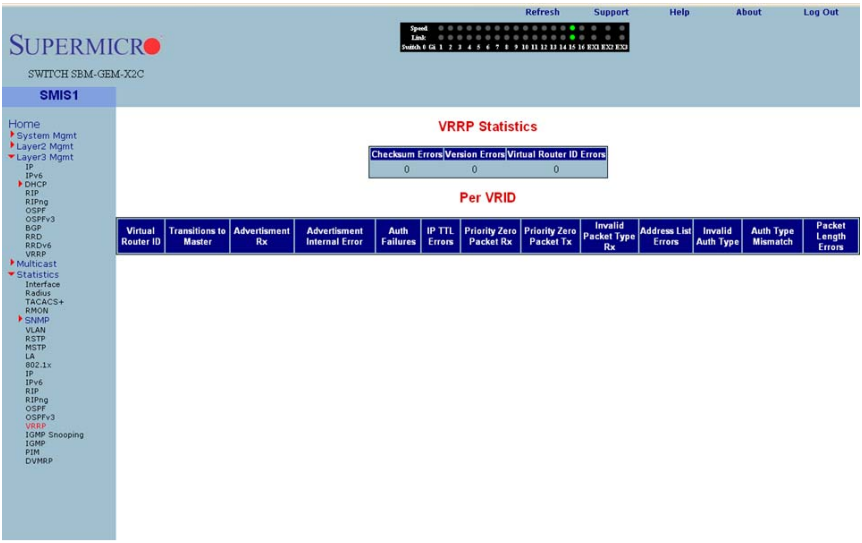
Clicking the OSPFV3 LINK STATE DATABASE tab brings up the OSPFV3 LINK STATE DATABASE page (Figure 5-194), which displays information about OSPF link state database. The parameters for this page are shown in Table 5-166.

Table 5-166. 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 Statistics

Figure 5-195. VRRP Statistics Page



Clicking the VRRP link brings up the VRRP STATISTICS page (Figure 5-195), which displays VRRP global statistics and VRRP router specific statistics. The parameters for this page are shown in Table 5-167.

Table 5-167. 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.
Advertisment Receive	This parameter specifies the number of advertisement packets received.
Advertisment 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 5-167. VRRP Statistics Page Parameters (Continued)

Parameter	Description
Priority Zero Packet Received	This parameter specifies the number of priority zero packets received.
Priority Zero Packet Transmited	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.

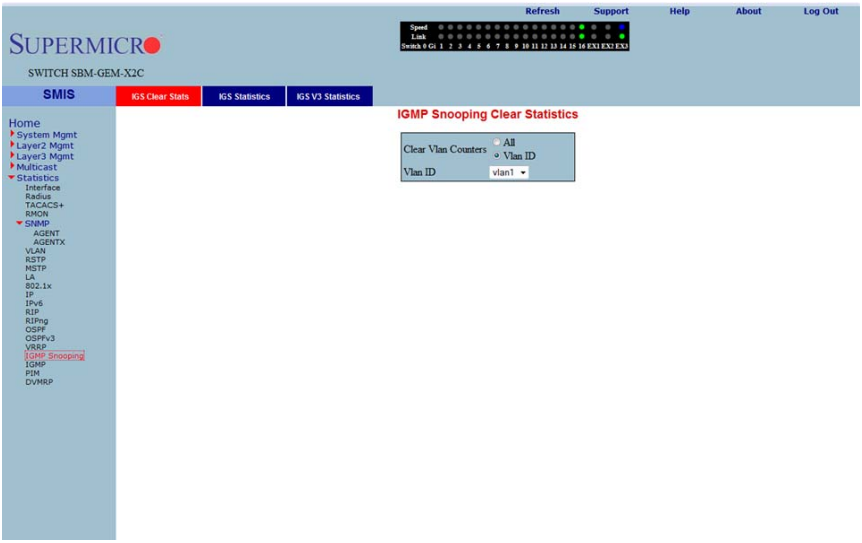
IGMP Snooping

The IGMP link allows you to view IGMP statistics through the following pages:

- IGMP Snooping Clear Statistics
- IGMP Snooping V1/V2 Statistics
- IGMP Snooping V3 Statistics

IGMP Snooping Clear Statistics

Figure 5-196. IGMP Snooping Clear Statistics Page



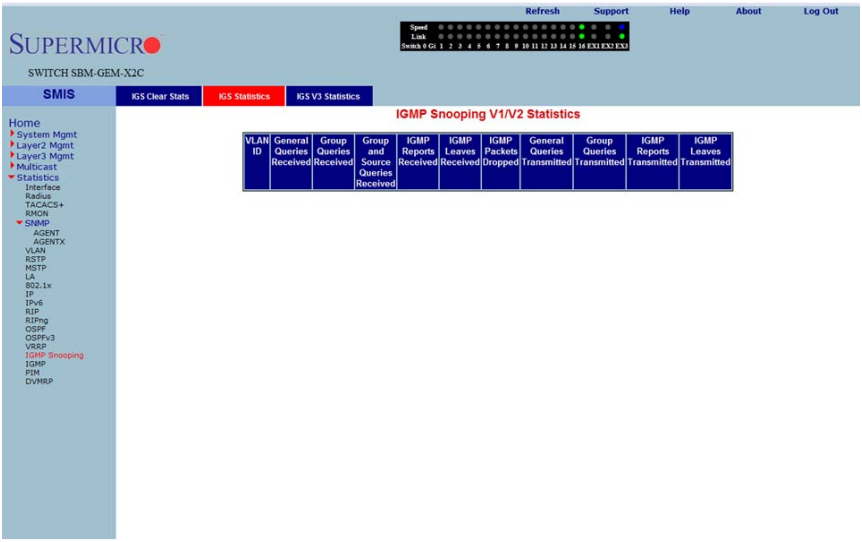
Clicking the IGS CLEAR STATS tab brings up the IGMP SNOOPING CLEAR STATISTICS page (Figure 5-196), which displays clearing IGMP snooping statistics. The parameters for this page are shown in Table 5-168.

Table 5-168. 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.

IGMP Snooping V1/V2 Statistics

Figure 5-197. IGMP Snooping V1/V2 Statistics Page



Clicking the IGS STATISTICS tab brings up the IGMP SNOOPING V1/V2 STATISTICS page (Figure 5-197), which displays IGMP snooping statistics. The parameters for this page are shown in Table 5-169.

Table 5-169. IGMP Snooping V1/V2 Statistics Page Parameters

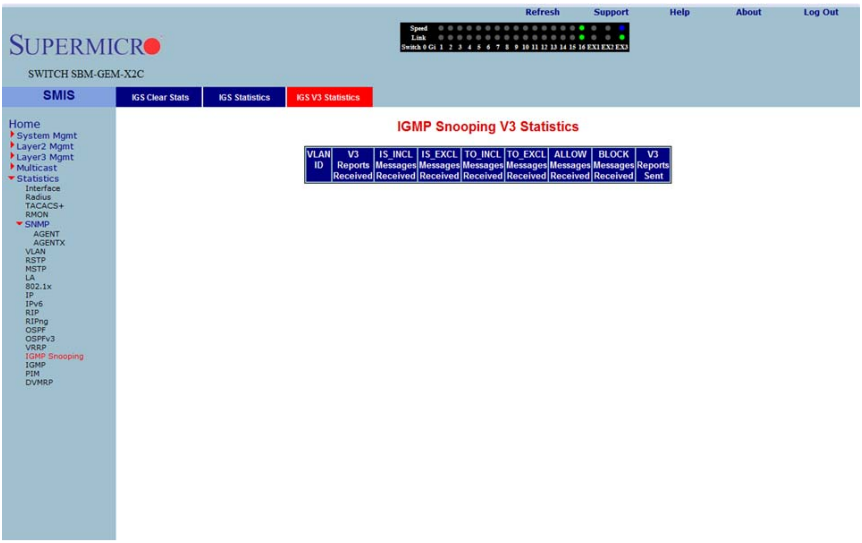
Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
General Queries Received	This parameter specifies the number of general query packets received.
Group Queries Received	This parameter specifies the number of group query packets received.
Group and Source Queries Received	This 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 5-169. 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.

IGMP Snooping V3 Statistics

Figure 5-198. IGMP Snooping V3 Statistics Page



Clicking the IGS V3 STATISTICS tab brings up the IGMP SNOOPING V3 STATISTICS page (Figure 5-198), which displays IGMP snooping V3 statistics information. The parameters for this page are shown in Table 5-170.

Table 5-170. IGMP Snooping V3 Statistics Page Parameters

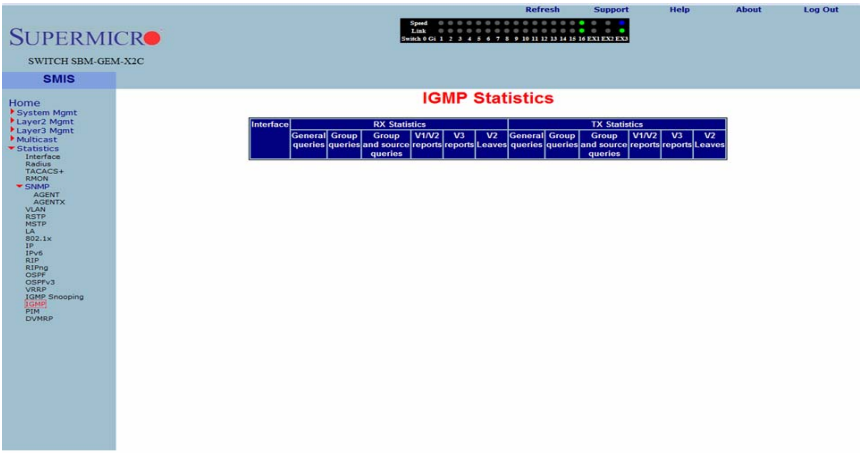
Parameter	Description
VLAN ID	This parameter specifies the VLAN identifier.
V3 Reports Received	This parameter specifies the number of Reports messages received.
IS_INCL Messages Received	This parameter specifies the number of messages received with is include field.
IS_EXCL Messages Received	This parameter specifies the number of messages received with is exclude field.

Table 5-170. 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 Statistics

Figure 5-199. IGMP Route StatisticsPage



Clicking the IGMP link brings up the IGMP ROUTE STATISTICS page (Figure 5-199), which displays IGMP route information. The parameters for this page are shown in Table 5-171.

Table 5-171. 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 5-171. 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.

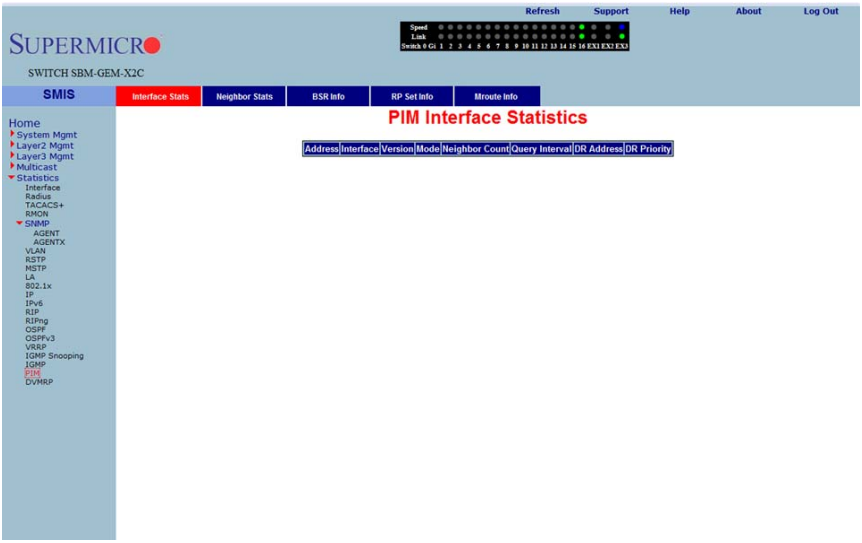
PIM

The PIM link allows you to view PIM statistics through the following pages:

- PIM Interface Statistics
- PIM Neighbor Statistics
- PIM BSR Info
- PIM RP Set Information
- PIM Route Information

PIM Interface Statistics

Figure 5-200. PIM Interface Statistics Page



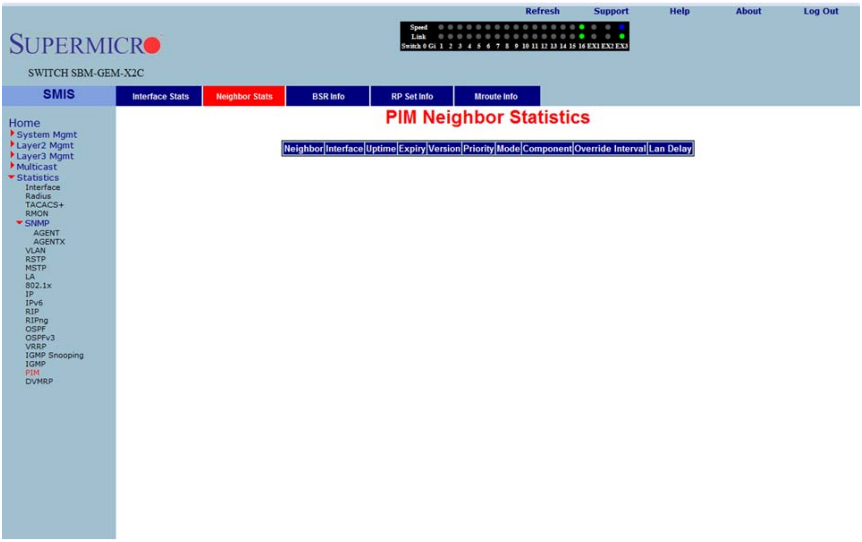
Clicking the INTERFACE STATS tab brings up the PIM INTERFACE STATISTICS page (Figure 5-200), which displays PIM interface statistics. The parameters for this page are shown in Table 5-172.

Table 5-172. 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.

PIM Neighbor Statistics

Figure 5-201. PIM Neighbor Statistics Page



Clicking the NEIGHBOR STATS tab brings up the PIM NEIGHBOR STATISTICS page (Figure 5-201), which displays PIM neighbor statistics. The parameters for this page are shown in Table 5-173.

Table 5-173. 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.

PIM BSR Info

Figure 5-202. PIM BSR Info Page

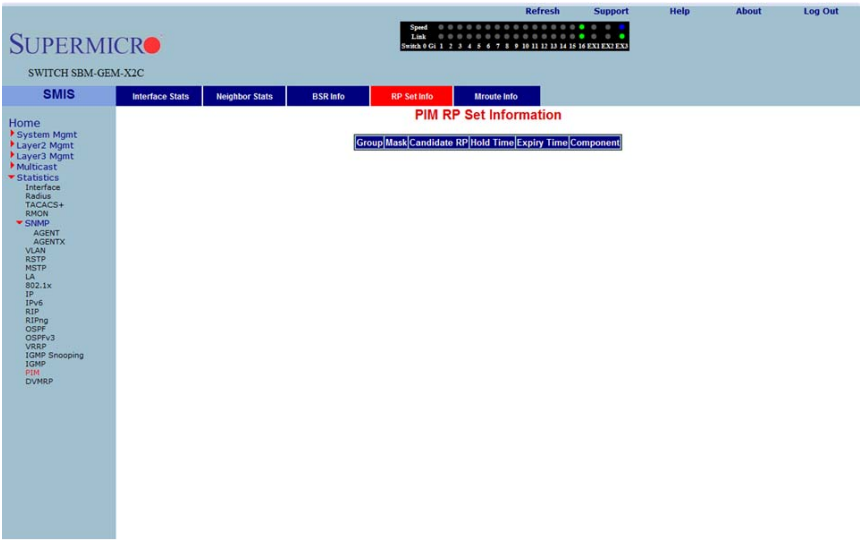
Clicking the BSR INFO tab brings up the PIM BSR INFO page (Figure 5-202). The parameters for this page are shown in Table 5-174.

Table 5-174. 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.

PIM RP Set Information

Figure 5-203. PIM RP Information Page



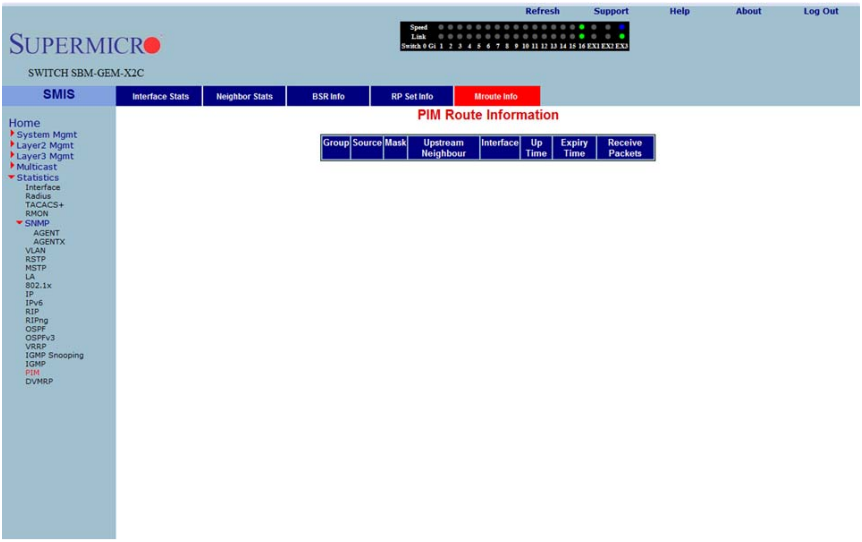
Clicking the RP SET INFO tab brings up the PIM RP INFORMATION page (Figure 5-203), which displays PIM RP information. The parameters for this page are shown in Table 5-175.

Table 5-175. 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.

PIM Route Information

Figure 5-204. PIM Route Information Page



Clicking the MROUTE INFO tab brings up the PIM ROUTE INFORMATION page (Figure 5-204), which displays PIM route information. The parameters for this page are shown in Table 5-176.

Table 5-176. PIM Route Information Page Parameters

Parameter	Description
Group	This parameter specifies the group address.
Source	This parameter specifies the source address.
Mask	This parameter specifies the PIM route mask.
Upstream Neighbor	This parameter specifies the upstream neighbor address.
Interface	This parameter specifies the
Up Time	This parameter specifies the up time in seconds.
Expiry Time	This parameter specifies the expiry time in seconds.
Receive Packets	This parameter specifies the number of packets received.

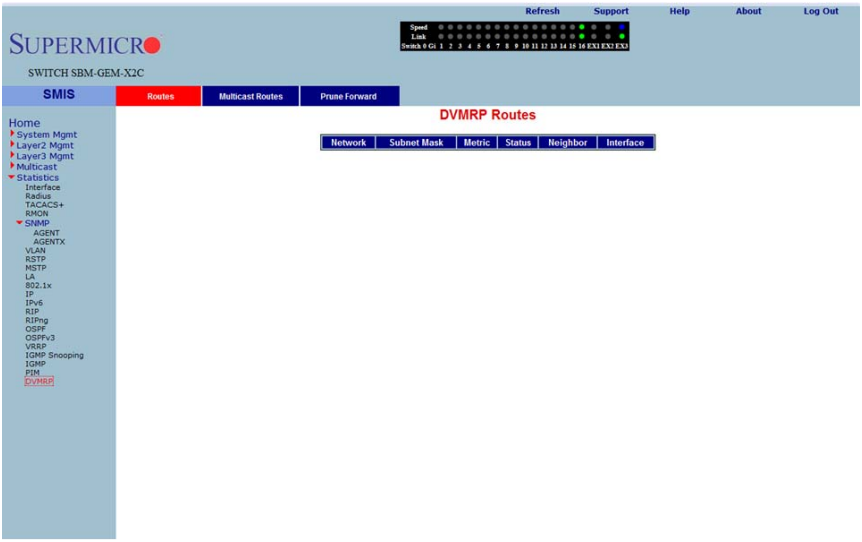
DVMRP

The DVMRP link allows you to view DVMRP statistics through the following pages:

- DVMRP Routers
- DVMRP Multicast Routers
- DVMRP Prune Statistics

DVMRP Routers

Figure 5-205. DVMRP Routes Page



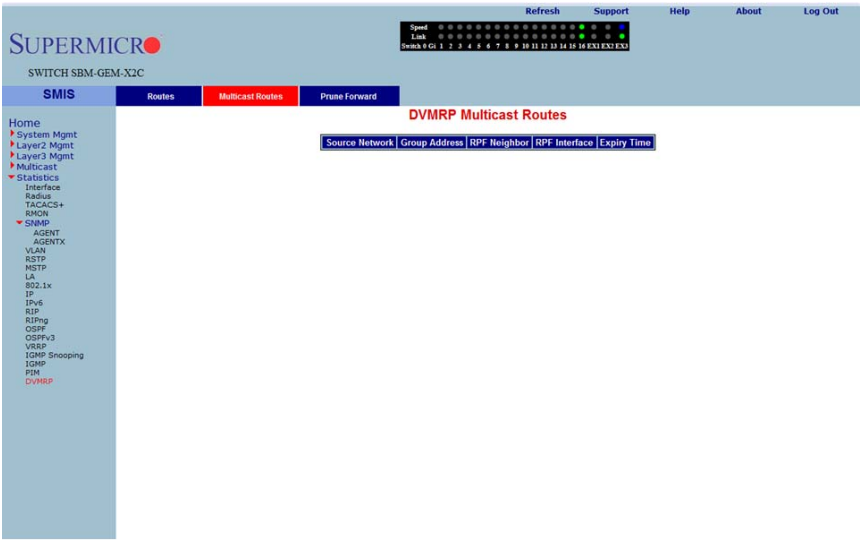
Clicking the ROUTES tab brings up the DVMRP ROUTES page (Figure 5-205), which displays DVMRP routes information. The parameters for this page are shown in Table 5-177.

Table 5-177. 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.

DVMRP Multicast Routers

Figure 5-206. DVMRP Multicast Routes Page



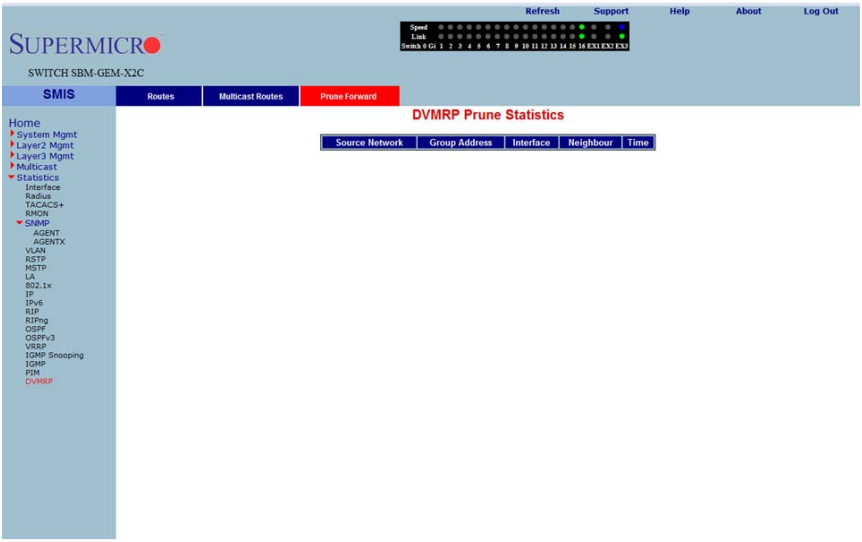
Clicking the MULTICAST ROUTES tab brings up the DVMRP MULTICAST ROUTES page (Figure 5-206), which displays DVMRP multicast routes information. The parameters for this page are shown in Table 5-178.

Table 5-178. 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.

DVMRP Prune Statistics

Figure 5-207. DVMRP Prune Statistics Page



Clicking the PRUNE FORWARD tab brings up the DVMRP PRUNE STATISTICS page (Figure 5-207), which DVMRP prune statistics information. The parameters for this page are shown in Table 5-179.

Table 5-179. 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.

Notes

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 (Tmra).

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.

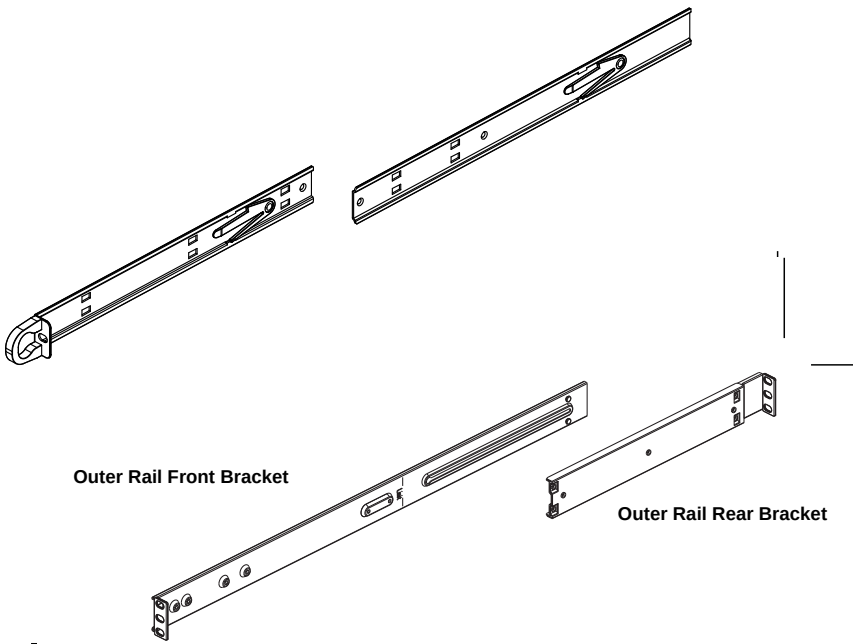
NOTE: This rail will fit a rack between 26" and 33.5" deep.

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. Silde 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.

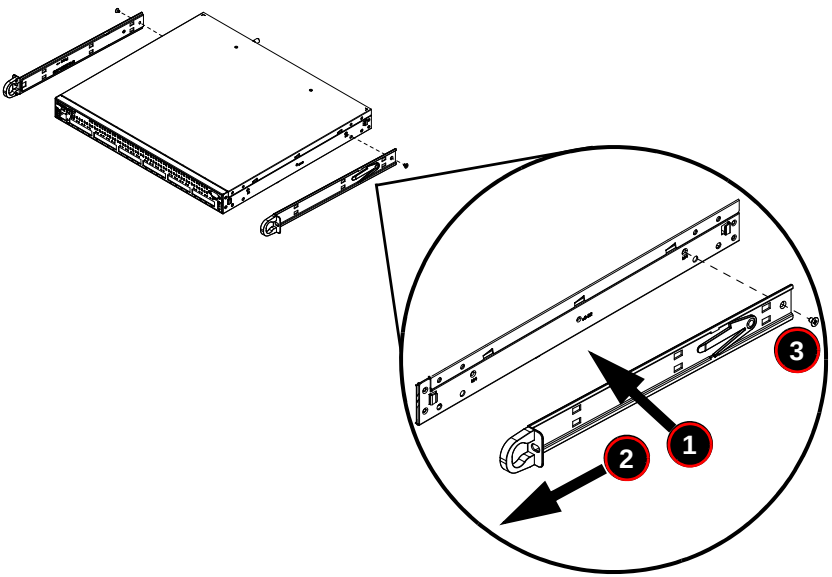
Installing the Inner Rails

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

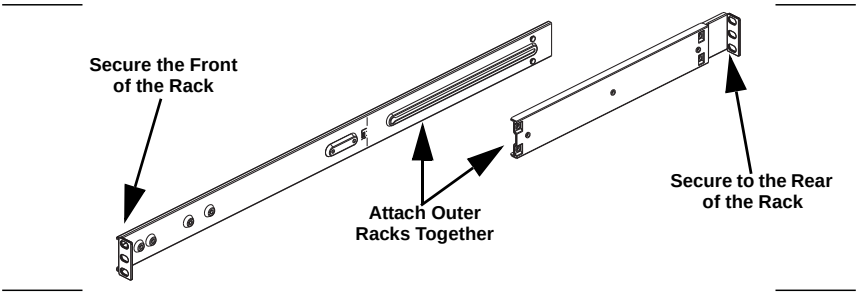
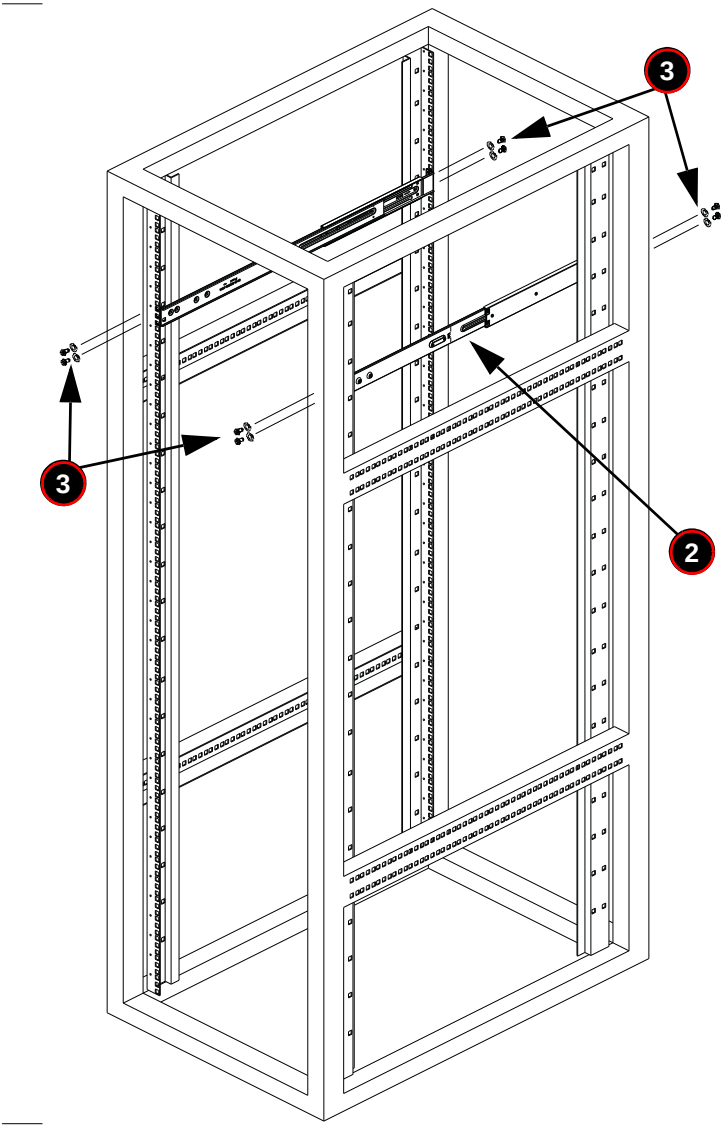


Figure A-4. Installing the Outer Rails onto the Rack



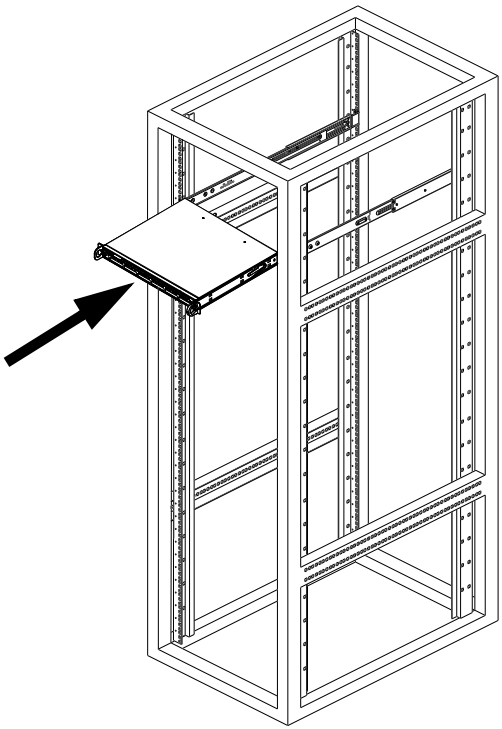
Installing the Switch into a Rack

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.

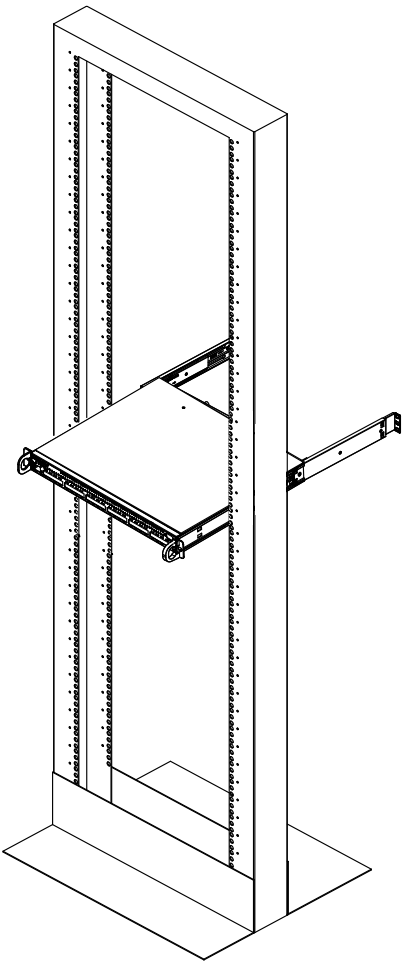
Figure A-5. Installing the Switch into a Rack



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



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.