Web GUI Guide for MBM-GEM-004

Release 1.0

Super Micro Intelligent Switch
Release: **1.0**
Document status: Standard
Document release date: 12/9/2016

Contents

1 Introduction

1.1 Purpose

This document is designed to provide Supermicro Switch module MBM-GEM-004 users with the information required to configure the switch through the Web interface. The web pages have been presented as screenshots in this document to make the information more accessible.

1.2 Scope

This document explains in detail about all web pages and fields that are useful to configure the MBM-GEM-004 switch product.

1.3 Definitions and Acronyms

ACL	Access Control Lists
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common Internal Spanning Tree
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DLF	Destination Lookup Failure
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
IGMP	Internet Group Management Protocol
IGS	IGMP Snooping
IP	Internet Protocol
LA	Link Aggregation
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
PDU	Protocol Data Unit
QoS	Quality of Service
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLV	Type Length Value
TOS	Type Of Service
UDP	User Datagram Protocol
VLAN	Virtual LAN

2 Overview

MBM-GEM-004 can be configured through Web browsers like the Chrome, Firefox, Safari or Internet Explorer. For managing the switch through web browsers, type in the management IP address to start accessing the switch in browser address bar. For example, if the management IP address of the switch is 192.168.100.102, the switch can be accessed through the Web browser by typing **http://192.168.100.102** in the address bar of the web browser.

2.1 Management IP Address

MBM-GEM-004 comes with default DHCP settings for management IP address.

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

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

2.2 Login Page

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

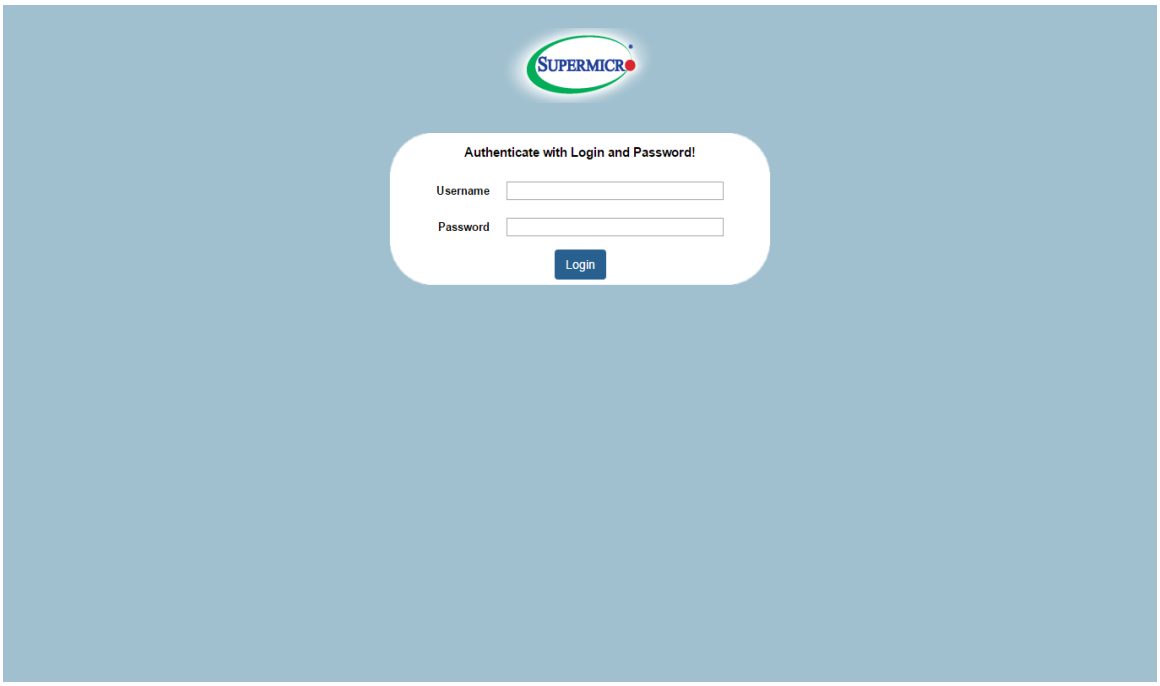


Fig: login page

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

2.3 Home page

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

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

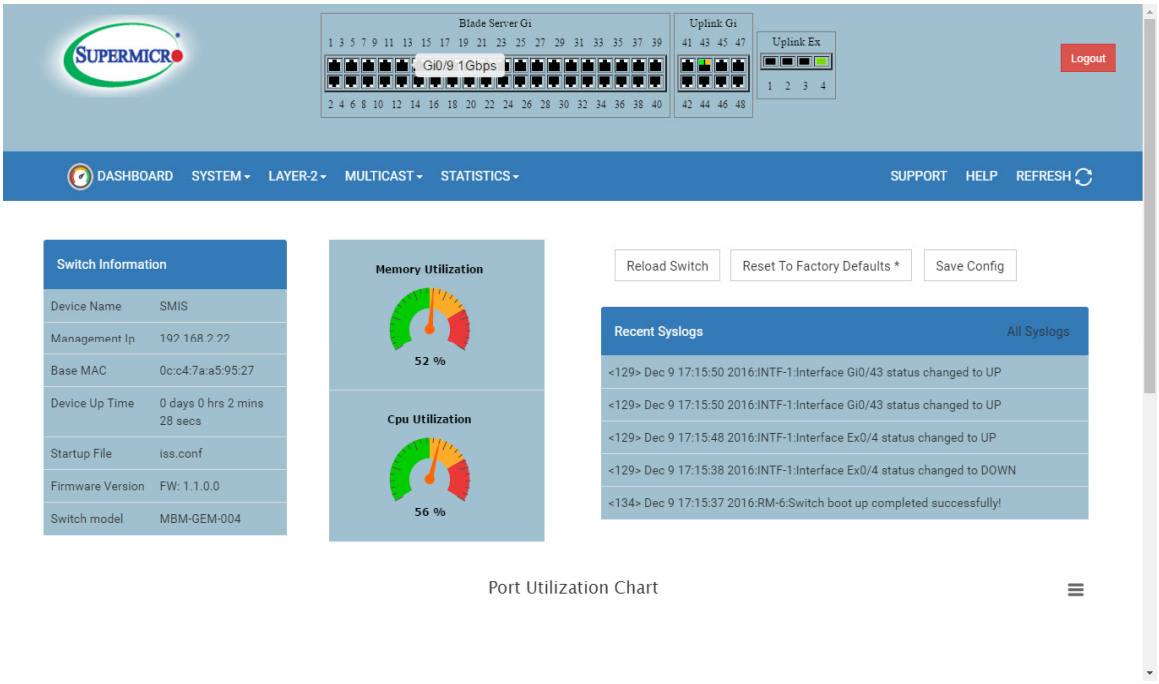


Fig: Homepage

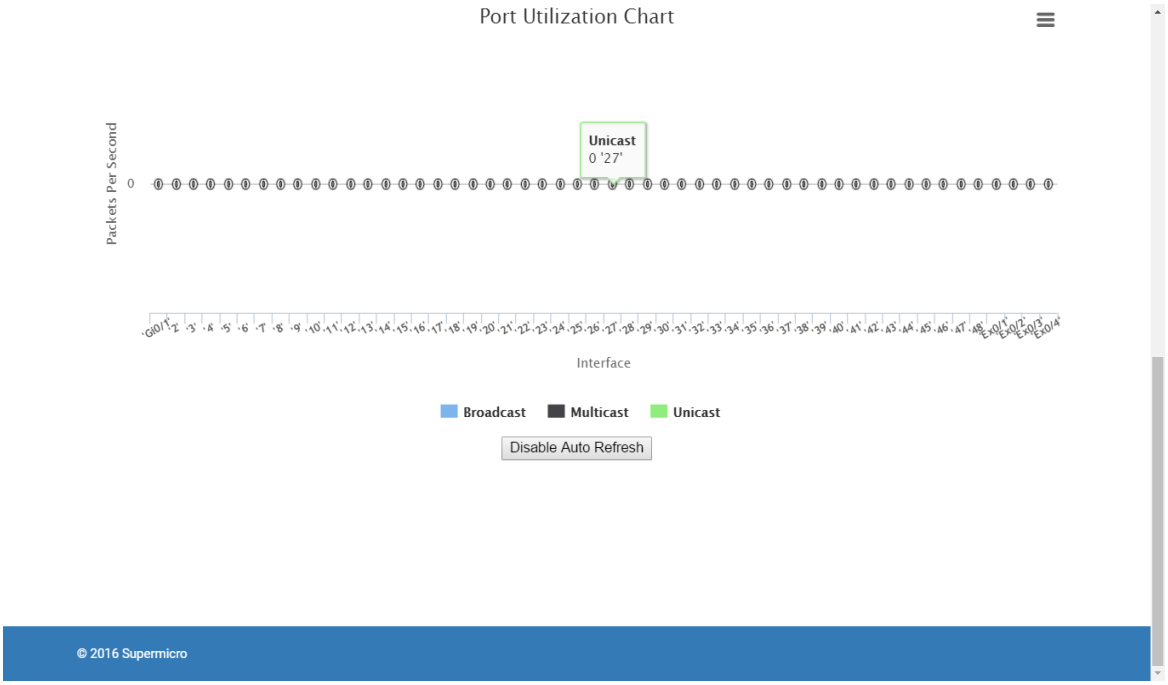


Fig: Homepage Port Utilization

2.3.1 Dashboard

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

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

Device name - Displays the Switch name.

Management IP - Management IP Address of the Switch.

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

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

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

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

Switch model - Displays the model of the Switch.

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

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

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

Following buttons are used for quick configuration:

Reload Switch - Use this button to reload the switch.

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

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

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

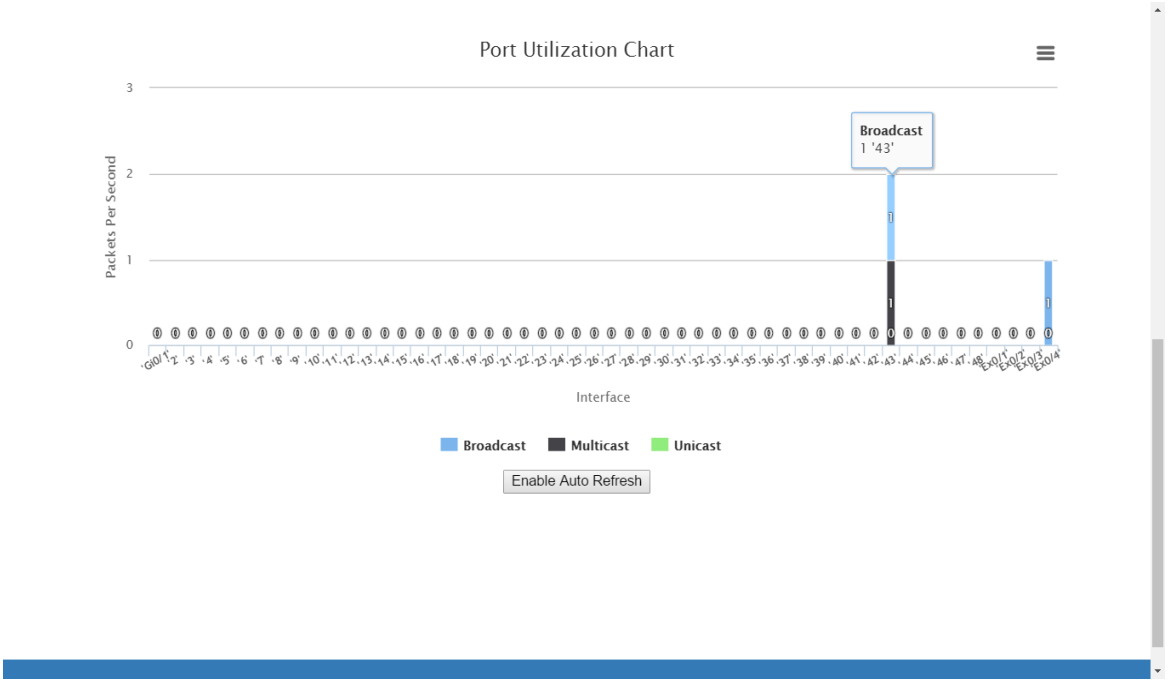


Fig : Port Utilization Chart

2.3.2 Page Top Links

This section provides the following links.

Refresh

Help

Support

Logout

Refresh link helps refreshing contents of the page. Unlike browser provided refresh button and refresh icon, these are refreshes only the contents of middle page which has active data.
Help link provides context specific help texts. This link opens a new help text page relevant to the configurations of current configuration page displayed.
Support link provides link to customer support help of Supermicro.
Logout link helps signing out of management web application. This link takes the user back to login screen requesting user name and password for login.

2.3.3 Top LED Display

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

2.3.4 Menu

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

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

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

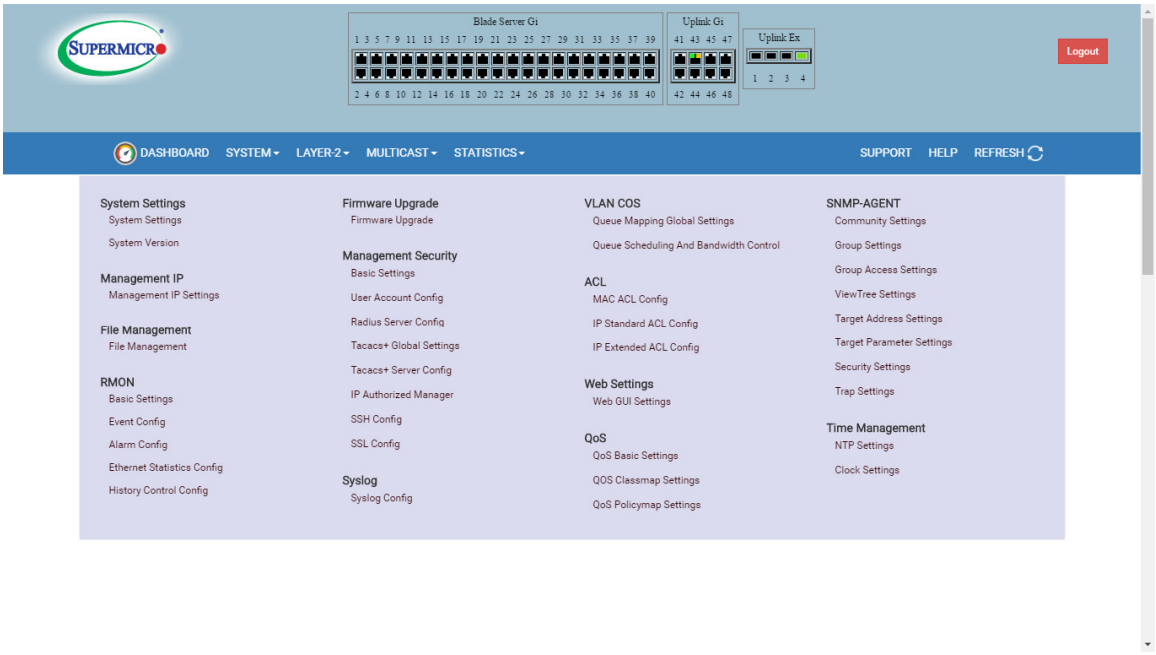


Fig: Menu List

3 System Management

System Management covers the following features of Switch.

- System Settings
- Management IP
- File Management
- RMON
- Firmware Upgrade
- Management Security
- Syslog
- ACL
- Web Settings
- QoS
- SNMP AGENT
- Time Management

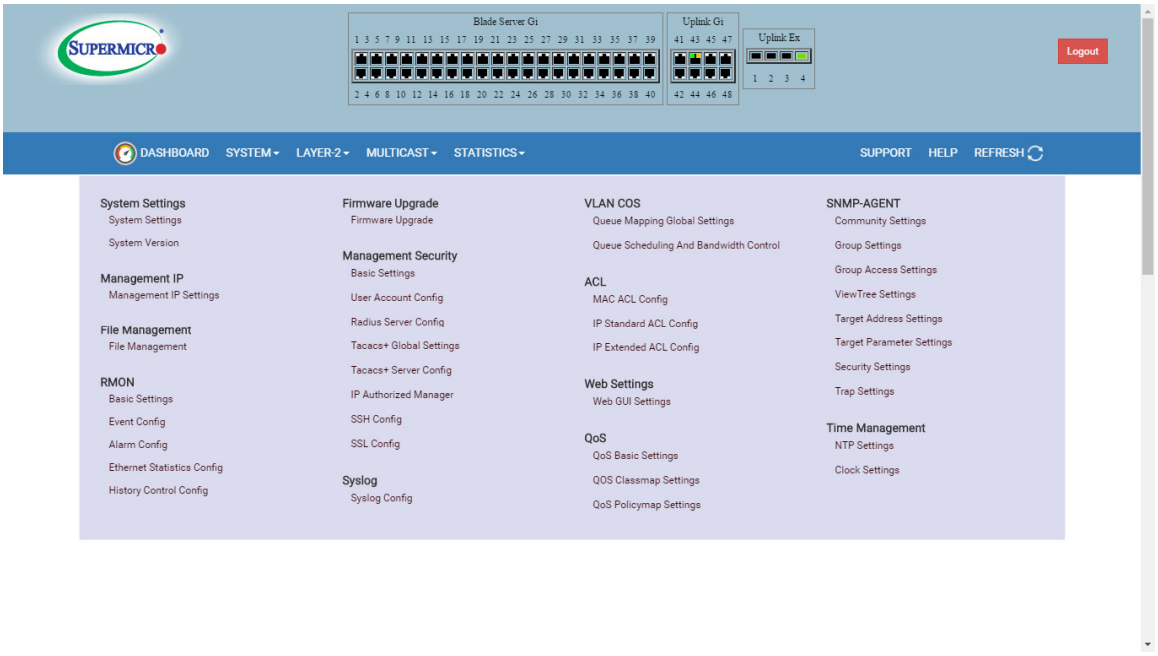


Fig: System Management

3.1 System Settings

System Settings covers basic System Settings and System Version information.

3.1.1 System Settings Page

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

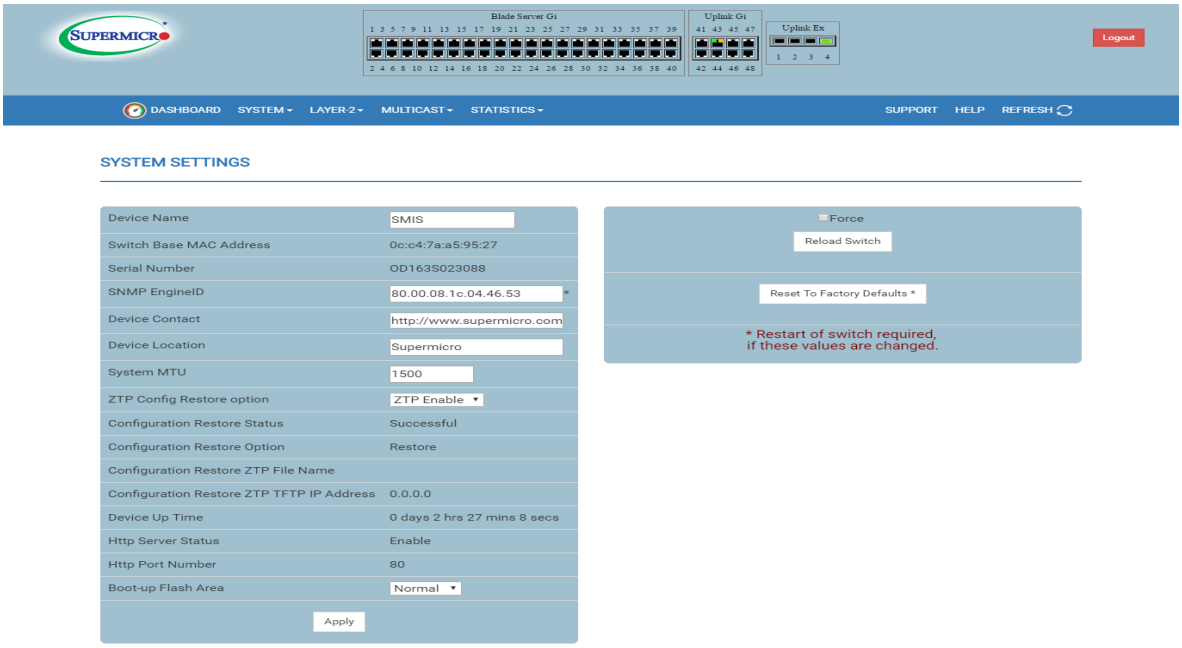


Fig: Basic System Settings

User can configure the below listed parameters in System Settings.

Device name - configure the device name

SNMP Engine ID - SNMP Engine Identifier

Device contact - change device contact

Device Location - change device location

System MTU - Configure MTU value. The allowed value ranges between 1500 to 9216. The default value is 1500.

ZTP Config Restore Option - User can configure ZTP Enable or Disable option.

Boot-up Flash Area - User can specify whether the switch boots up from Normal firmware image or Fallback firmware image. The default is boot up from Normal firmware image.
User can view the below listed parameters.
Switch Base MAC address
Serial Number
Configuration Restore Option
Configuration Restore Status
Configuration Restore ZTP File Name
Configuration Restore ZTP TFTP IP Address
Device Up Time
HTTP Server Status
HTTP Port Number
This page also has control to “Reset To Factory Defaults”. This will clear all Switch configurations and local user accounts information. Make sure to have all necessary configurations backed up before doing “Reset To Factory Defaults.”. This reset requires reboot of the switch.

This page also provides control to reboot the switch.

3.1.2 System Version Page

System Version page displays hardware,firmware, OS and bootloader version of the Switch.

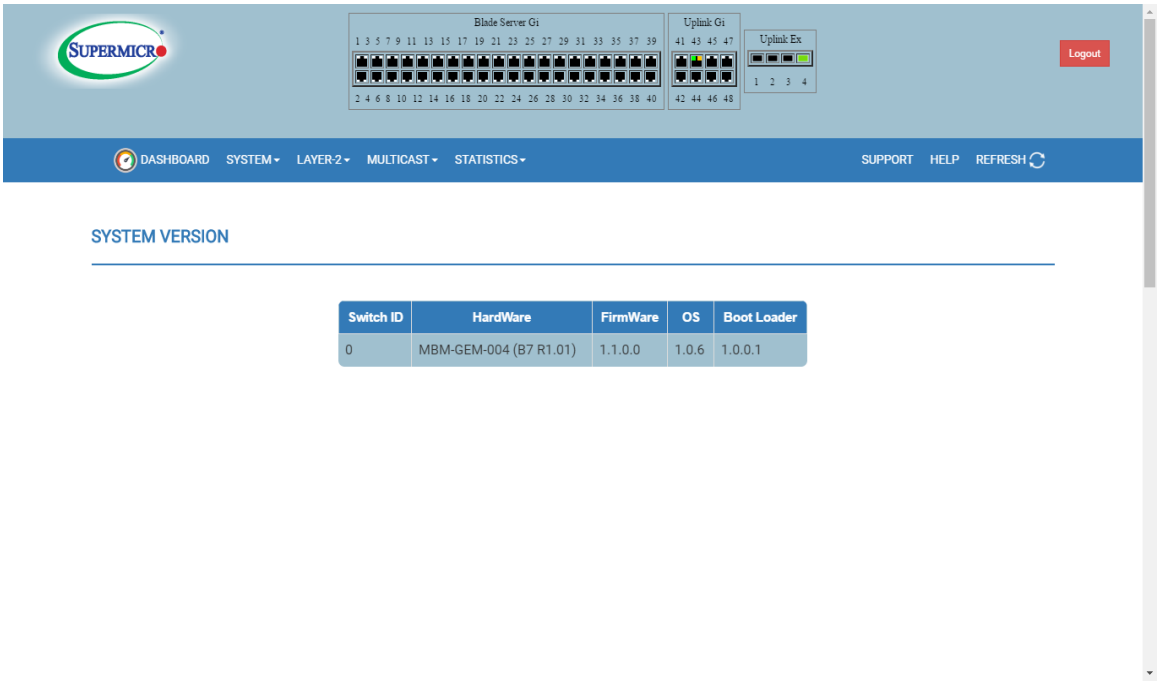


Fig: System Version Page

3.2 Management IP

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

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

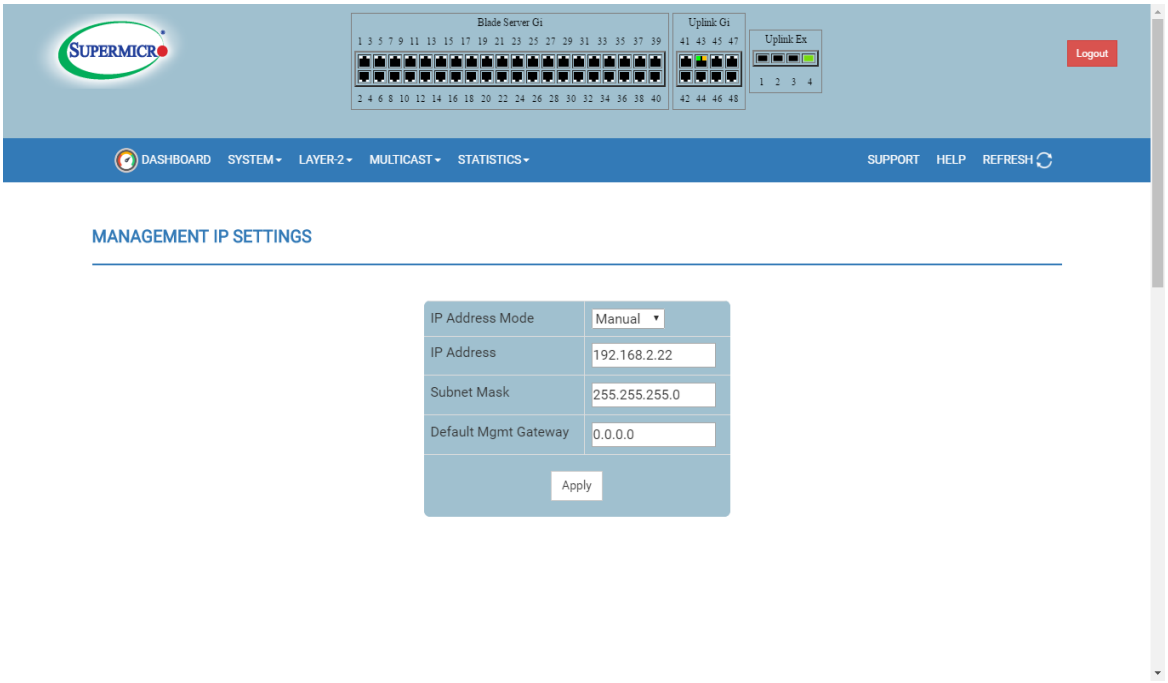


Fig: Management IP settings

User can configure the below listed parameters in Management IP Settings.

IP address mode - This can be either manual or dynamic. If manual mode is selected, then the management interface takes the configured IP address as Default IP Address. If dynamic mode is selected, the management interface gets the IP address through DHCP.
IP address - Configures the management IP address. This is configurable only if IP Address Mode is manual
Subnet Mask - Configures the management IP subnet mask. This is configurable only if IP Address Mode is manual
Default Mgmt Gateway - Configures the default gateway IP address in blade switches.

3.3 File Management

File Management page helps user to manage the configuration files in Switch.

This page provides the below three main features.

- Save Configuration
- File Upload
- File Lists

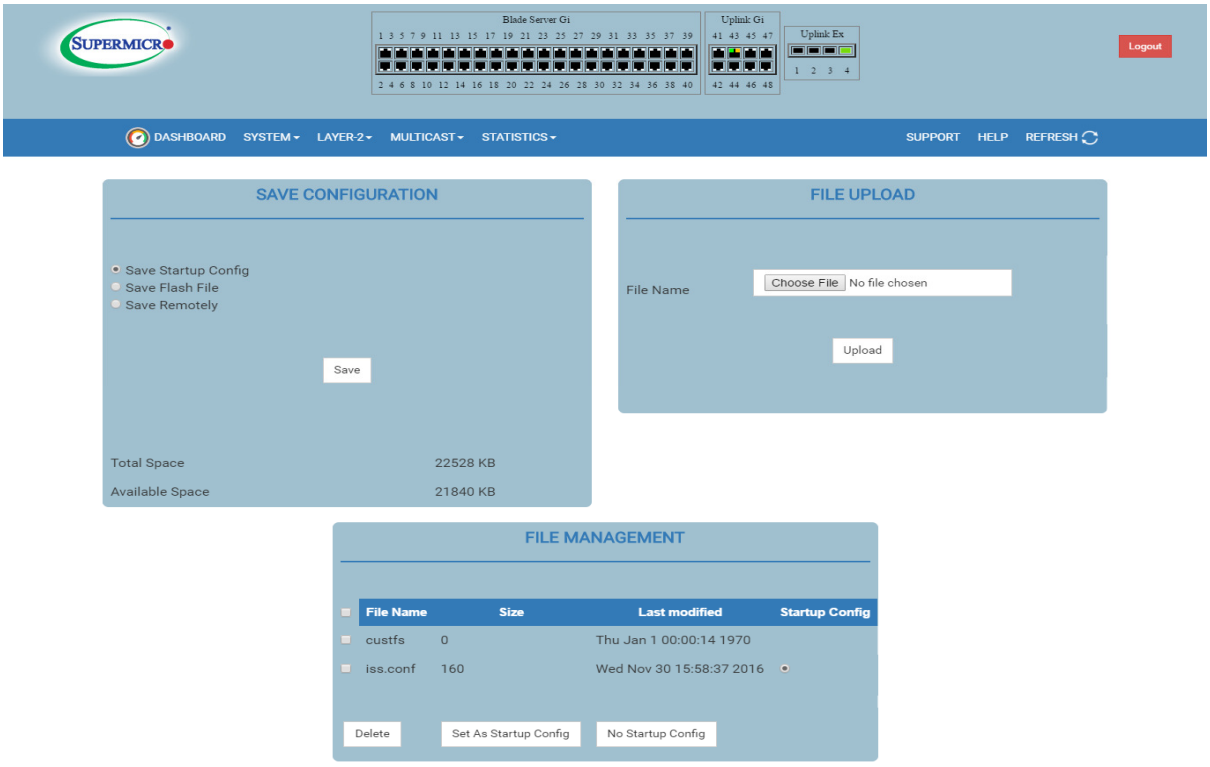


Fig: File Management

Save Configuration

User can save currently running switch configuration in following three ways.

Save Startup Config – This option saves the current running configuration in local flash with the file name configured as “startup configuration” file.

Save Flash File – This option saves the current running configuration in a local flash with user specified file name.
Save Remotely – This option saves the current running configuration in remote TFTP server. User needs to provide IP address and file name of TFTP server.

The total configuration memory space and available free space are displayed.

File Upload

File upload can be used to uploading any configuration file to switch. This file will be saved in a switch. TFTP or FTP is not required for file upload from this page.

File List

This section displays the information about configuration files stored in switch. User can select one or more files and delete them.
User can also choose “Startup Configuration” file from this file list.
User can also choose “No Restore” option for not to load any configuration on next reboot of the switch.
Files can be downloaded from the list. Onclick download option is not available. User can download file from switch to any other location by right click option. Hence TFTP or FTP is not required for file download from this page.

3.4 RMON Basic Settings

RMON Basic Settings page helps enabling disabling RMON feature.

RMON Status - Enable or disable RMON feature.

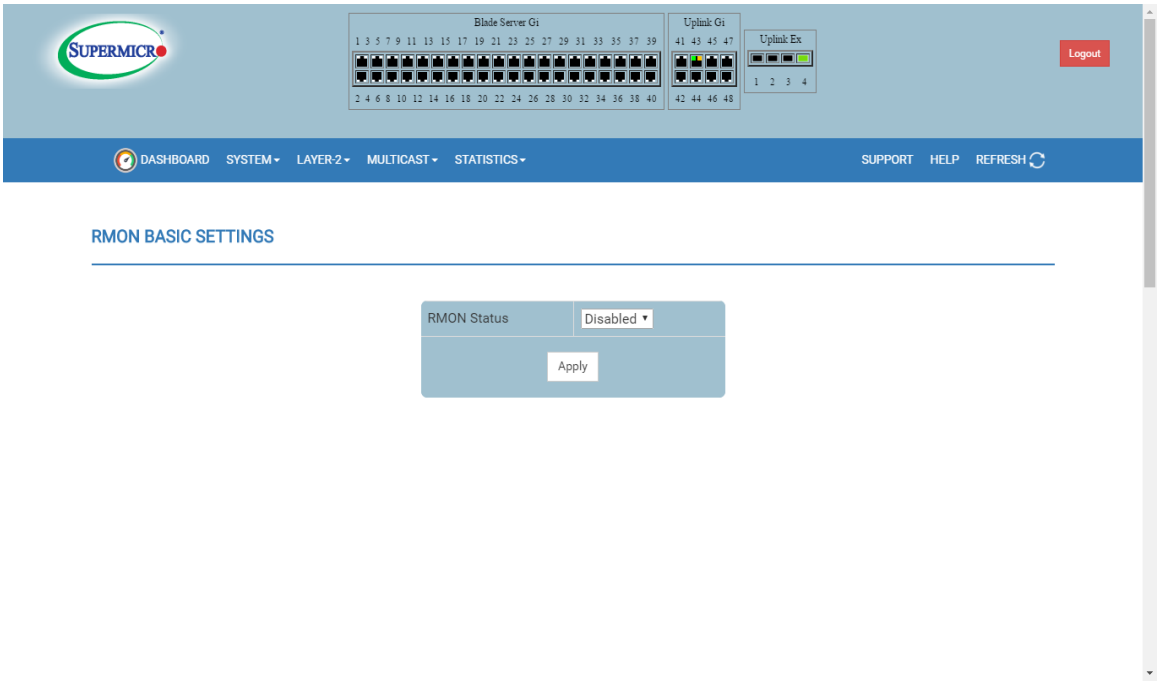


Fig: RMON Basic Settings

3.4.1 RMON Event Configuration

Event Configuration page helps configuring RMON events.

Index - Specifies the index to the Events table. This value must be in the range from 1 to 65535.

Description - Specifies a brief description of the event.

Type - Specifies the event configured can be a Log, or an SNMP trap, or both, or none. For event type TRAP and Log and TRAP community must be configured.

Community - Specifies the SNMP community string used for this trap. This is relevant when an SNMP trap is requested for an event. For event type TRAP and Log and TRAP community must be configured. Also make sure the configured community is active before adding event on that community.

Owner - Indicates the owner of this event.

Last Time Sent - Denotes the time this event entry last generated an event.

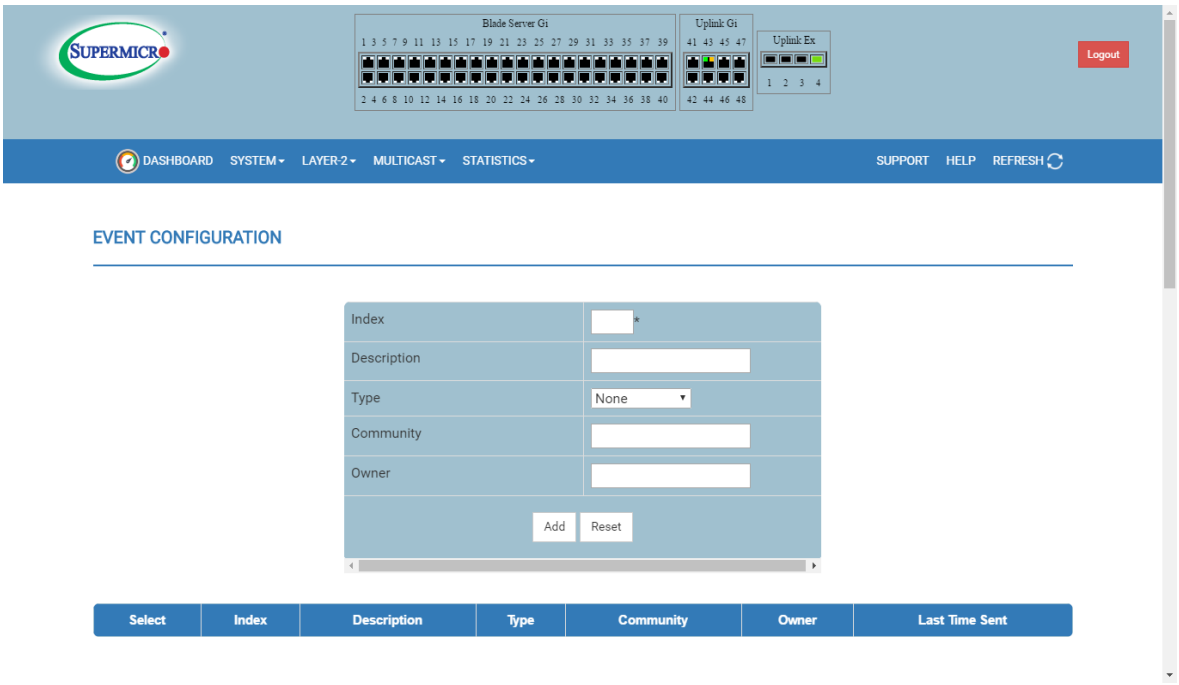


Fig: Event Configuration

3.4.2 RMON Alarm Configuration

RMON Alarm Configuration page helps configuring RMON Alarm parameters.

Index - Specifies the table index. This value must be in the range from 1 to 65535.

Interval - Specifies the time interval for which the alarm monitors the variable. This value must be in the range from 1 and 4294967296.

Variable - Specifies the MIB object on which the alarm is set.

Sample type - User can set this to an absolute value or as just incremental values of the timer.

Rising Threshold - If the startup alarm is set as rising alarm and this threshold is reached, an alarm is raised. This value ranges between 0 and 2147483647.

Falling Threshold - If the startup alarm is set as Falling alarm and this threshold is reached, an alarm is raised. This value ranges between 0 and 2147483647. The falling threshold must be less than the rising threshold.

Rising Event Index - Indicates the index of the event to be raised when the Rising threshold is reached. This value must be in the range from 0 to 65535.

Falling Event Index - Indicates the index of the event to be raised when the Falling threshold is reached. This value must be in the range from 1 to 65535.

Owner - Specifies the owner of the alarm.

Fig: RMON Alarm Settings

3.4.3 Ethernet statistics Configuration

Ethernet Statistics monitoring page helps configuring RMON Ethernet statistics parameters.

Index - Specifies the index to the table. This value must be in the range from 1 to 65535.

Port - Specifies the Ethernet Port.

Owner - Specifies the owner string.

Bytes – Displays the total number of bytes received from the network.

Packets - Displays the total number of packets received from the network.

Broadcast Packets - Displays the total number of broadcast packets received from the network.

Multicast Packets - Displays the total number of multicast packets received from the network.

Undersized Packets – Displays the number of undersized packets received from the network.

Oversized Packets – Displays the number of oversized packets received from the network.

Fragments - Displays the number of fragments received from the network.

Jabbers – Displays the number of jabbers in the network.

CRC – Displays the number of packets received with CRC errors from the network.

Collisions – Displays the number of Collisions in the network.

64 Octets - Displays the number of Ethernet packets received with size 64 octets or less.

65-127 Octets - Displays the number of Ethernet packets received with size between 65 to 127 octets.

128-255 Octets - Displays the number of Ethernet packets received with size between 128 to 255 octets.

256-511 Octets - Displays the number of Ethernet packets received with size between 256 to 511 octets.

512-1023 Octets - Displays the number of Ethernet packets received with size between 512 to 1023 octets.

1024-1518 Octets - Displays the number of Ethernet packets received with size between 1024 to 1518 octets.

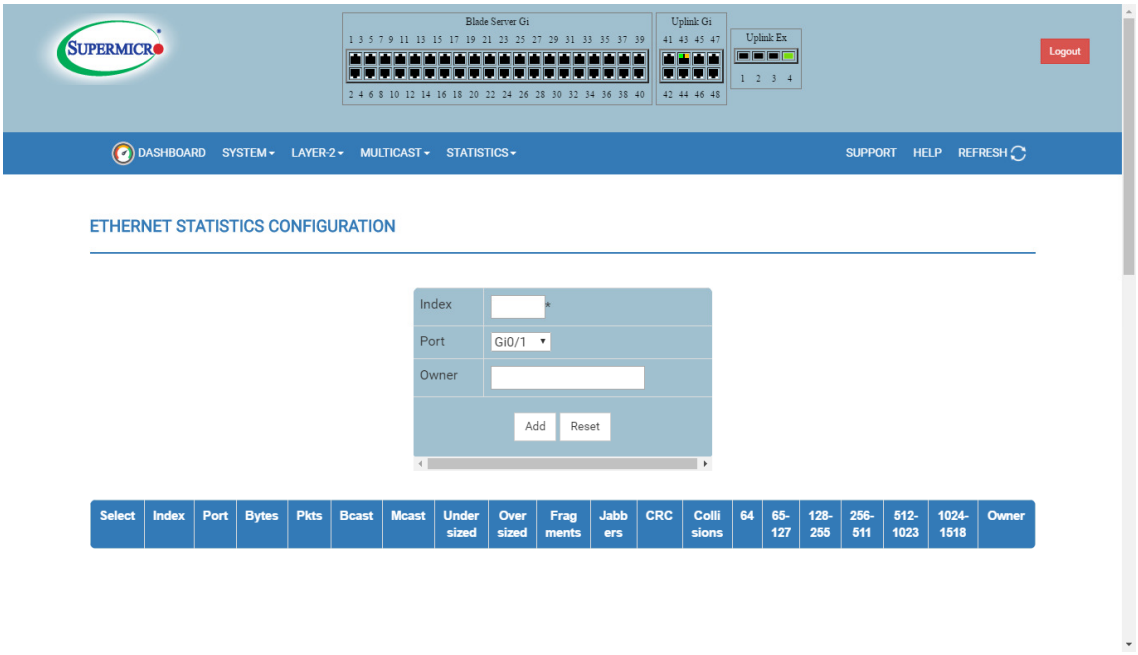


Fig: Ethernet statistics configuration

3.4.4 History Control Configuration

History Control Configuration page helps configuring RMON history configuration parameters

Index - Specifies the index to the table. This value must be in the range from 1 to 65535.

Port – Specifies the port number.

Buckets Requested - Indicates the number of buckets to be configured for collecting the RMON statistics. This value must be in the range from 1 to 65535.

Interval - Specifies the time interval between two successive polling to collect the statistics. This value must be in the range from 1 to 3600.

Owner - Denotes the owner of the RMON group of statistics.

Buckets Granted - Denotes the number of bucket granted for collecting the RMON statistics.

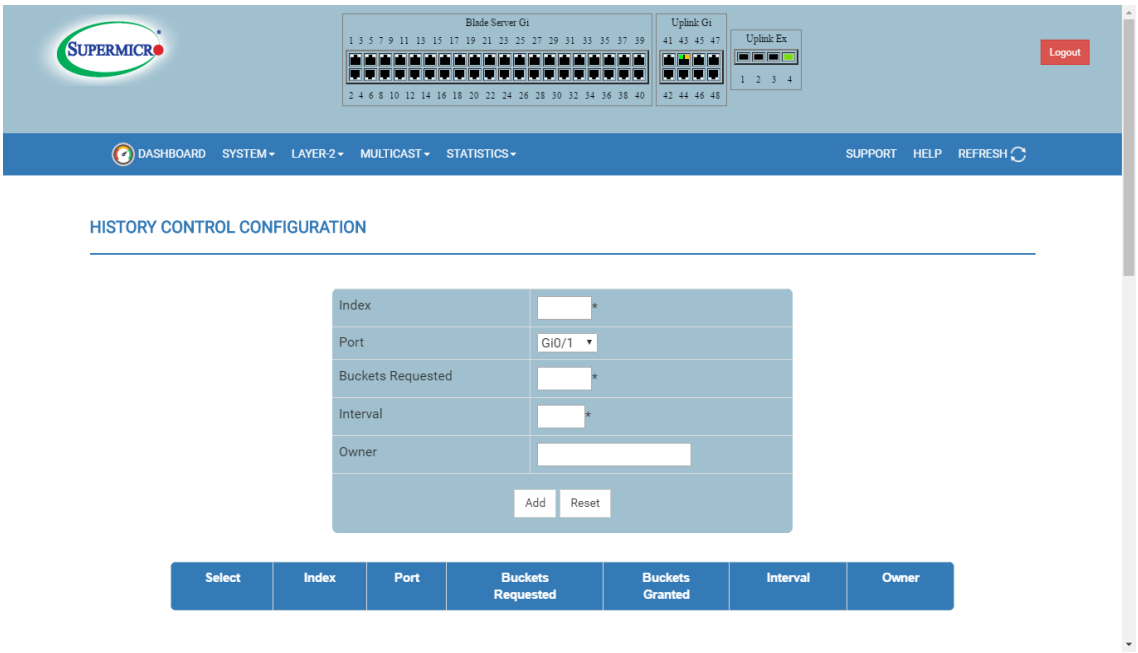


Fig: History control Configuration

3.5 Firmware Upgrade

This Page allows the user to upgrade the firmware in normal or fallback memory.

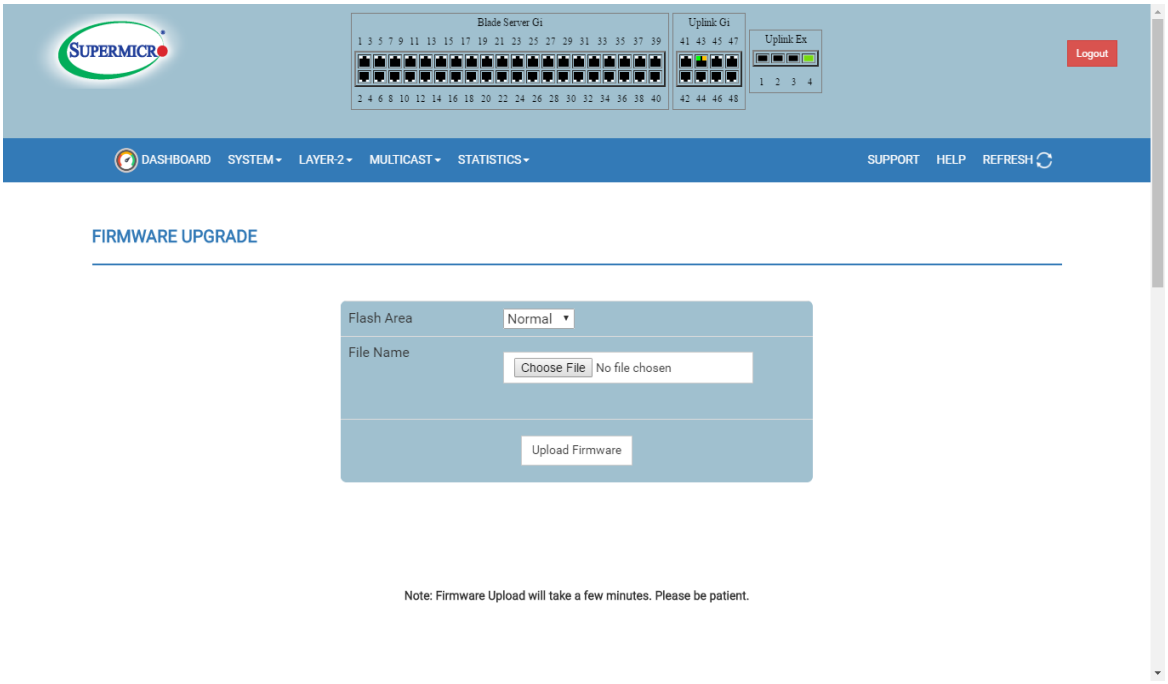


Fig: Firmware upgrade

3.6 Management security

Management Security link provides configuration for the below list of features.

- Management Security
- User Accounts
- Radius
- TACACS+
- TACACS+ Servers
- IP Authorization Managers
- SSH
- SSL

3.6.1 Management Security Basic Settings

This page helps below listed basic security configurations.

Login Authentication mode – User can choose the mode of authentication for management access. By default the management access are authenticated with “Local” user accounts information. User can choose to authenticate using “Radius” or “TACACS”.

Tacacs Authentication Mode – User can configure TACACS specific authentication mode PAP or CHAP, when login authentication mode is TACACS.

Authentication traps – User can enable 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 “Web Settings” page to enable access to privilege configurations.

Administrative users can set “Enable” password for all privilege levels. By default “Enable” password is set only for highest level “Level_15”. This default password is same as the default password set for ADMIN user login.

Authorization Status – User can enable or disable the authorization status, when login authentication mode is TACACS.

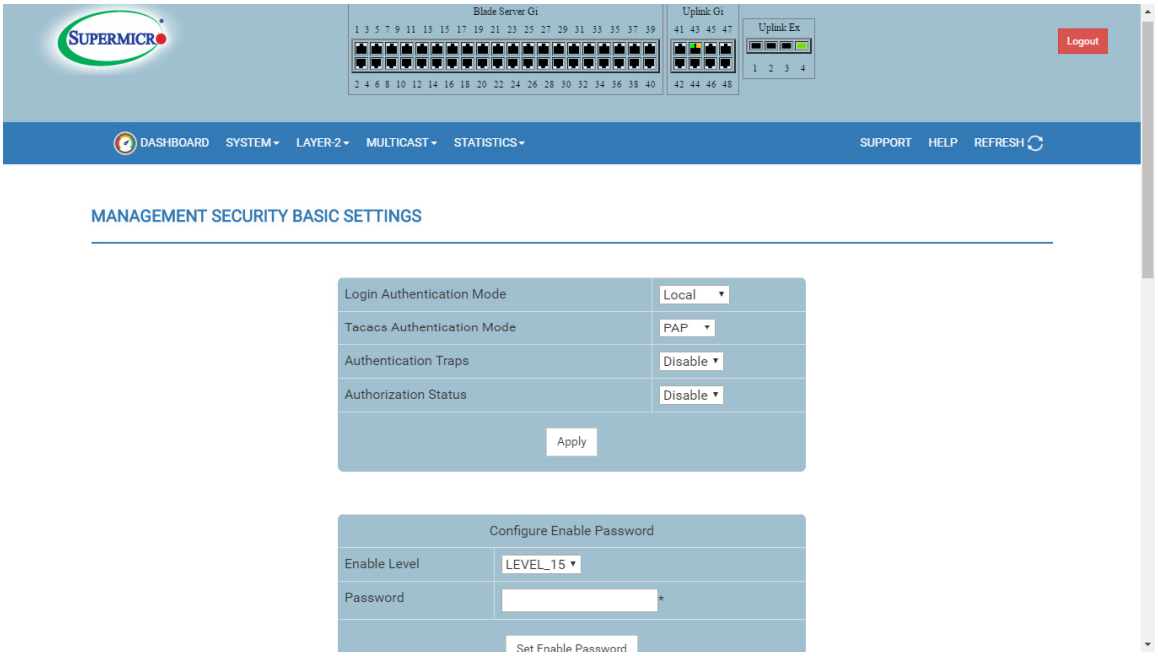


Fig: Management Security Basic Settings

3.6.2 Management User Account

This page helps creating or deleting local user accounts. Users 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 administrator privilege. Any one of the configured users can be specified as ADMIN user.

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

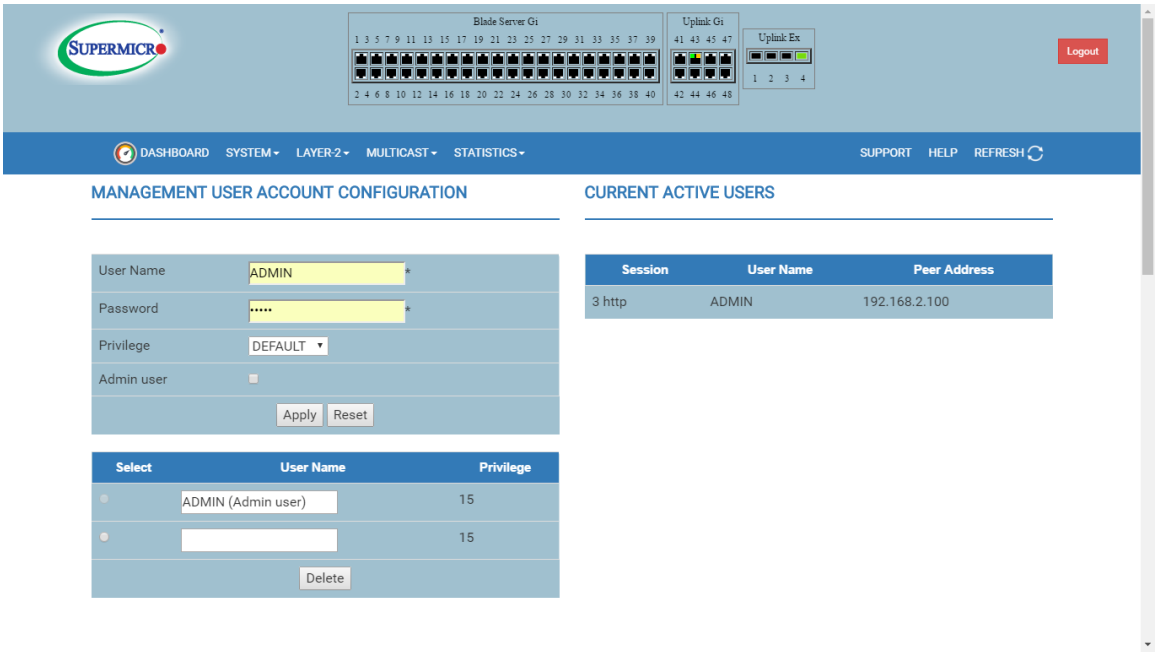


Fig: Management user Account

3.6.3 Radius

Radius Server Configuration page allows to configure the RADIUS server details.

Server ID - Specifies the unique identifier of the Radius Server Entry. The allowed value ranges between 1 to 10.

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

Shared Secret - Specifies the secret string, which is to be shared between the Radius Server and the Radius Client.

Server Type - Specifies the following RADIUS server type

- Authentication
- Accounting
- Both (Authentication and Accounting).

Response Time (secs) - Specifies the maximum time within which the Radius Server has to respond for a request from the Radius Client. The allowed value ranges between 1 to 120.

Retry Count - Specifies the maximum number of times a radius request is to be re-transmitted before getting response from the Radius Server. The allowed value ranges between 1 to 254.

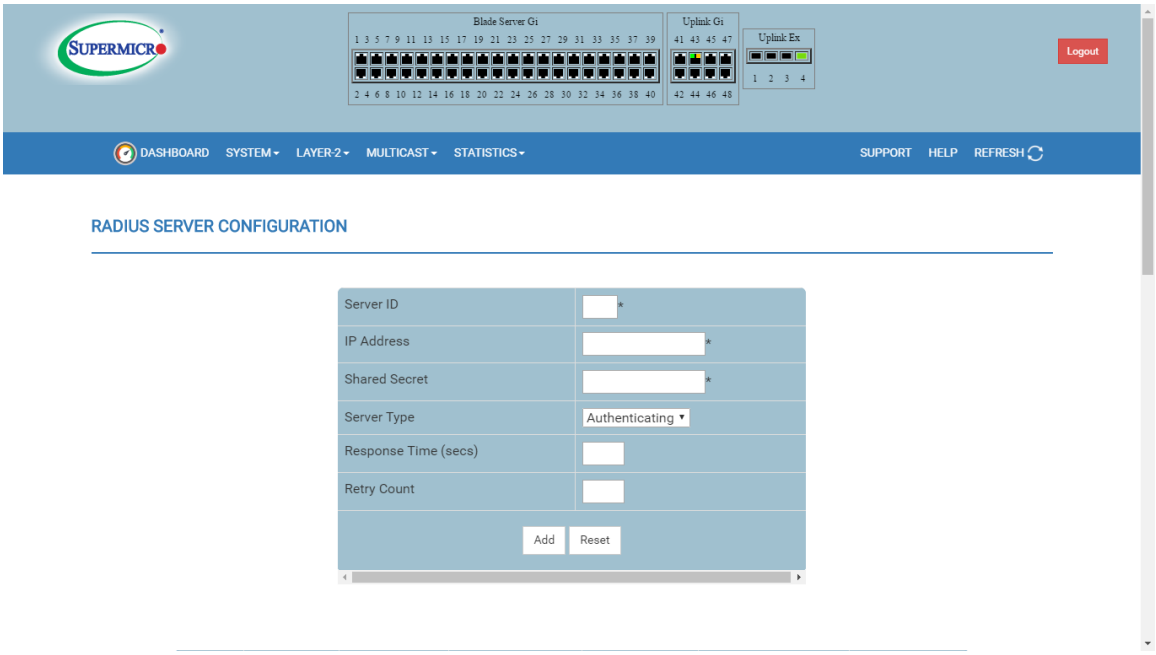


Fig: Radius

3.6.4 TACACS+ Global Settings

TACACS+ Global Settings page helps configuring TACACS retries and choosing active TACACS server.

Active Server IP Address - Specifies the IP address of the active TACACS server. This server should have been already configured in TACACS+ Server Configuration page.

Retries - The number of times the switch searches the active TACACS server from the list of servers maintained. The allowed values are between 1 to 100. The default value is 2.

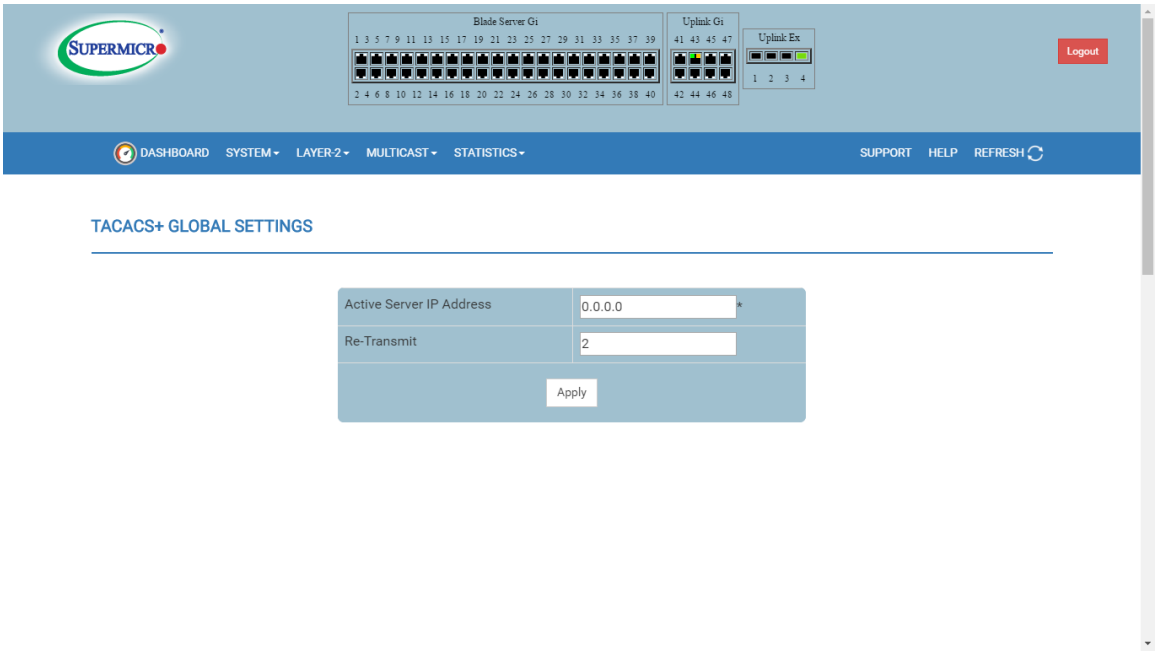


Fig: TACACS+

3.6.5 TACACS+ Server Configuration

TACACS+ Server Configuration page helps configuring TACACS servers.

IP Address - Specifies the IP address of the TACACS server."

Port - TCP port for TACACS protocol.

Single Connection - Yes or No for single TCP connection. If Yes, it establishes only single TCP connection with given TACACS server.

Timeout - The time for which switch will wait for response from TACACS server before closing the connection. It is configurable in seconds. The allowed value ranges between 4 to 15 seconds. The default is 5 seconds.

Key Type – Specifies the Key Type for the TACACS server. The allowed key type is 0 or 7. The default key type is 0. The key 0 type key is plain text. For key 7 type, user has to provide the encrypted key string.

Secret Key - Encryption key for the given TACACS server.

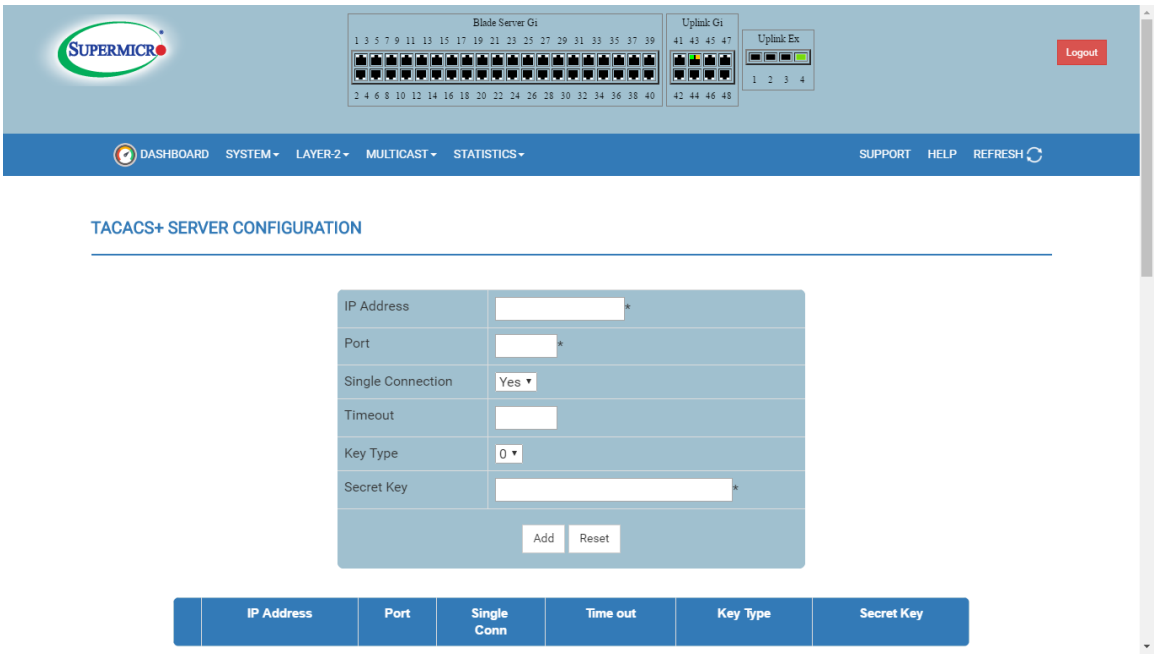


Fig: TACACS+ Server Configuration

3.6.6 IP Authorized Manager

IP authorized manager page helps configuring allowed management nodes for managing switch.

IP Address - Specifies the IP address of the manager. An address 0.0.0.0 indicates 'Any Manager'.

Subnet Mask - Subnetwork mask for the specified IP address.

Services Allowed - Indicates service type. Can be one or more of the following: telnet, ssh, http, https or snmp.

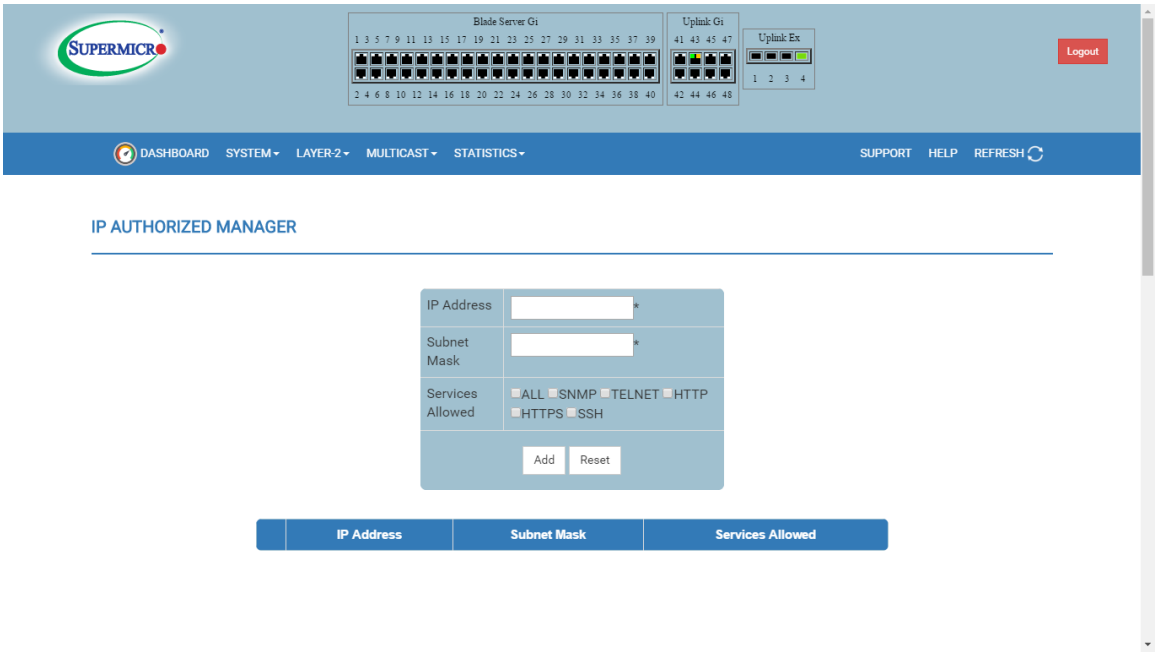


Fig: IP authorized Manager

3.6.7 SSH

SSH Configuration page helps configuring SSH version and keys.

SSH Version - Default version 2. User can choose to configure as compatible with version 1.

Cipher - Default is 3DES-CBC. User can choose to configure as 3DES-CBC or DES-CBC or both.

Authentication - Default is HMAC-SHA1. User can choose to configure as HMAC-SHA1 or HMAC-MD5 or both.

SSH Port - Default is 22. User can choose to configure any value between 1024 - 65535 or the default value 22.

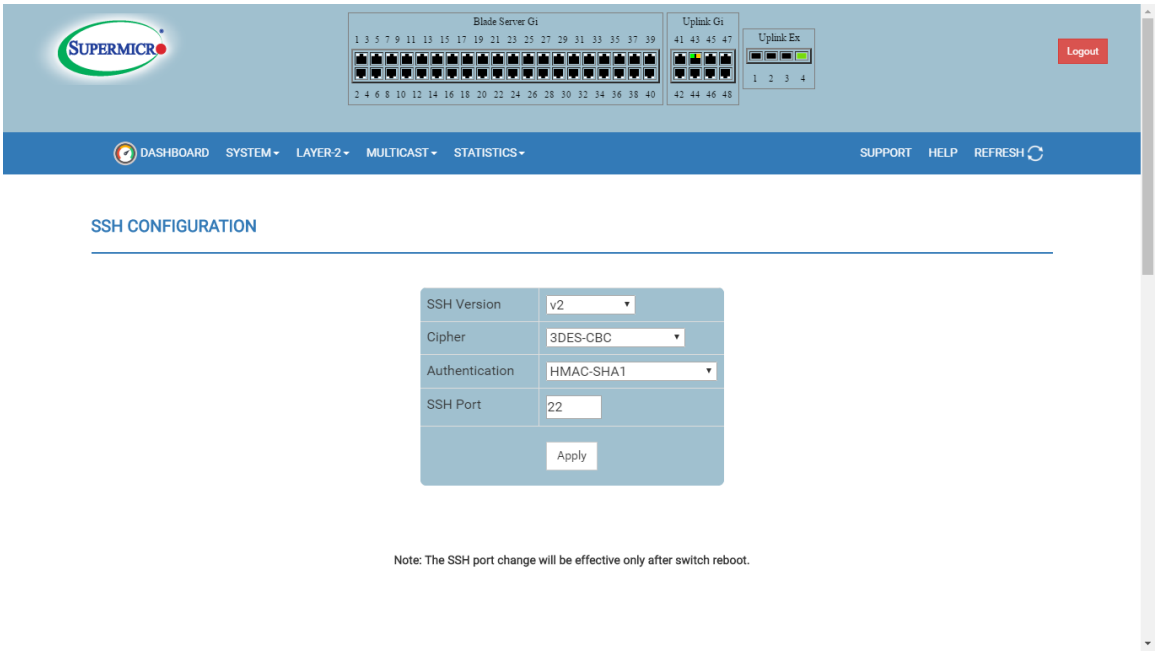


Fig: SSH Configuration

3.6.8 SSL

SSL Configuration page helps configuring SSL parameters and generate SSL certificates for HTTPS.

To configure SSL and enable HTTPS following the below steps.

1. Configure Cipher Suite and Crypto Key RSA of your choice.

2. Create certificate request. Enter the subject name and click on CREATE button. When the page reloads, the text box below the CREATE button will display certificate request. Copy paste these contents to a text file say a.csr.

3. To generate SSL certificate openssl application can be used. The following steps 4 and 5 can be executed in any linux machine to generate SSL certificates. For other openssl implementation refer the openssl documentation to find the equivalent steps for 4 and 5.

4. Execute the below command in inux shell.
openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem

5. Execute the below command also in linux shell.
openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CA key cakey.pem -CAcreateserial

6. The above steps 4 and 5 would generate certificate file cert.pem.

7. Open the generate certificate file cert.pem.
Delete first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--).
Join all the remaining lines as single line to avoid line breaks processed.
Copy paste these joined texts in Enter Certificate text box.
Click CONFIGURE button.

8. The above step 7 would configure the certificate and save it to flash.

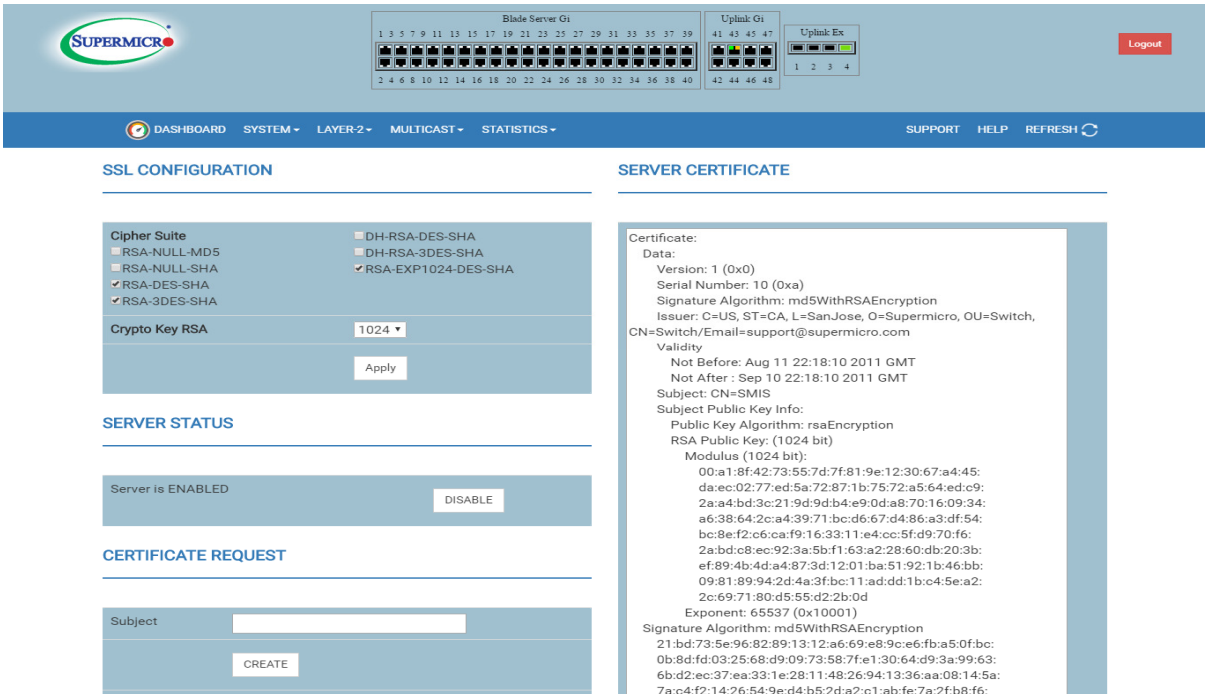


Fig: SSL Configuration

3.7 Syslog configuration

Syslog Configuration page helps configuring logging parameters

Syslog - Enable or disable syslog feature.

Server IP Address - Syslog server IP address. Make sure Server IP is reachable.

Buffer Size - Buffer size is specified in log entries. Max entries buffered is 200.

Timestamp - Enable or disable adding timestamp to log messages.

Console Log - Enable or disable logging to console.

Mac Address Log – Enable or disable logging of MAC address table update in syslog. By default Mac address logging is disabled.

Facility - This allows selecting supported facilities. Switch supports syslog standard supported facilities local0, local1, local2, local3, local4, local5, local6, local7 and user.

Trap - This helps selecting particular trap type. The following types of traps are supported Alerts, Critical, Debugging, Emergencies, Error, Informational, Notification and Warnings.

File Name – Configuring file name enables file logging. To disable file logging, remove the file name from this field.

File Max Size –Specifies the maximum size of the file entries. The default size is 4096.

File Min Size – Specifies the minimum size of the file entries. The default size is 2048.

Buffer Entries – Displays currently available number of log entries in syslog buffers.

File Entries – Displays currently available number of log entries in syslog files.

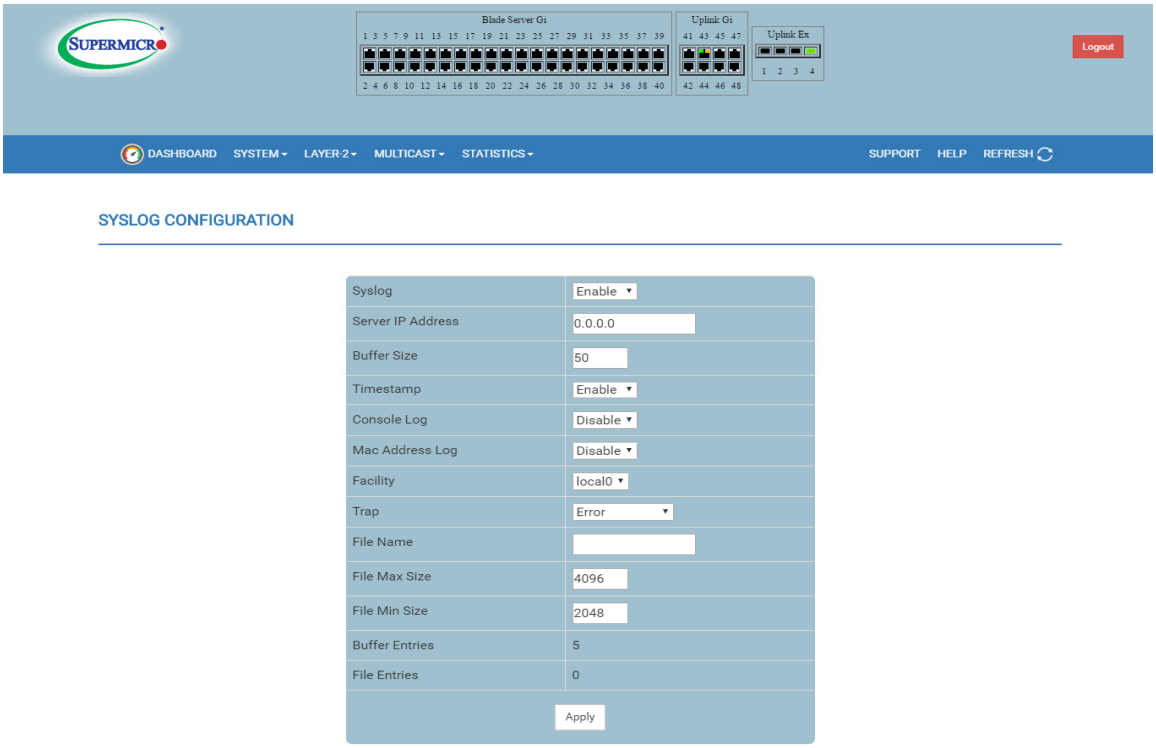


Fig: Syslog Configuration

3.8 ACL

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

- MAC ACL
- IP Standard ACL
- IP Extended ACL

3.8.1 MAC Based ACL

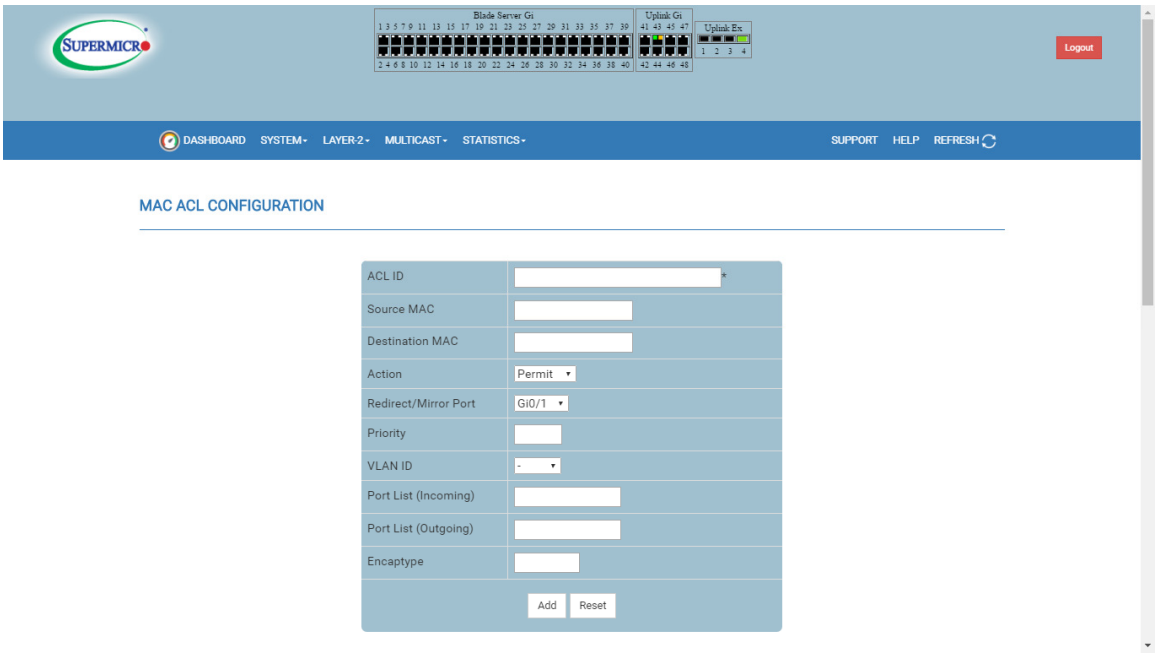


Fig: MAC ACL

The *MAC ACL* link opens the **MAC ACL Configuration** Page. This page displays the various parameters to configure the MAC Access List. This table includes the following parameters for configuration.

ACL ID – Specifies the unique Id for the access list. This value must be in the range from 1 to 32768.

Source and Destination MAC – Specifies 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

Action – Specifies the action to be taken for the access list.***Redirect Port*** - Configure the port to which packets matching this ACL need to be redirected.

Redirect/Mirror **Port** - Specifies redirect/mirror port to be used.

Priority – Specifies the priority for the access list. This value must be in the range from 1 to 255. The default priority value is 1.

VLAN ID – Specifies the VLAN ID for which the access list has to be applied.

Port List (Incoming) – Specifies the incoming Port List for which the access list has to be applied.

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

Encaptype – Specifies the Encapsulation type of the packet for which the access list has to be applied. This value must be in the range from 1 to 65535.

3.8.2 IP Standard ACL

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

This page displays the various parameters to configure the Standard IP access lists.

ACL ID – Specifies the unique ID for the access list. This value must be in the range from 1 to 32768.

Action – Specifies whether the packets must be allowed or dropped when a match has been found.

Redirect/Mirror Port – Configure the port to which packets matching this ACL need to be redirected.

Priority - Specifies the priority for the access list. This value must be in the range from 1 to 255. The default priority value is 1.

Source and Destination IP Address – Specifies the IP Address of the Source and Destination for which the access list must be applied.

Subnet Mask– Specifies the Source and Destination Address Mask corresponding to the IP Address. ***Ports List (Incoming)*** – Specifies the Incoming Port List for which the access lists has to be applied.

Ports List (Outgoing) – Specifies the Outgoing Port List for which the access lists has to be applied

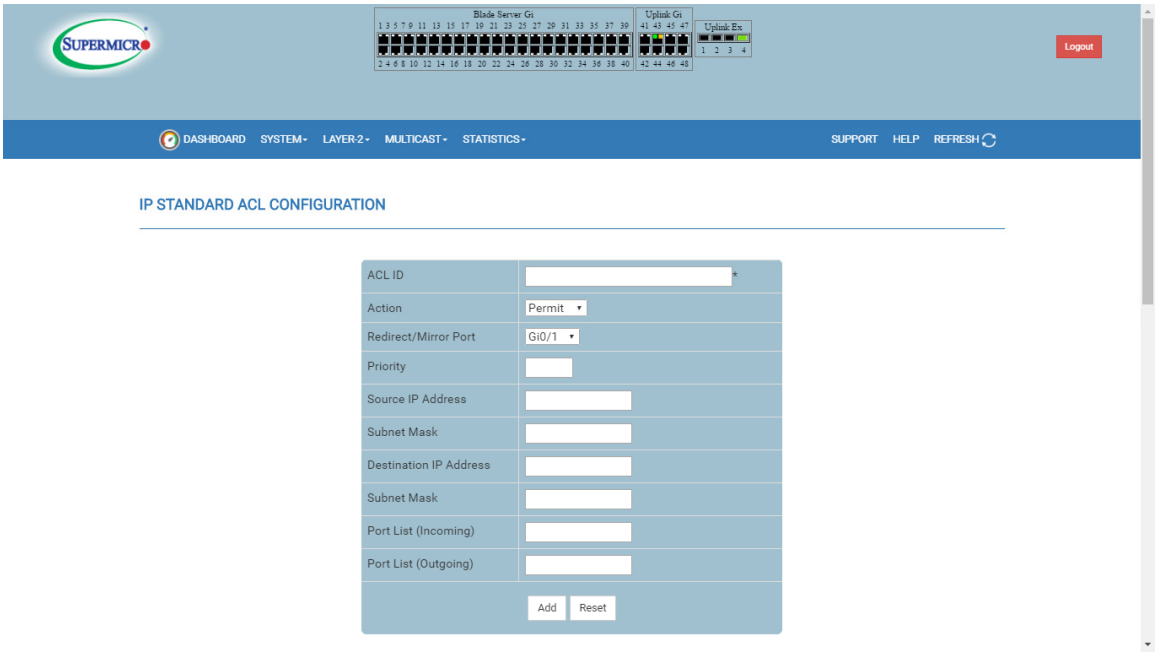


Fig : IP standard ACL

3.8.3 IP Extended ACL

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

This page displays the various parameters required to configure the Extended IP access lists. This table includes the following parameters for configuration.

ACL ID – Specifies the unique ID for the access list. This value must be in the range from 1 to 32768.

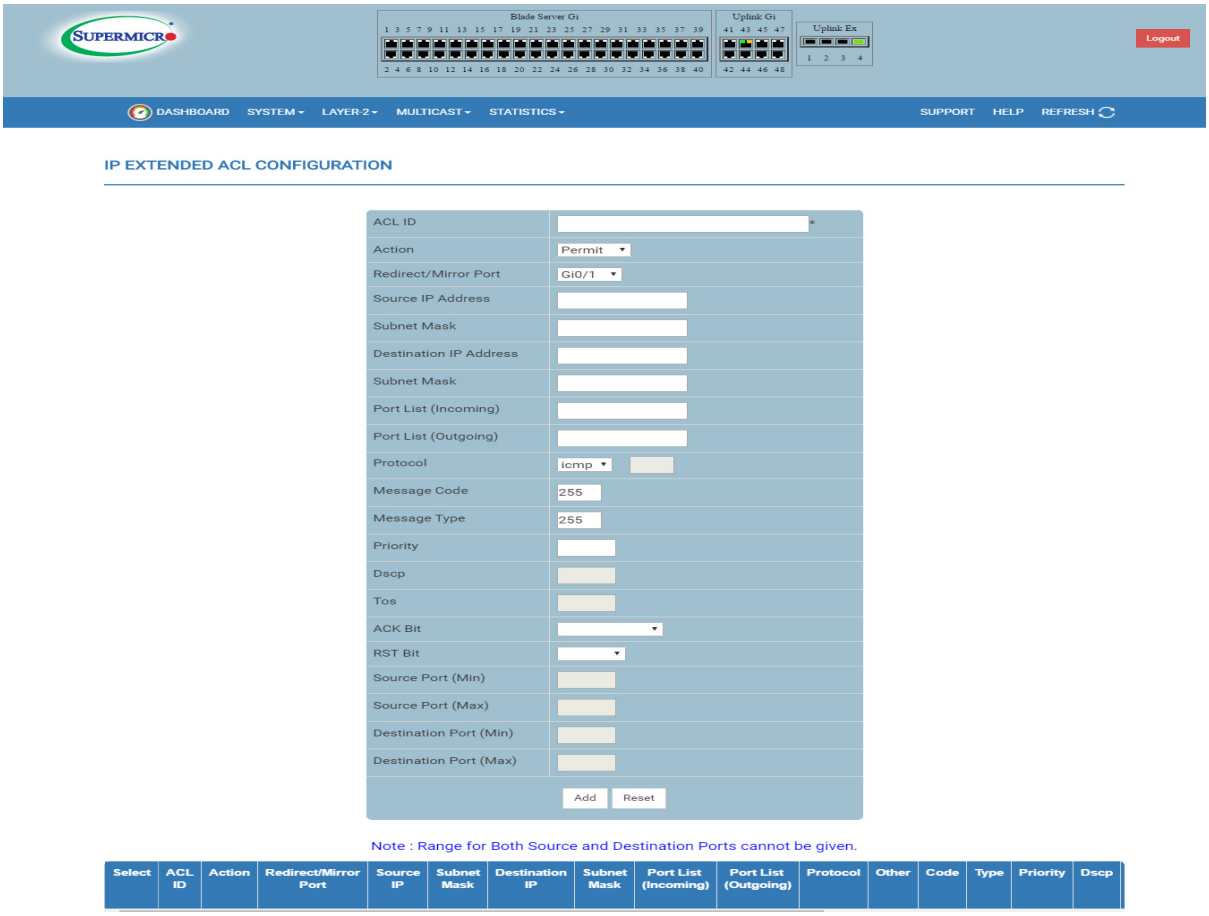


Fig: IP Extended ACL

Action – Specifies whether the packets must be allowed or dropped when a match has been found.

Redirect/Mirror Port **-** Configure the port to which packets matching this ACL need to be redirected.

Source and Destination IP Address – Specifies the IP Address of the Source and Destination for which the access list must be applied.

Subnet Mask – Specifies the Source and Destination Address Mask corresponding to the IP Address.

Ports List (Incoming) – Specifies the Incoming Port List for which the filter has to be applied.

Ports List (Outgoing) – Specifies the Outgoing Port List for which the filter has to be applied.

Protocol - Specifies the type of protocol.

Message Code – Specifies the Message Code to be checked for ICMP Packets

Message Type – Specifies the Message Type to be checked for ICMP Packets.

Priority – Specifies the Priority for the filter. This value must be in the range from 1 to 32768. The default priority value is 1.

Dscp - Specifies the DSCP value for the access list. Allowed range is 0 to 63 .

TOS – Specifies the Type of Service for the access list.

ACK Bit – Indicates the TCP Ack Bit to be checked against the incoming packet.

RST Bit – Indicates the TCP Reset Bit to be checked against the incoming packet.

Source Port (Min) – Specifies the TCP/UDP source port from which the access list has to be applied.

Source Port (Max) – Specifies the TCP/UDP source ports to which the access list has to be applied.

Destination Port (Min) – Specifies the TCP/UDP destination port from which the access list has to be applied.

Destination Port (Max) – Specifies the TCP/UDP destination port to which the access list has to be applied.

Other – This is only visible user to choose the Protocol as “other”. The allowed value ranges are 1 to 255. The default value is 1.

3.9 WEB GUI Settings

This page has all basic web GUI settings.

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. User can choose to enter other privilege level using this configuration if they have the enable password for the required privilege levels. The enable passwords for different levels are configurable in Management Security web page.

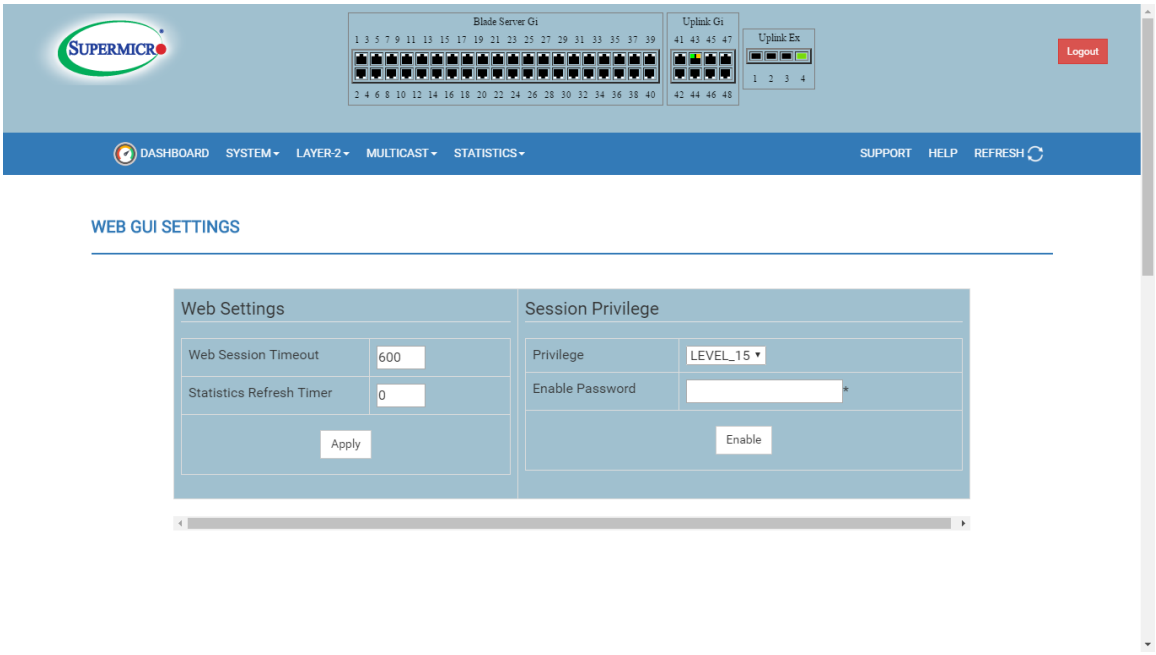


Fig: Web GUI Settings

3.10 QoS Basic settings

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

Basic Settings

Classmap

Policymap

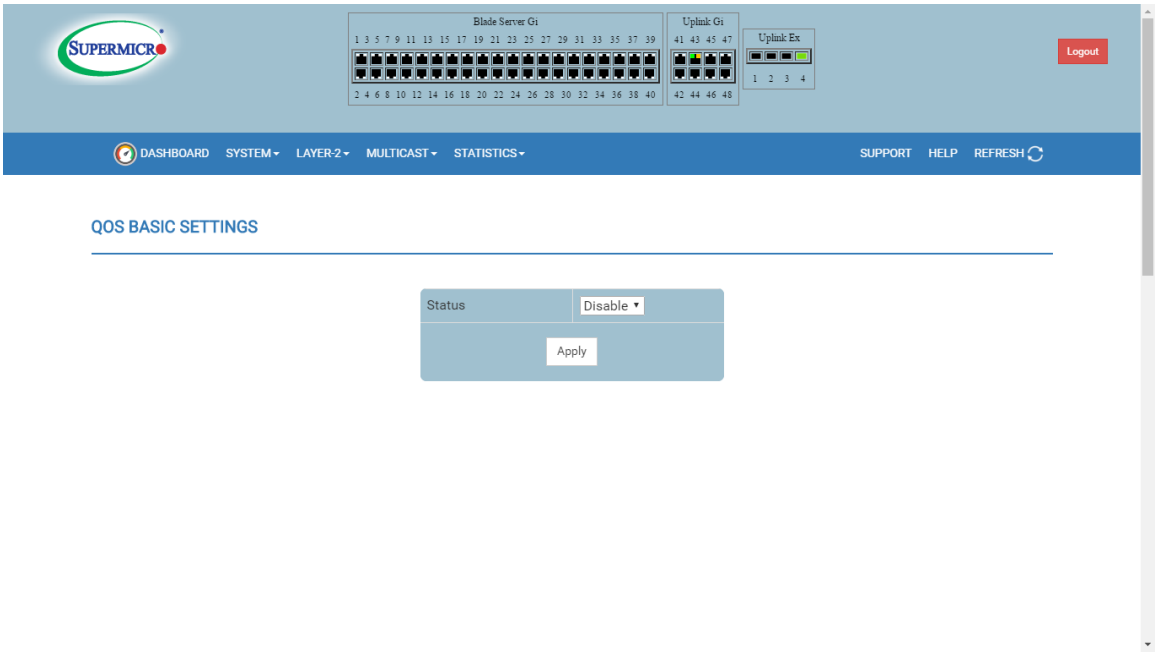


Fig: QoS Basic settings

The *Basic Settings* tab opens the **QoS Basic Settings** page. You need to configure the following:

Status- Allows enabling / disabling QoS status.

3.10.1 QoS Class Map

Classmap is used to classify the stream of traffic. The *Classmap* tab opens the **QoS Classmap Settings** page. The following fields are to be configured for classmap.

Classmap ID - Specifies a unique ID for Classmap. It must be in the range from 1 to 65535.

Filter ID – Specifies the unique filter ID associated with this Classmap.

Filter Type – Specifies the filter type associated with the Classmap. It can be set as either MAC filter (1) or IP filter (2).

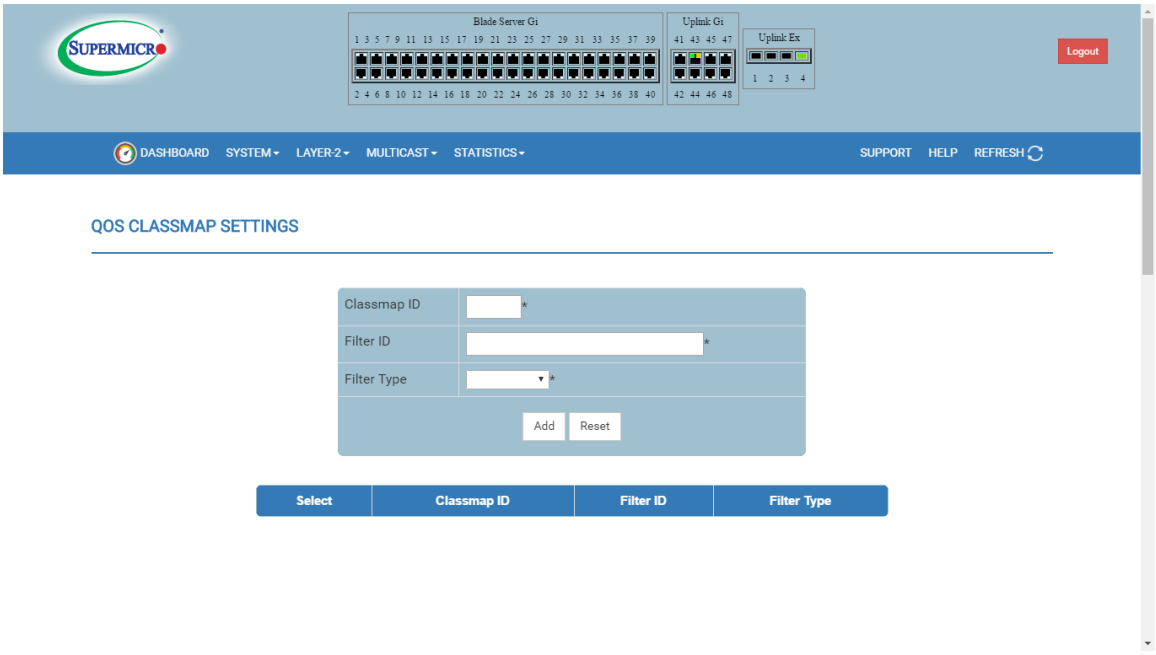


Fig: QoS Class Map

3.10.2 QoS Policy Map

Policymap is used to specify action for a specified classmap. The *Policymap* tab opens the **QoS Policymap Settings** page. This page has the following fields to configure Policymap.

Policy Map ID - Specifies the unique ID for Policy Map. The value ranges between 1 to 65535.

Class Map ID - Specifies the Class map Id to associate with Policy map. The value ranges between 1 to 65535.

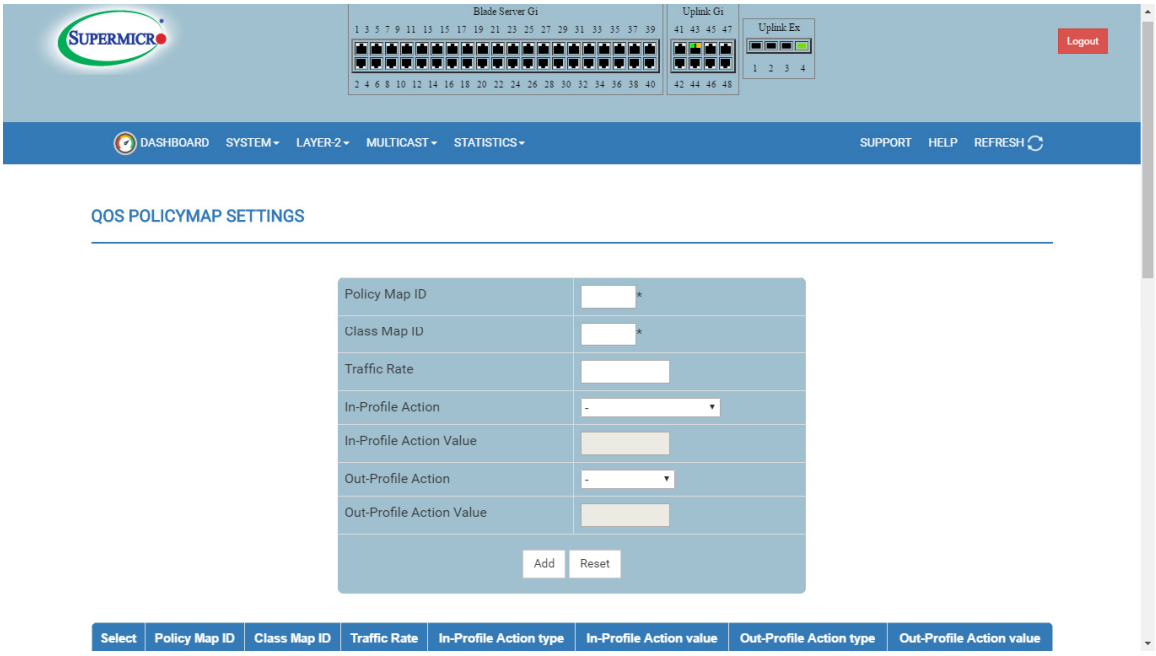


Fig: QoS Policy Map

Traffic Rate - Specifies the Traffic rate of data for which action has to be applied.

In-Profile Action- Specifies the action to be applied on matched data. In Profile Action can be specified as Policy DSCP or Policy Precedence.

Out-Profile Action- Specifies the action to be applied on out profile data. Out Profile Action can be specified as Policy DSCP or Drop.

In-Profile Action Value- In Profile Action Value can be specified from 0 to 7 for IP precedence and Priority or from 0 to 63 for DSCP .

Out-Profile Action Value – Out Profile Action Value can be specified as drop or from 0 to 63 for DSCP.

The VLAN COS link allows user to configure VLAN COS through following pages:

1. COS Queue Mapping
2. Queue Configuration

3.10.3 COS Queue Mapping

COSQ Mapping page allows to choose the Class of Service(COS) for VLAN.

COS – Configure the Class of Service value ranges from 0 to 7. The value 0 for low priority, 7 for high priority.

Queue – This supports to configure the mapping of CoS priority to a queue. Each queue is mapped to eight egress queues in the switch. This allows values from 0 to 7.

Reset to Defaults – Set default CosQ mapping.

COS	Default value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

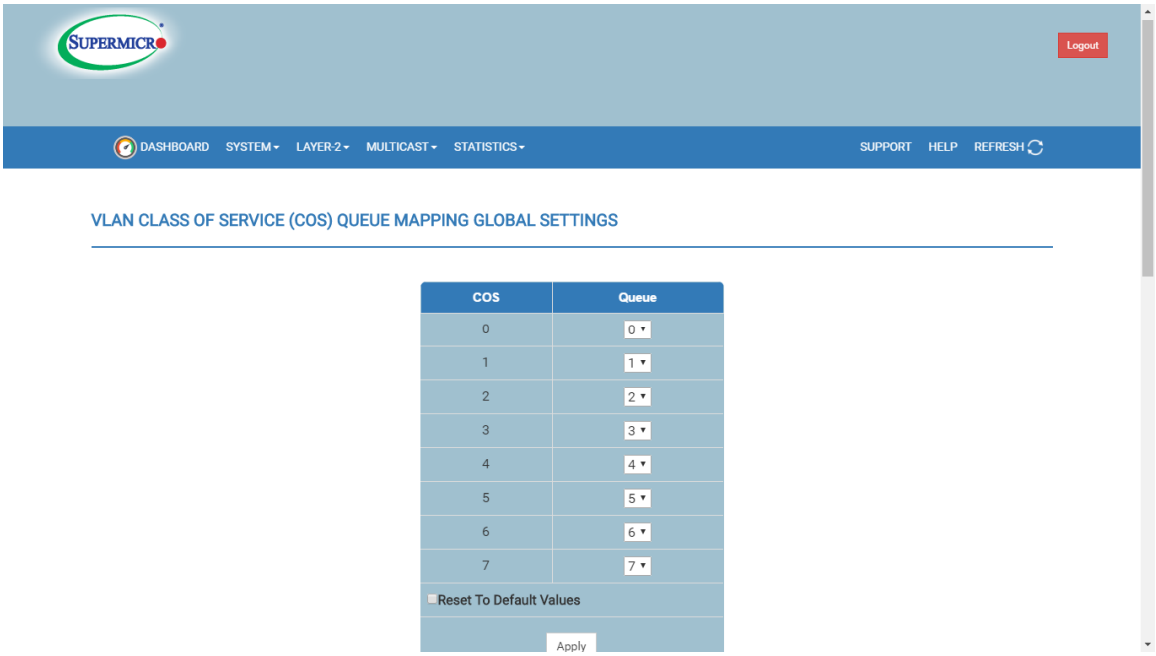


Fig: COSQ Mapping Global Setting

3.10.4 Queue Configuration

COSQ scheduling and Bandwidth Control page allows to configure the weight and bandwidth for Queues.

Port - Specifies the Port number .

Scheduling Algorithm – Specifies the scheduling algorithm, which can be Strict Priority or Round Robin or Weighted Round Robin or Deficit Round Robin.

Default Priority (Ingress) – This priority shall be used for incoming untagged packets. Specifies the priority value from 0 to 7. The default priority is 0.

Queue – To configure the weight, minimum and maximum bandwidth for each queue. This range is 0 to 7.

Weight - Configures the queue weights in range of 0-15 .

Min Bandwidth - Configures minimum bandwidth between 1 to 1000000000.

Max Bandwidth - Configures minimum bandwidth between 1 to 1000000000.

Reset to Defaults - Sets the default values for all the configuration in this page.

Apply On Port Lists - To apply the same configuration on multiple ports, provide the port list on this field and click on Apply. For example the port list should be like gi0/1-10, gi0/12, gi0/15.

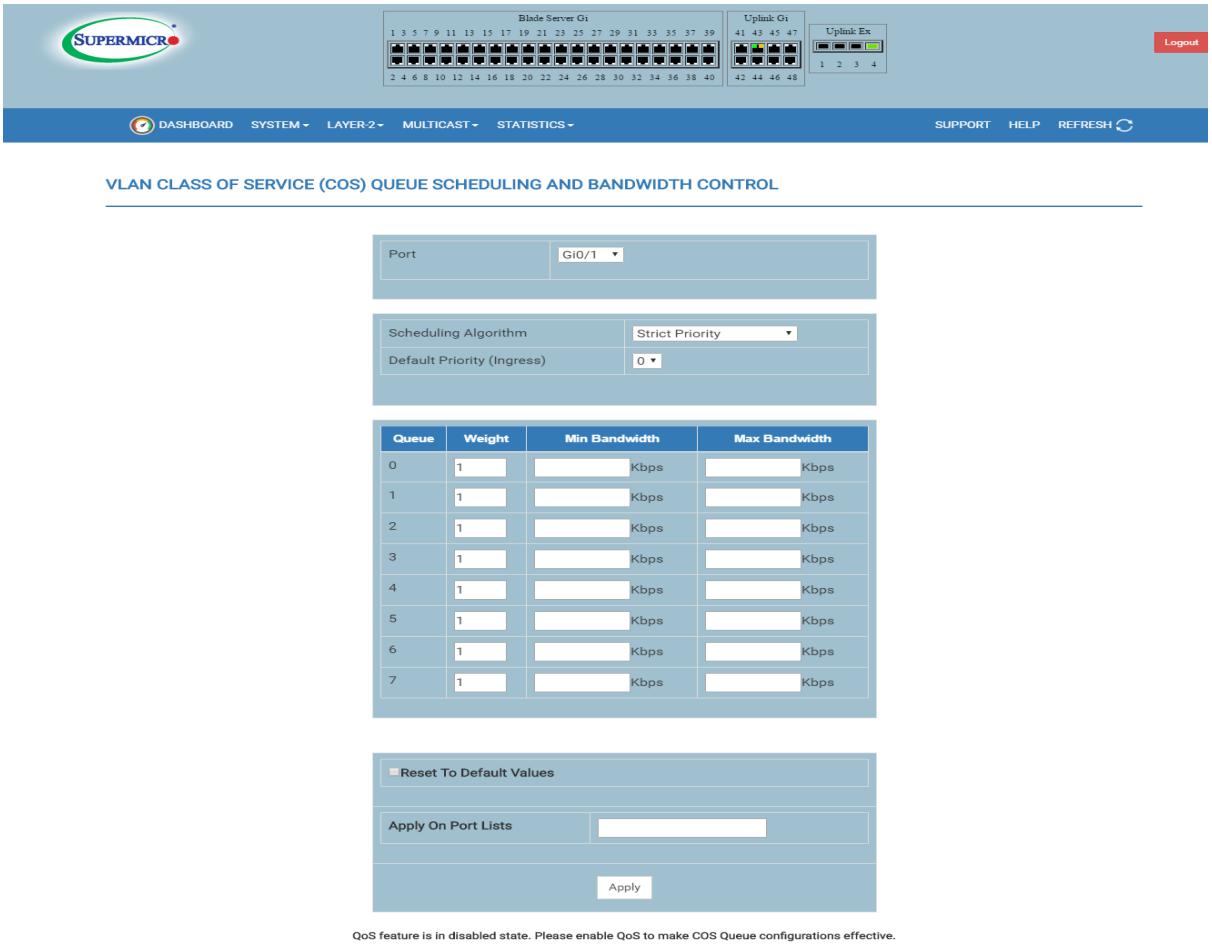


Fig: COSQ Scheduling and Bandwidth Control

3.11 SNMP AGENT

Layer2 SMIS supports only SNMP Agent. By default SNMP Agent is enabled.

SNMP Agent provides the following configurations.

SNMP Community Settings - To configure SNMP community including community index, name, security name, context name, transport tag and storage type.

SNMP Group Settings - To configure SNMP groups including group name, security name, security model and storage type.

SNMP Group Access Settings - To configure SNMP groups access parameters including group name, security model, security level, storage type, and read, write, notify view.

SNMP View Tree Settings - To configure SNMP view tree including view name, sub tree, mask, type of the view and storage type.

SNMP Target Address Settings - To configure SNMP target including target name, target IP, transport tag, param and storage type.

SNMP Target Parameter Settings - To configure SNMP target parameters including parameter name, MP model, security model, name, level and storage type.

SNMP Security Settings - To configure SNMP security including user name, authentication protocol, authentication key, privacy protocol, privacy key and storage type.

SNMP Trap Settings - To configure SNMP trap notifications including notify name, notify tag, notify type and storage type.

3.11.1 SNMP Community settings

SNMP community settings page allows to add SNMP managers or remove existing managers.

Community index - Community index identifier.

Community name - Community name string.

Security name - User name string.

Context name - Context name through which the management information is accessed when using the community string specified by the corresponding instance of SNMP community name.

Transport tag - Transport tag identifier.

Storage type - Volatile storage or non-volatile storage.

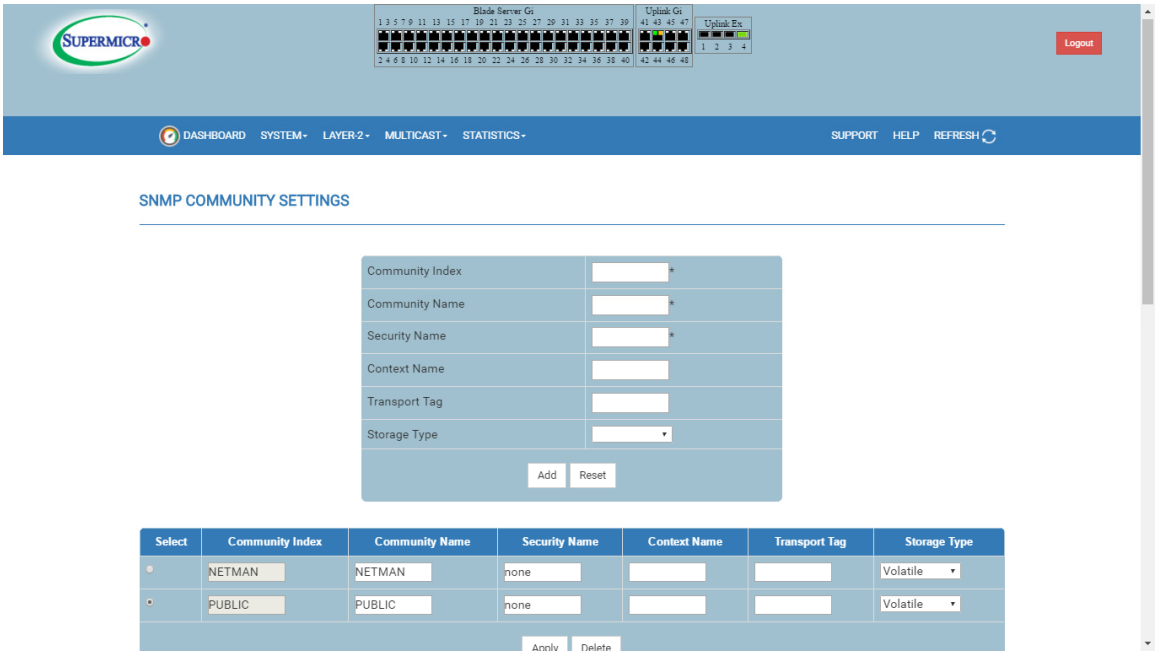


Fig: SNMP Community settings

3.11.2 SNMP Group Settings

SNMP group settings page helps mapping a combination of Security Model and 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.

Security model - version 1, version 2 or version 3.

Security name - security name string.

Group name - group name string.

Storage type - volatile or non-volatile.

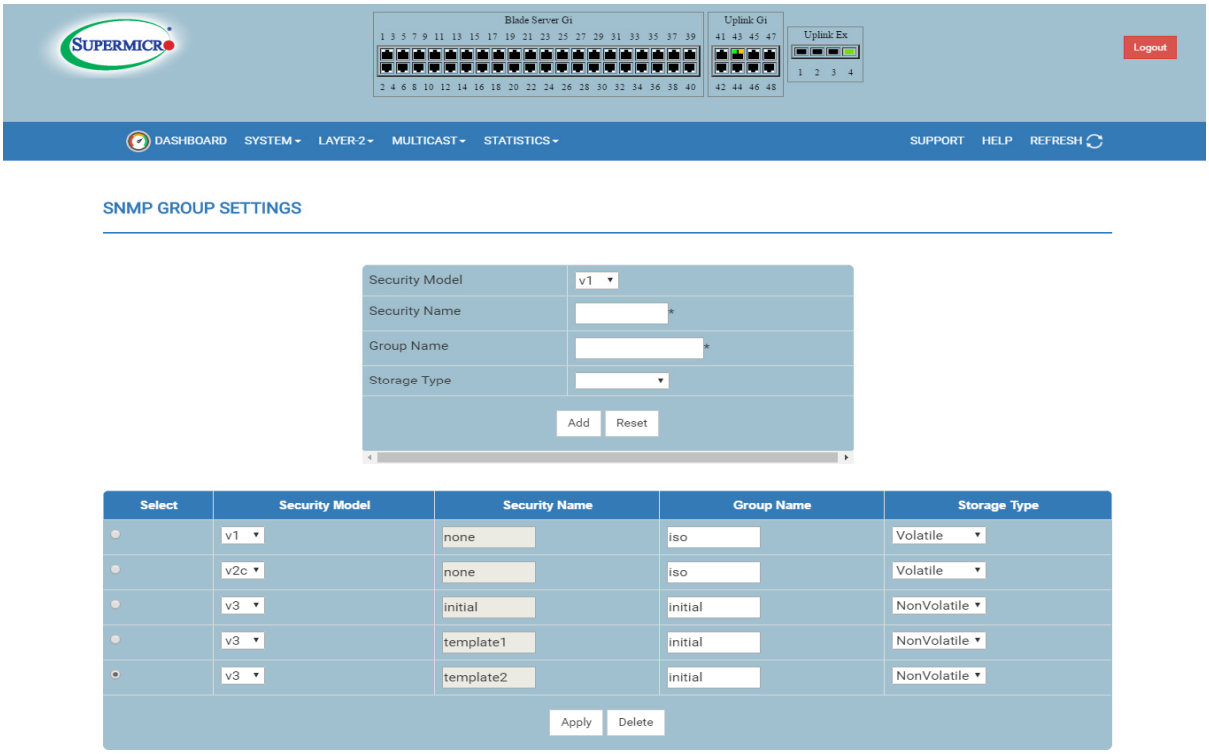


Fig: SNMP Group settings

3.11.3 SNMP Group Access Settings

SNMP group access settings page displays access rights of groups. Each entry is indexed by a Group Name, a Context Prefix, a Security Model and a Security Level. 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. A SNMP Group has to be created prior to the Group Access configuration.

Group name - group name string.

Security model - SNMP version v1, v2 or v3. Version 3 is the most secure model as it allows packet encryption with the private key word.

Security level - no-authentication option disables authentication. Authentication option enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. Private option selects both authentication and privacy.

Read view - read view identifier.

Write view - write view identifier.

Notify view - notify view identifier.

Storage type - Volatile storage or non-volatile storage.

Context – User can configure a SNMP context name that identifies this group.

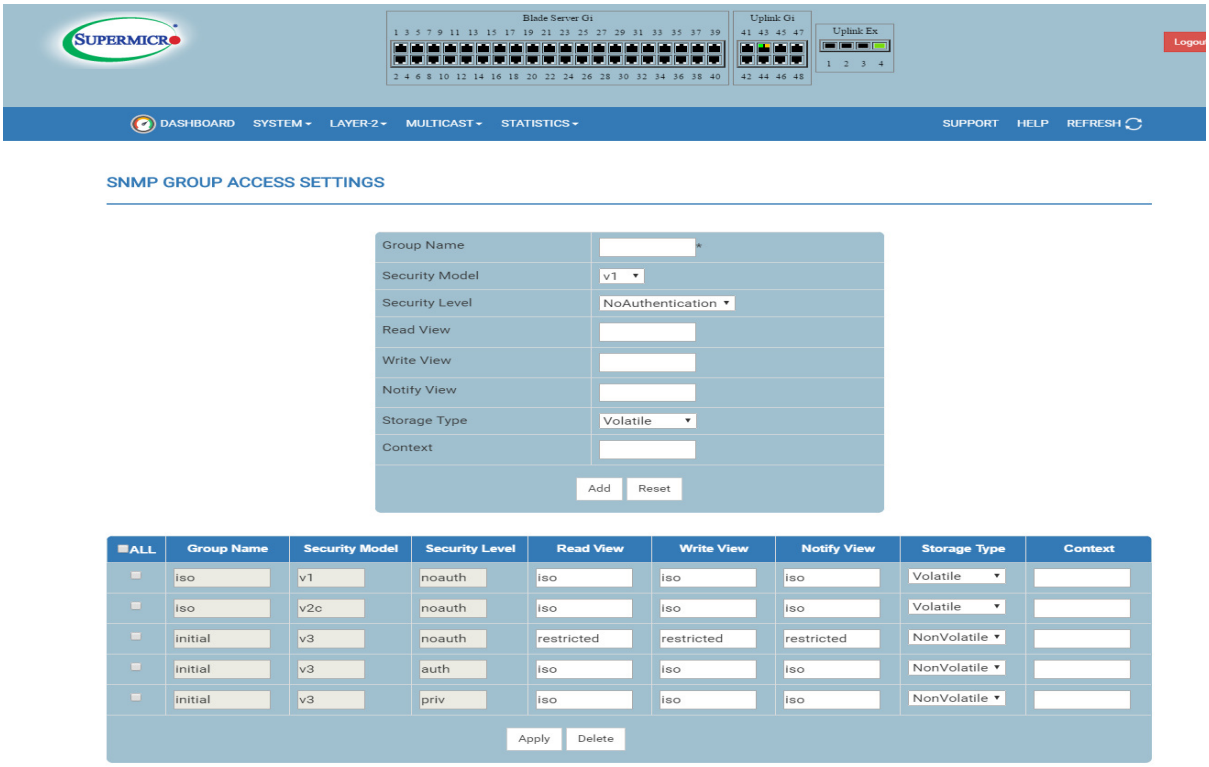


Fig: SNMP Group Access Settings

3.11.4 SNMP View Tree settings

SNMP view tree settings page allows configuration of view trees. A SubTree when combined with the corresponding instance of Mask defines a family of view sub trees. View Name is the name for a family of view sub trees. This page also displays the Storage Type of the View Tree table. A SNMP Group and SNMP Access settings have to be created prior to the Group View configuration.

View name - view name string.

SubTree - tree OID.

Mask - OID mask.

View type - included or excluded.

Storage type - volatile or non-volatile.

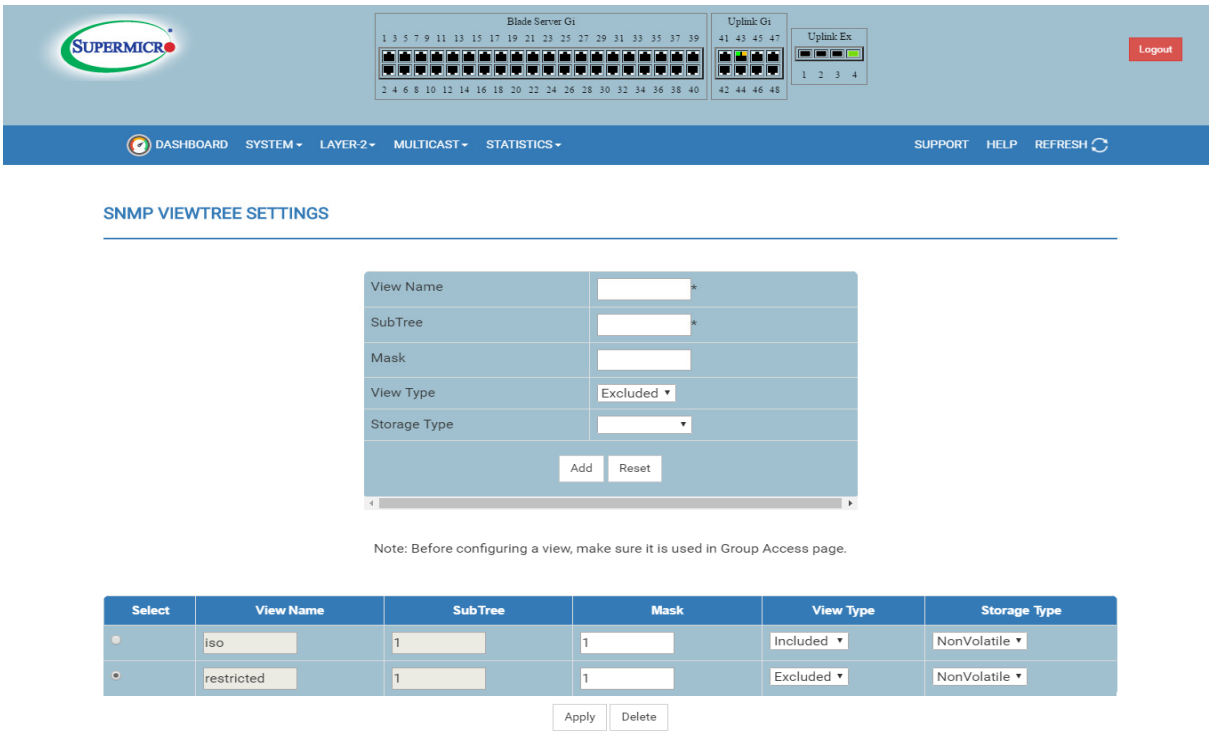


Fig: SNMP View Tree settings

3.11.5 SNMP Target Address Settings

SNMP target address settings page helps configuring SNMP target address parameters.

Target name - Target Name is 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 - Timeout specifies the maximum round trip for communicating with the Target IP address.

Target Retries - Retries specifies number of attempts to be made when no response is received.

Transport tag - Transport tag value is used to select target address for a particular operation.

Param - Param contains SNMP parameters to be used when generating messages to be sent to transport address.

Storage type - volatile or non-volatile.

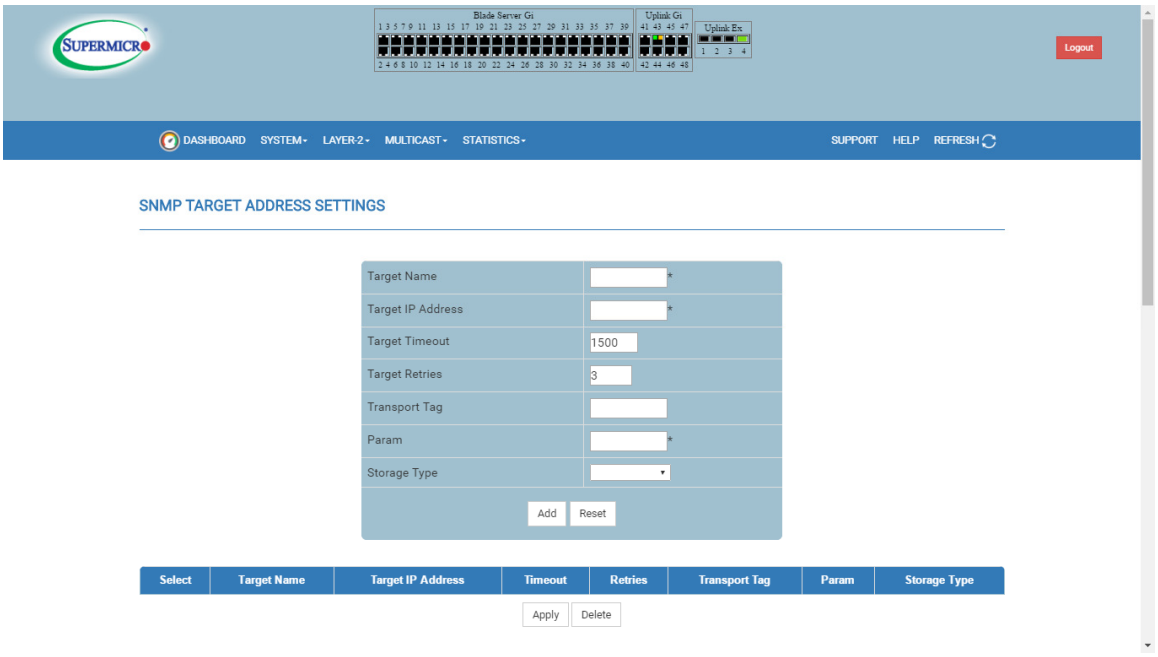


Fig: SNMP Target Address Settings

3.11.6 SNMP Target Parameter Settings

SNMP target parameter settings page helps configuring SNMP target address parameters.

Parameter name - The target param is an unique name, specifies SNMP target information to be used in the generation of SNMP messages.

MP model - Message Processing (MP) Model will be used when generating SNMP messages using this entry.

Security model - Security Model will be used when generating SNMP messages using this entry.

Security name - The Security Name identifies the current Param Name, on whose behalf SNMP messages will be generated.

Security level - Security Level specifies the Level of Security to be used when generating SNMP messages.

Storage type - Storage Type can be configured as Volatile or Non-Volatile.

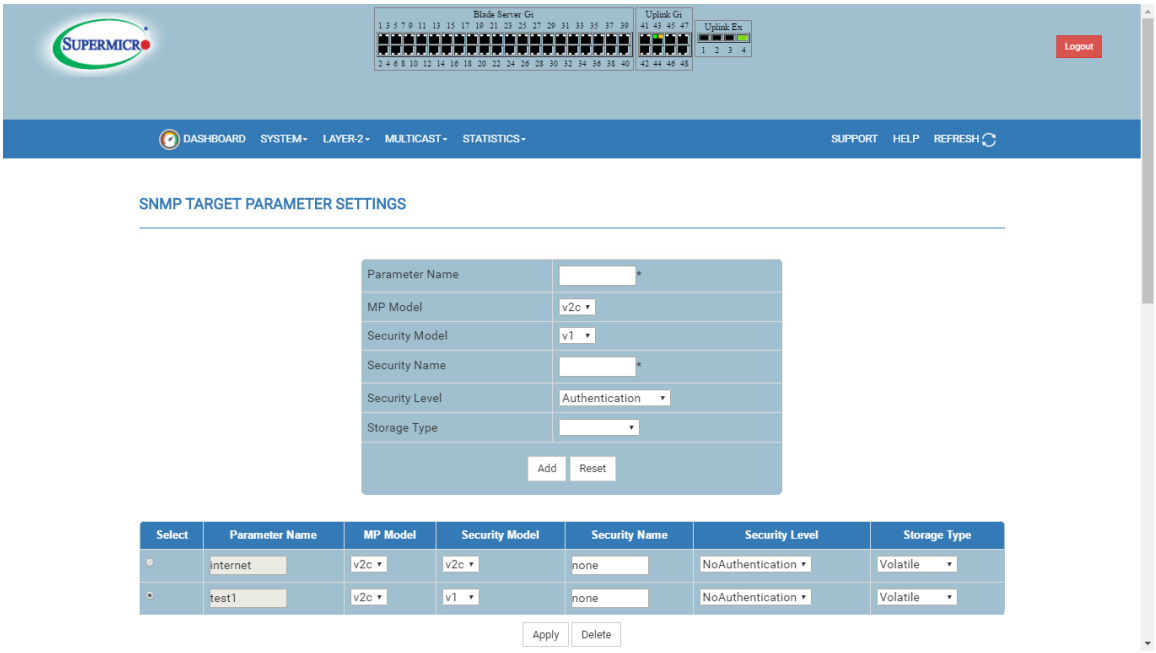


Fig: SNMP Target Parameter settings

3.11.7 SNMP User settings

SNMP security settings page helps configuring users configured in the SNMP for the User-based Security Model.

User name - User Name is the (User-based Security) Model dependent security ID.

Authentication protocol - Authentication Protocol is the type of authentication protocol used for authentication.

Authentication key - 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 messages sent on behalf of this user to/from the SNMP, can be protected from disclosure, and if so, the type of privacy protocol which is used.

Privacy key - Privacy key is an indication of whether messages sent on behalf of this user to/from the SNMP, can be protected from disclosure.

Storage type - Storage Type can be configured as Volatile or Non-Volatile.

Engine Id – Displays the SNMP Engine Id.

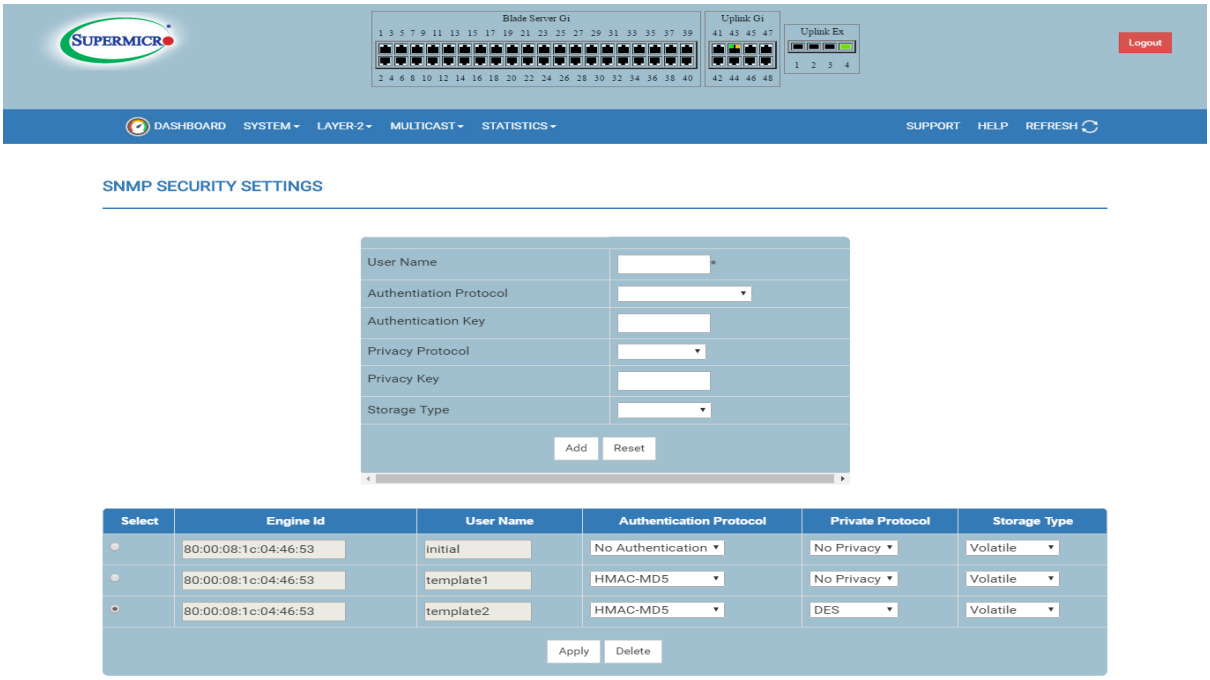


Fig: SNMP Security settings

3.11.8 SNMP Trap Settings

SNMP trap settings page helps configuring set of management targets which must receive notifications.

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, which 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 - volatile or non-volatile.

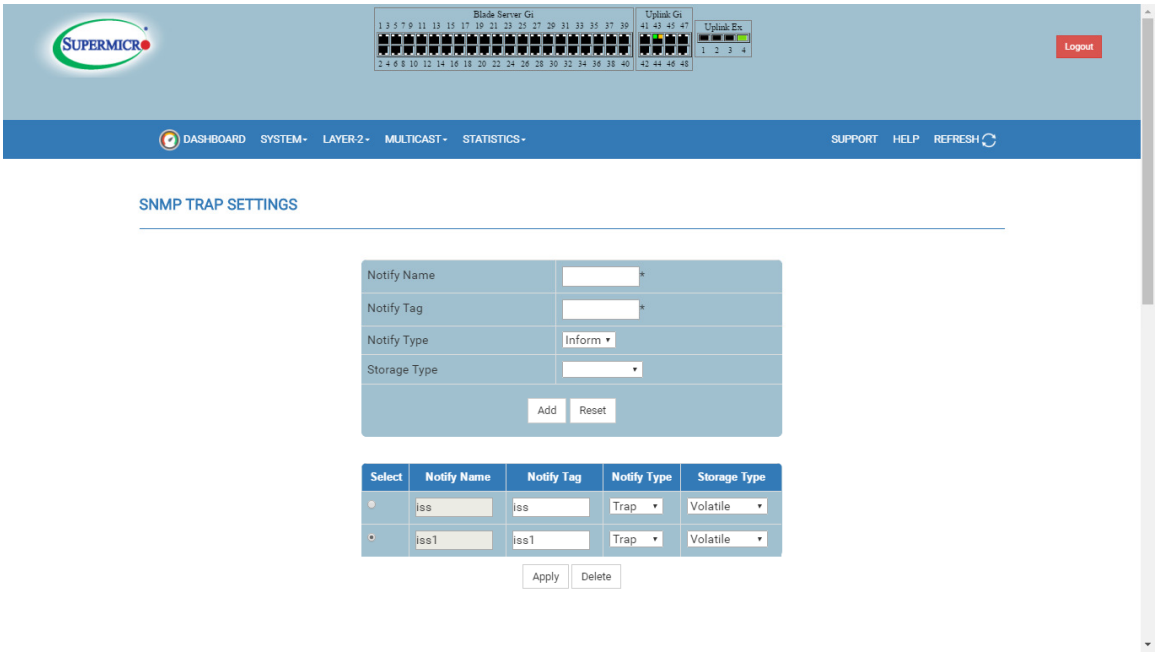


Fig: SNMP Trap Settings

3.12 Time Management

This page helps configuring Network Time Protocol (NTP) and clock.

3.12.1 NTP Settings

NTP Client Settings

Ntp Status - This field enables or disabled NTP in switch. Configure NTP servers to enable NTP.

Receive Server Update - It could be Broadcast or Unicast. To process the broadcast NTP updates from server, choose Broadcast option.

Time zone Settings

Posix Format Offset - Enter time zone name in a string format.

NTP Servers

Server IP Address - NTP server IP address.

Key - Choose the key from the configured list. These keys are configurable in this page in NTP Server Keys fields.

Preferred - Choose Yes in case if this server need to preferred over other configured NTP servers. User can add multiple NTP servers.

NTP Servers Keys

Key Id - A number to identify configure key strings.

Key String - Any string to be used as key to handshake with NTP servers.

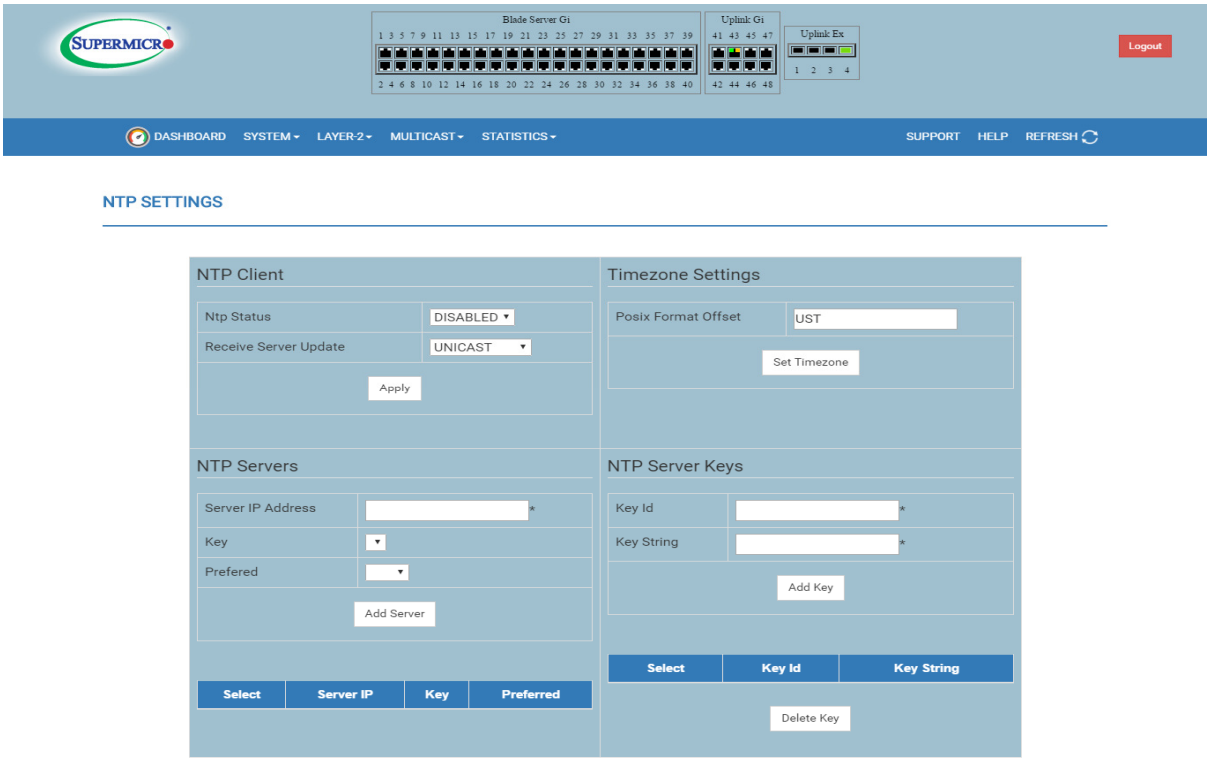


Fig: NTP

3.12.2 Clock Settings

The system clock in Supermicro switches runs from the time the switch starts up and keeps track of the system date and time. The system clock can also be manually configured. System time configured manually will remain accurate until the next restart. Manual configuration of the system clock is useful when the system time cannot be obtained from any other source, such as from NTP associations.

Clock Display – This displays the date, time and year.

Clock Set

Time – User can configure time in Hour: Minutes: Seconds format.

Date – User can configure day in 1 to 31, month in 1 to 12 and the year in 2000 to 2035.

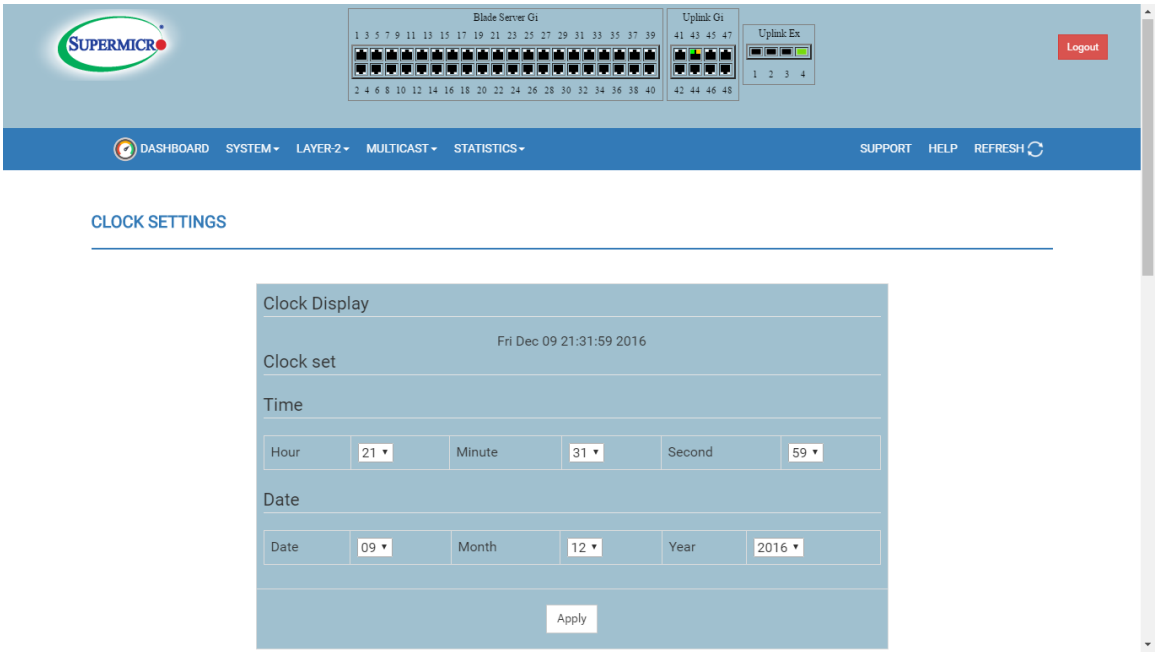


Fig: Clock Settings

4 Layer 2 Management

This page has links to all features present in the layer2 group.

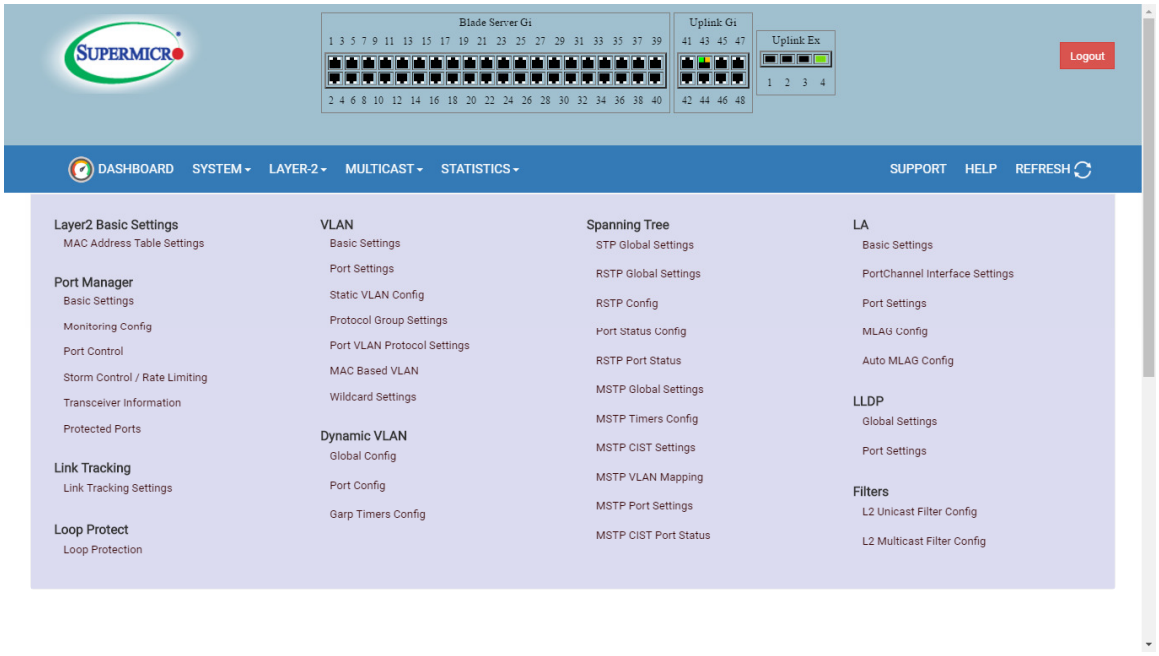


Fig: Layer 2 Management

4.1 Layer 2 Basic Settings

This page has option to change MAC aging time. Mac address confirmation can be done with this time interval. The MAC aging time value ranges between 10 to 1000000.The default value is 300.

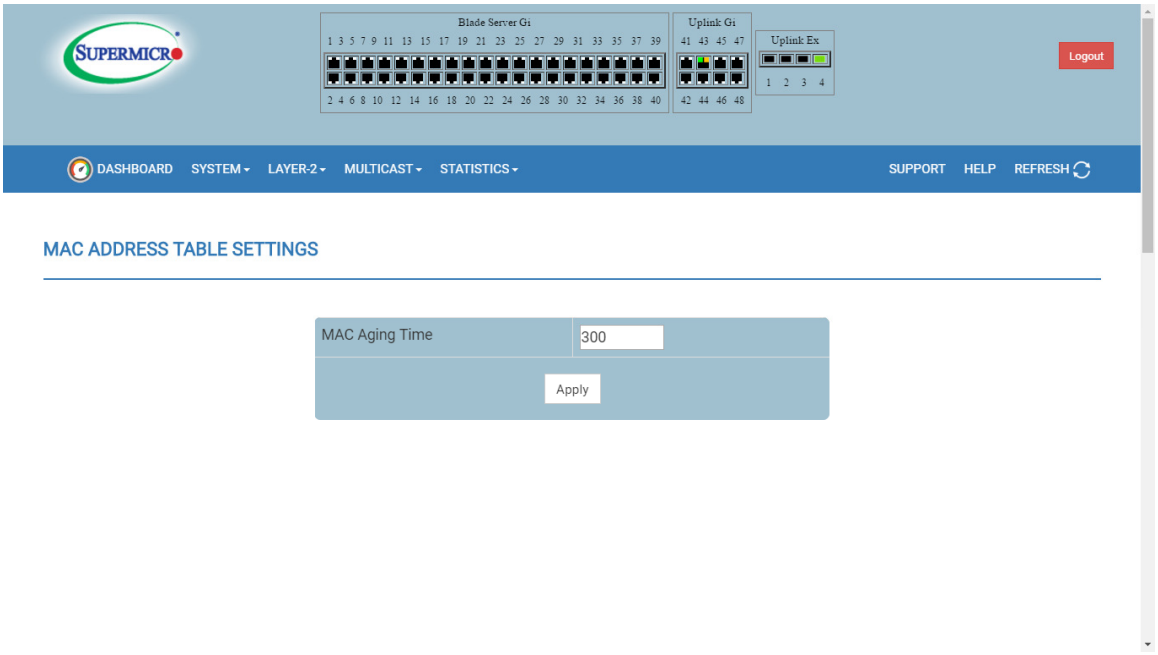


Fig: Layer 2 basic settings

4.2 Port Manager

The *Port Manager* link has links to the following web pages:

- Basic Settings
- Port Monitoring
- Port Control
- Strom Control / Rate Limiting
- Transceiver Information
- Protected Ports

Note

In all port based configuration pages, the port number group links are provided in top. For e.g. as Gi1/1 – Ex 1/2. In normal standalone operation of the switch, there shall be only one link and the corresponding port configuration are displayed below.

4.2.1 Port Basic Settings

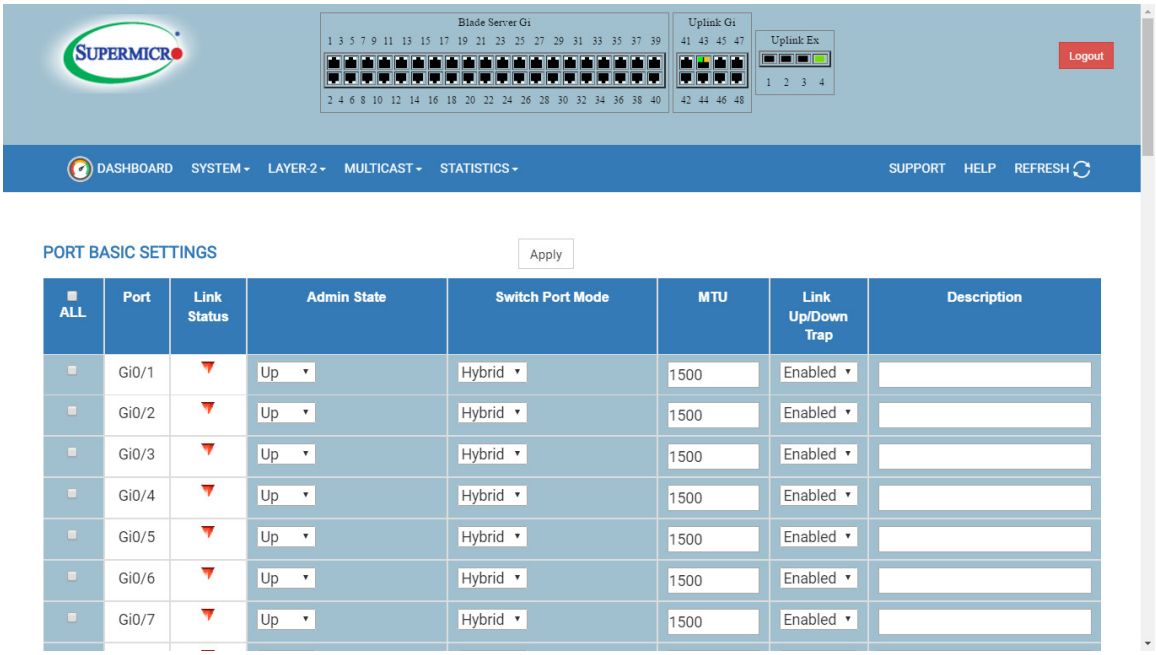


Fig: Port Manager Basic Settings

Port basic settings page allows to configure the port status and mode information. This page also helps configuring priority and MTU.

Port - Port number.

Link status - Physical link status as UP or Down arrow. A green arrow indicates that the status of the port is up and the red arrow indicates that the status of the port is down.

Admin state - Administratively configured state as Up or Down.

Switch port mode - Access or Trunk or Hybrid

MTU - MTU value. Minimum 1500 and Maximum 9216 . Port must be administratively down to change the MTU.

Link up / **Down trap** - Enables or disables SNMP trap generation for port up and down events.

Description – User can specify the description for each port.

4.2.2 Port Monitoring

Port monitoring page allows to enable or disable monitoring on port interface.

Session Id - User can configure session value between 1 to 4.

Destination Port – Port number for Destination.

Ingress Monitoring Source Ports - Receive port number.

Egress Monitoring Source Ports - Transmit port number.

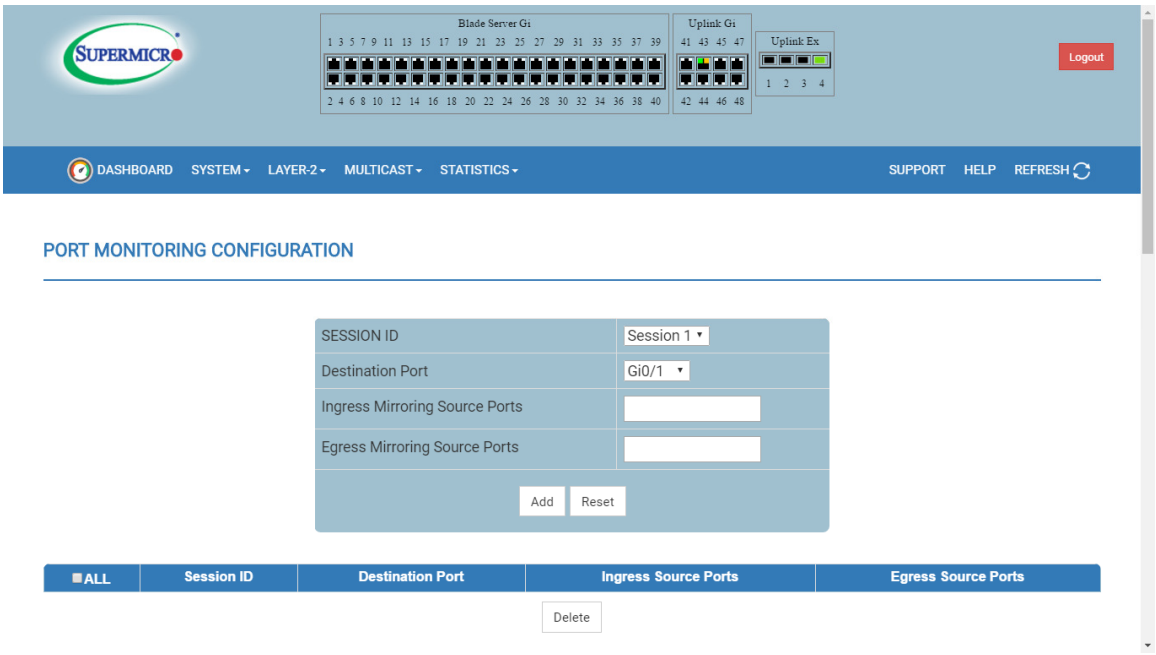


Fig: port Monitoring

4.2.3 Port Control

Port control settings page allows configuration of the port specific parameters. User can choose between auto-negotiation and no-negotiation for a port. If no negotiation is chosen then the speed of the link, Flow Control, duplex modes can be configured.

Port - Port number.

Mode - Auto negotiation or no-negotiation.

Advert - It is used only in Auto negotiation mode for 1G ports. The configuration options are 10MH, 10MF, 100MH, 100MF and 1000MF. By default all of these modes are initialized for each port.

Duplex - Full duplex or half duplex.

Speed - 10 Mbps, 100 Mbps, 1Gbps.

Flow control admin status - Either as disabled or transmit flow control enabled or receive flow control enabled or both transmit and receive flow control enabled.

Flow control operation status - Displays the status of the flow control.

HOL block prevention - Enable or disable Head of Line block prevention.

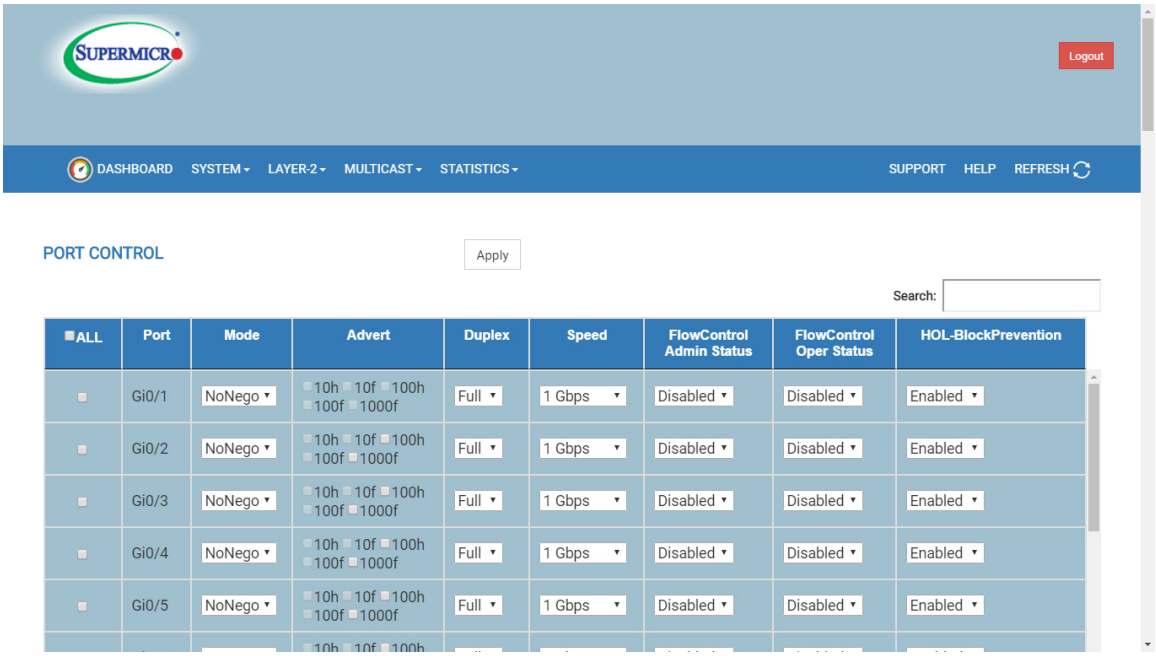


Fig: Port control

4.2.4 Rate Limiting

Rate limiting page allows to configure rate limiting for port interface.

Port - Port number. The following parameters configurable for storm control. .

DLF level- Destination lookup failure packets per second.

Broadcast level - Broadcast packets per second.

Multicast level - Multicast packets per second. The following parameters configurable for egress rate limiting.

Egress port rate limit - Egress limit of packets kilobits per second.

Egress port burst size - Egress limit of packet burst size in kilobits .

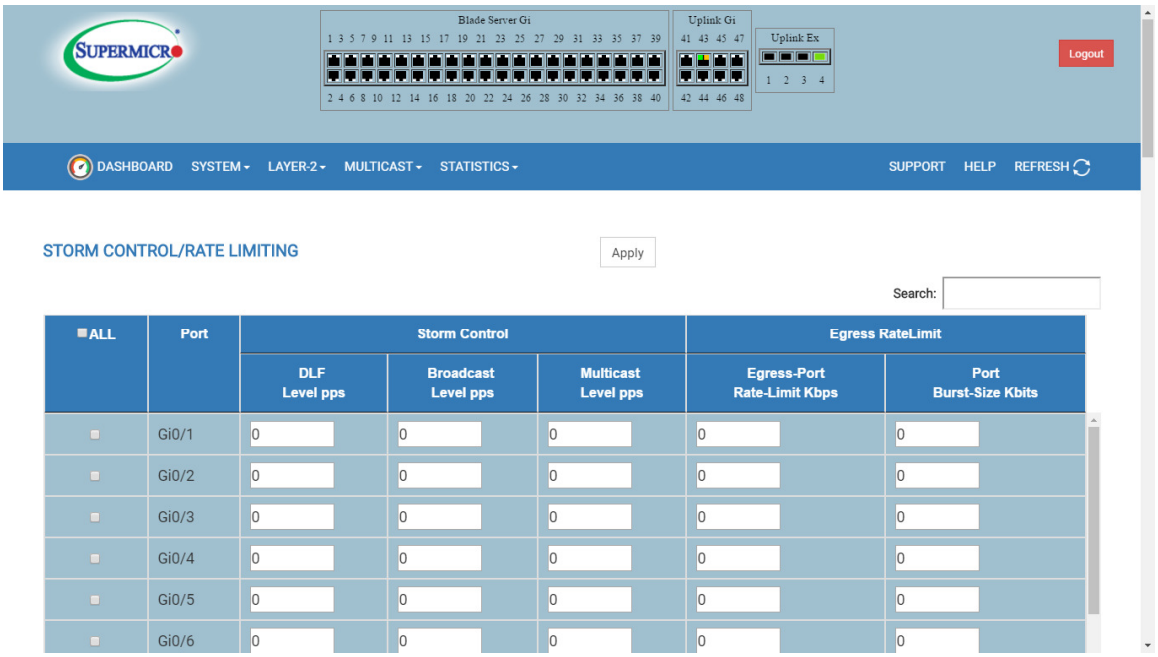


Fig: Rate Limiting

4.2.5 Transceiver Information

Transceiver Information page displays the EEPROM data of each SFP module.

Port - Port number.
Status - Present or Not Present.
Connector Type - Indicates the external optical or electrical cable connector provided as the media interface.
Vendor Name - The full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Part Number - The vendor part number or product name.
Revision - The vendor¡¦s product revision number.
Serial Number - The vendor¡¦s serial number for the transceiver.

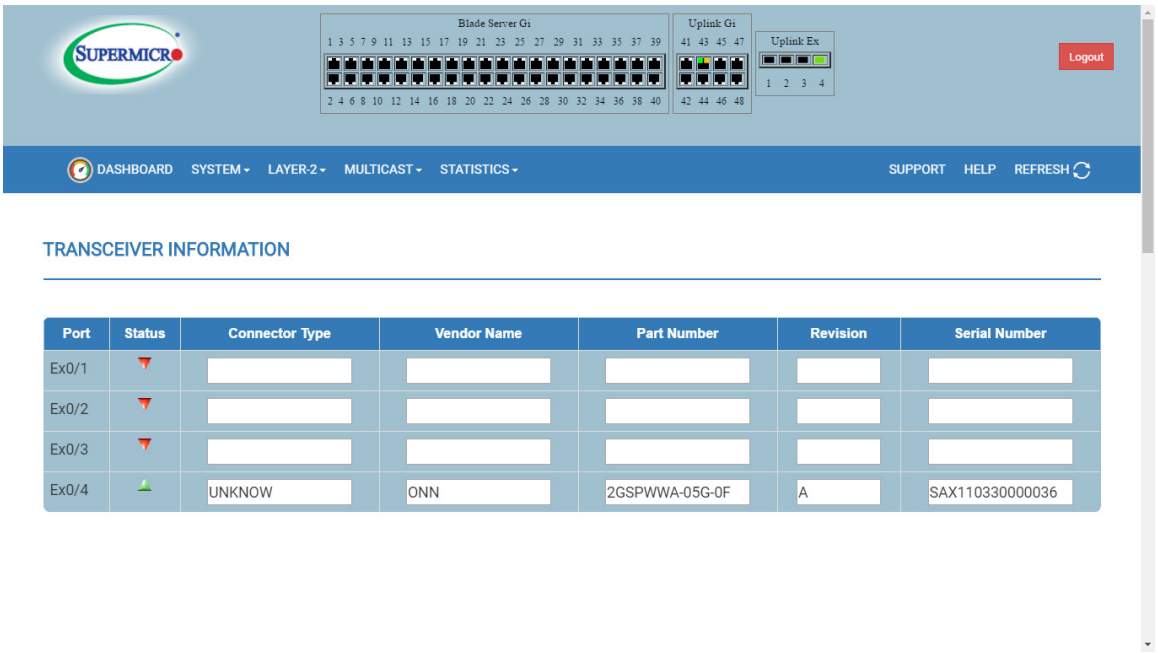


Fig: Transceiver Information

4.2.6 Protected Ports

Protected port settings page allows configuration of the port specific protected parameters. User can choose between non protected or protected for a port. If protected port, it can be standalone or the one group member.

Port – Port number.

Port Mode – This helps to configure the mode as Normal or Protected port or Protected Group,

Group ID – Choose the group identifier**.** This is enabled only in the Protected Group mode**.** 0 means the standalone protected port.

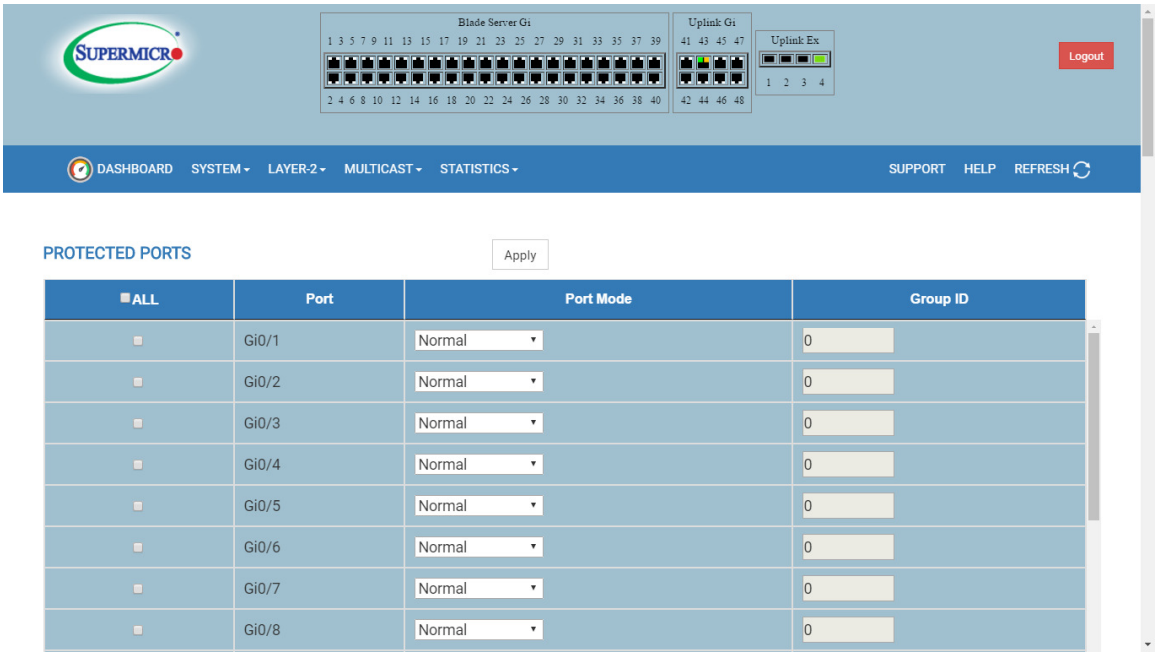


Fig: Protected Ports

4.3 Link Tracking

The Link Tracking allows user to configure link tracking information.

Link Status Tracking – Enable or Disable the link status.

Configure new Group has the below fields.

Group Id – Specifies the group Id***.*** The group identifiers should be valid number between 1 to 1024.

Upstream Interfaces – Each group can have one or more upstream interfaces. Physical ports (Gi/Ex) and port channel interfaces can be configured as upstream ports.

Downstream Interfaces - Each group can have one or more upstream interfaces. Physical ports (Gi/Ex) and port channel interfaces can be configured as upstream ports.

Status – Current status of link tracking up or down.

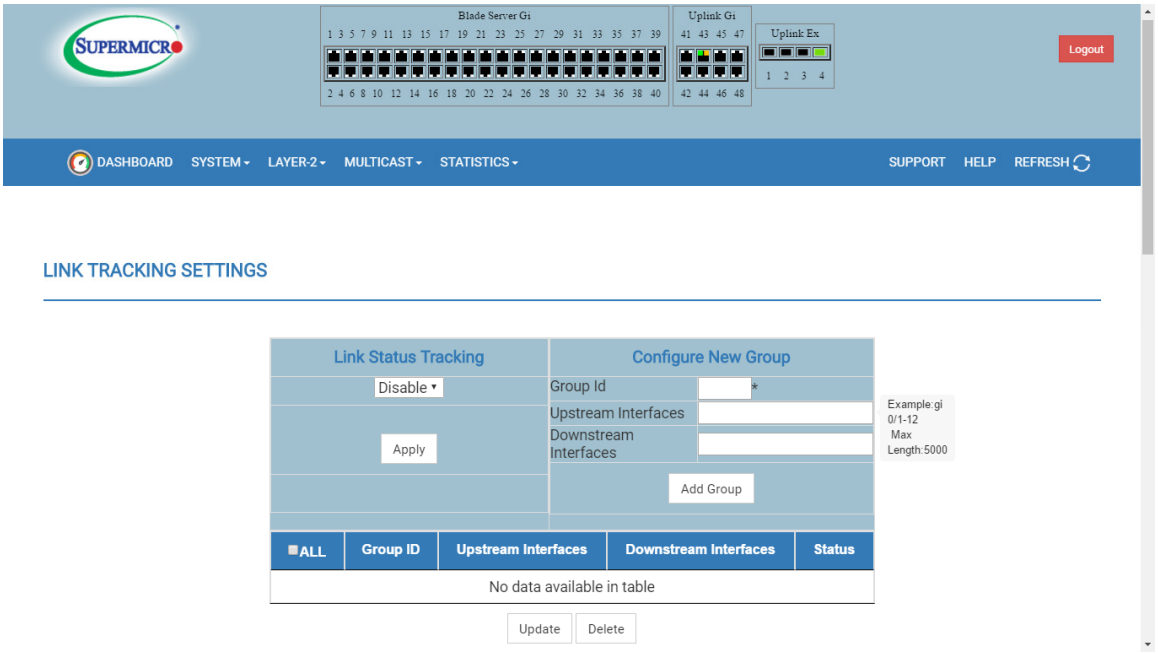


Fig: Link Tracking

4.4 Loop Protect

The Loop Protect page allows configuration of loop protect information.

Loop Protection – Enable or disable loop protection feature.

Transmit Interval – Number of seconds between subsequent Ethernet control frames sent out. User can choose the interval between 1 to 10 seconds. The default value is 5 seconds.

Disable Period – The number of seconds the loop detected ports should be in disabled state and will be enabled again after this interval of seconds. If this value zero, the ports will be kept in disabled state until user enable the port by disabling, enabling loop protection on that port. The supported values are from 0 to 604800 seconds.

Receive Action – This allows to configure the action whether “send disable” or “no disable”

Ports List – Configure the ports configured in which loop is to be detected. User can also specify port range, for example gi0/1-10, gi0/15, gi0/20..

The interface, interface status and loop detected status are displayed in second table.

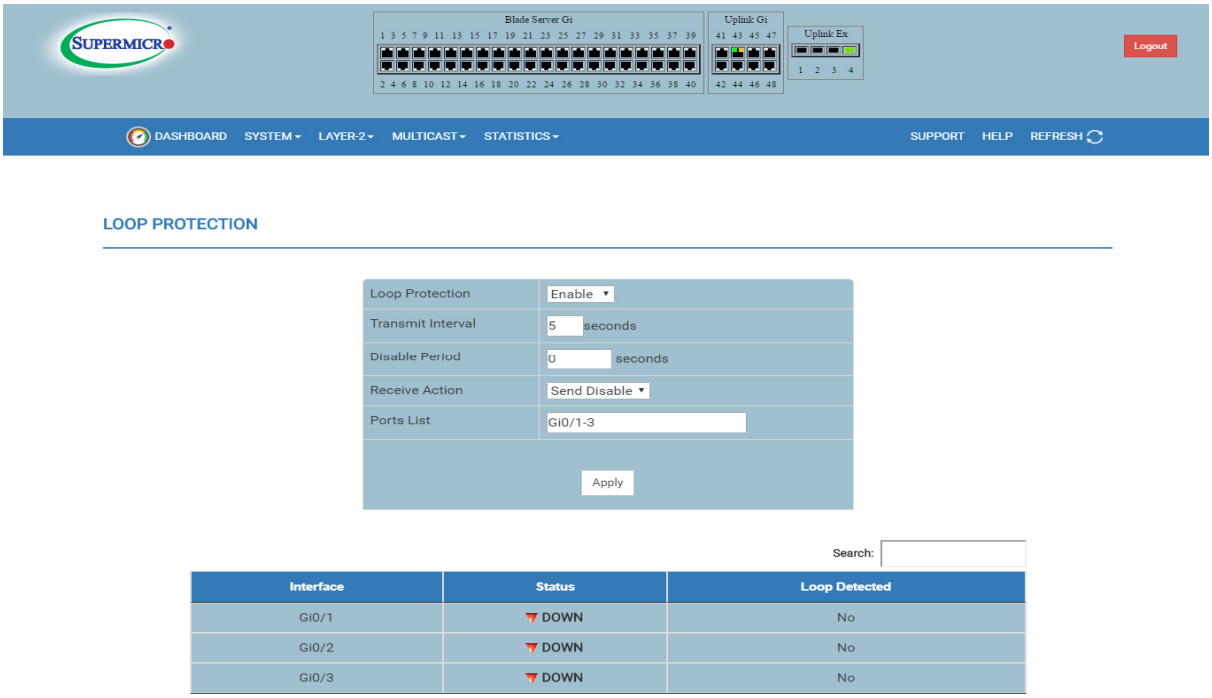


Fig: Loop Protect

4.5 VLAN

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

- Basic Settings
- Port Settings
- Static VLANs
- Protocol Group
- Port Protocol
- MAC Vlan
- WildCard

4.5.1 VLAN Basic Settings

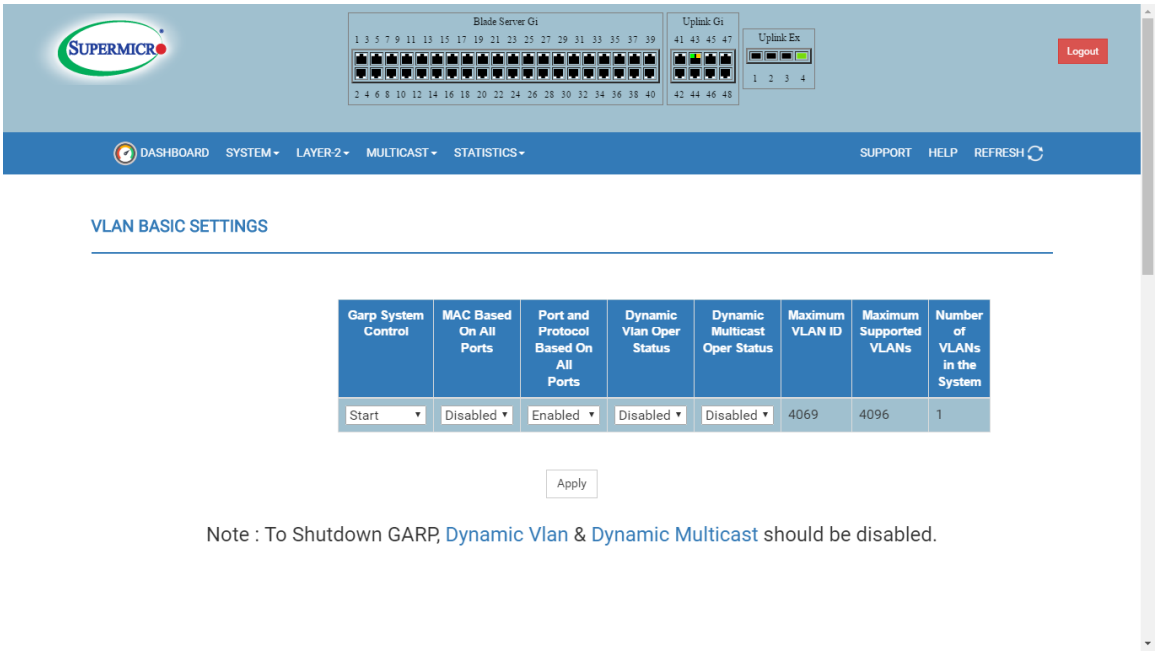


Fig : Basic Vlan settings

This page displays the following VLAN global configuration information:

Garp System Control – Starts or Shutsdown GARP in switch.

MAC Based on all Ports –User can enable/disable per-port MAC based classification.

Port and Protocol Based on all Ports - User can enable/disable per-port protocol based Classification, In addition, the Basic Settings page provides the configuration of Bridge Mode (Customer /Provider) and Priority for tunneled STP BPDUs. When user configure Bridge Mode to **Provider,** the Port Protocol based classification and MAC-based classification on all ports must be disabled.

Dynamic Vlan Oper Status – User can enable/disable vlan operational status.

Dynamic Multicast Oper Status - User can enable/disable multicast operational status.

Maximum VLAN ID– Displays the largest (4069) valid VLAN ID, which this switch can accept, above which all will be discarded.

Maximum supported VLANs – Displays the Maximum number of VLANs that this device can scale.

Number of VLANs in the system – Displays the active number of VLANs configured in the device.

.

4.5.2 Port Settings

The *Port Settings* link opens the **VLAN Port Settings** page, 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 frame type (accept tagged frame alone or all frames). The other configurations provided in this page are, enabling/disabling Port and Protocol based classification, enabling/disabling of tunneling and enabling/disabling of STP BPDU tunneling. To enable STP BPDU tunneling on an interface, enable tunneling on that interface. User can configure the Access Vlan, Trunk port allowed Vlans and Trunk Native Vlan.

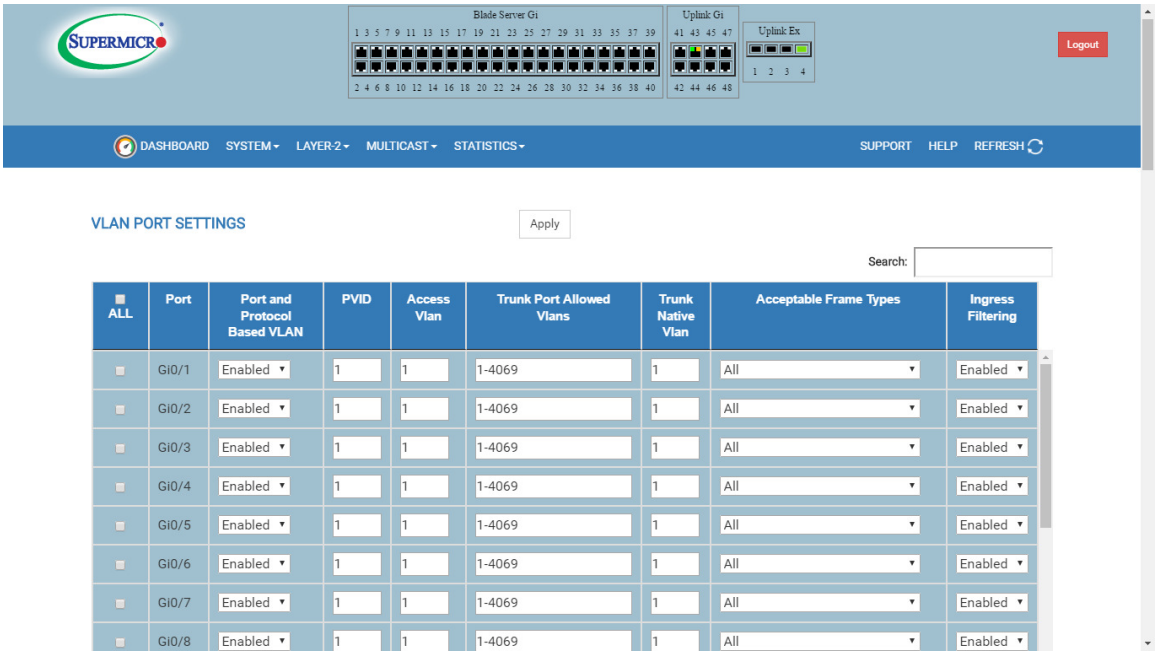


Fig: Port Settings

4.5.3 Static Vlan

The *Static VLANs* link opens the **Static VLAN Configuration** page, which allows you to configure the VLAN related information statically. Using the first table you will also be able to create new entries for uncreated VLANs. VLAN ID is the mandatory field in configuring a VLAN. There is also provision to enter VLAN Name, , Tagged Port, Untagged Port and the Forbidden Port for a VLAN. The second table displays the VLAN configurations saved in the switch.

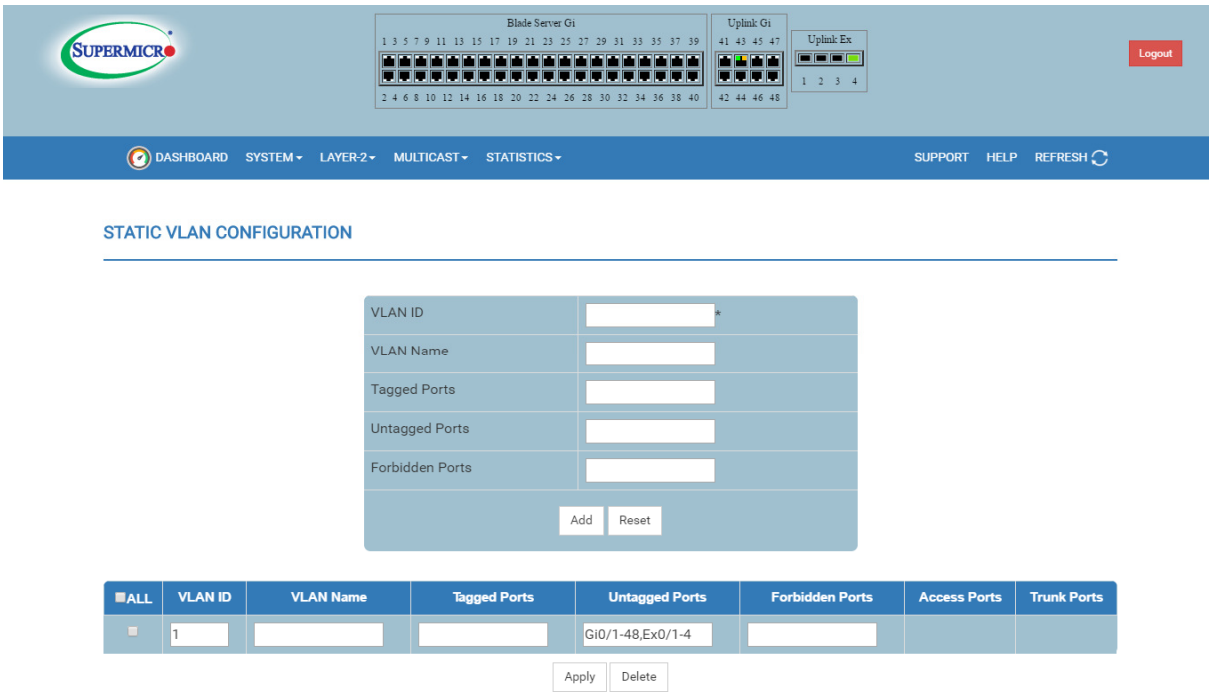


Fig: Static Vlan

4.5.4 Protocol Group

The *Protocol Group* link opens the **VLAN Protocol Group Settings** page. This table 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.

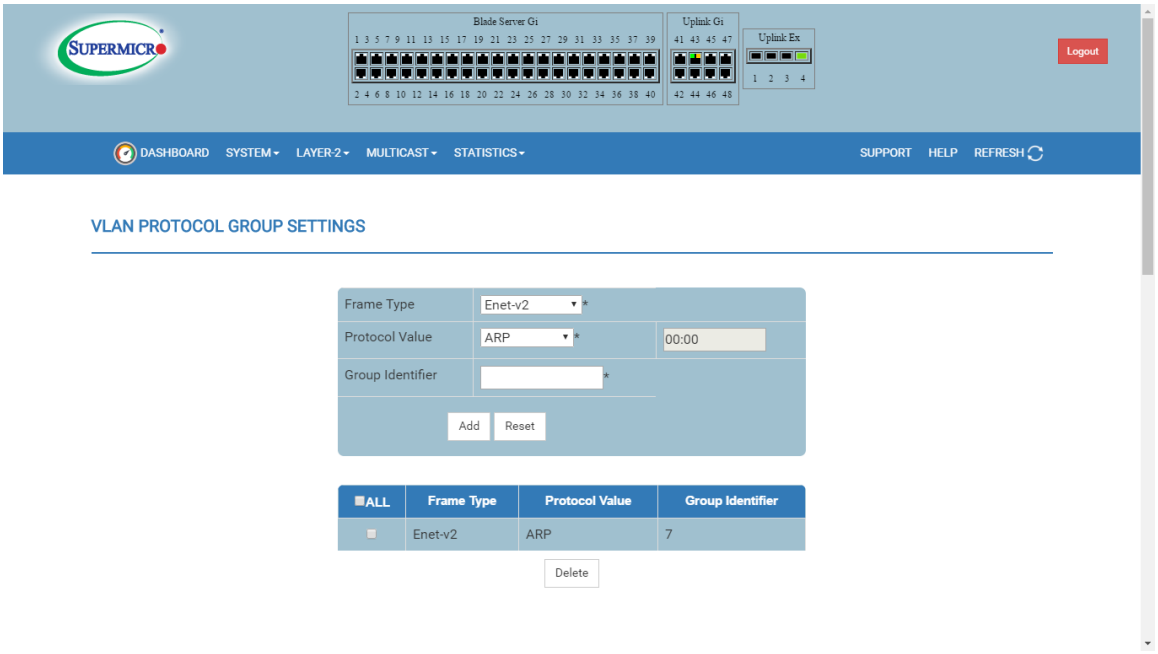


Fig: Vlan Protocol Group

4.5.5 Port Protocol

The *Port Protocol* link opens the **Port VLAN Protocol Settings** page. This table is 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.

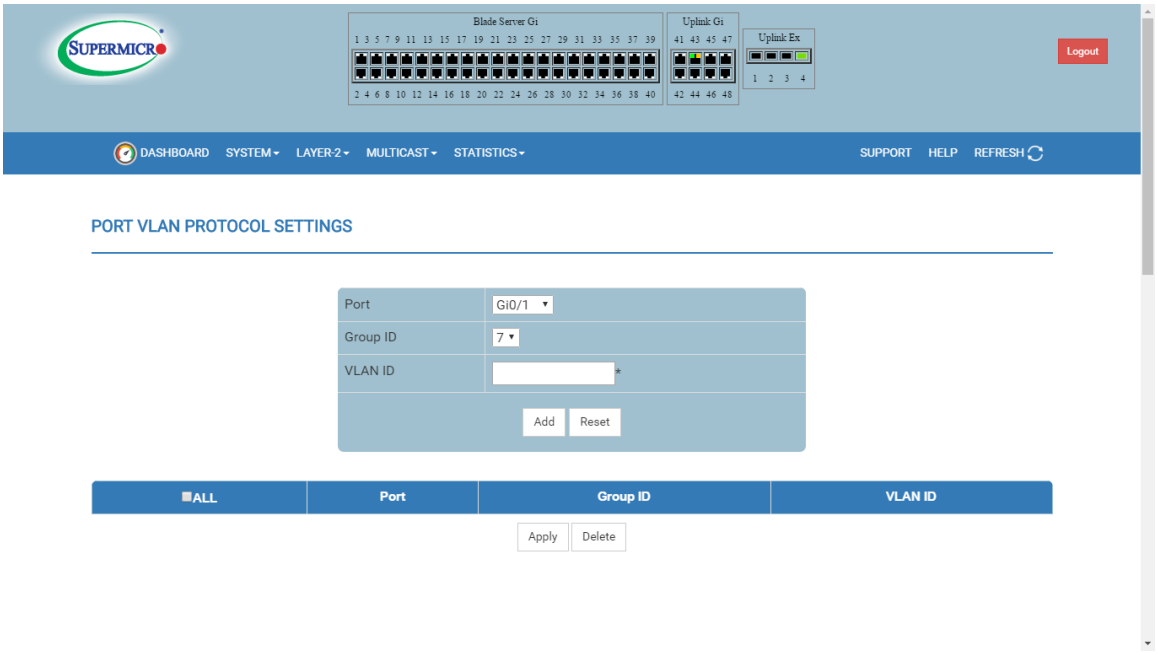


Fig: Port Protocol

4.5.6 MAC Vlan

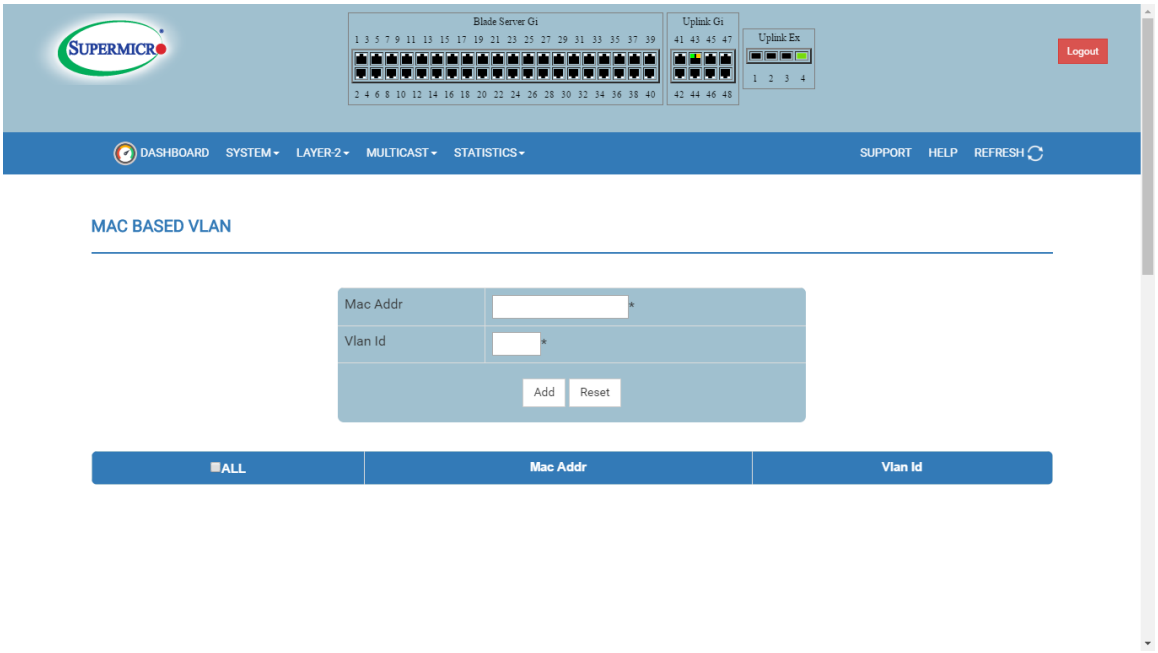


Fig: MAC Based VLAN

MAC VLAN page allows to configure the MAC based VLANs.

Mac Addr - Specifies the Port MAC address.

Vlan Id - VLAN identifier for this MAC based VLAN. The value ranges between 1 to 4069.

4.5.7 Wildcard

Wildcard Settings page helps configuring wildcard MAC addresses and ports for VLANs.

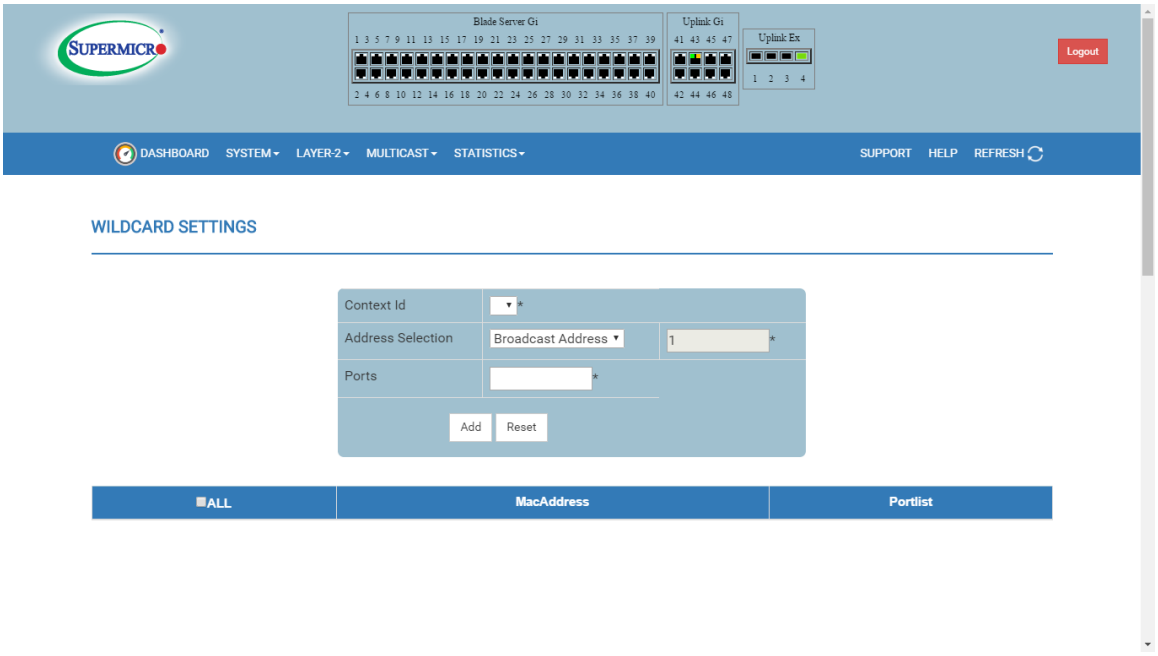


Fig: Wild card Settings

4.6 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.

- Basic Settings
- GVRP
- GARP Timers

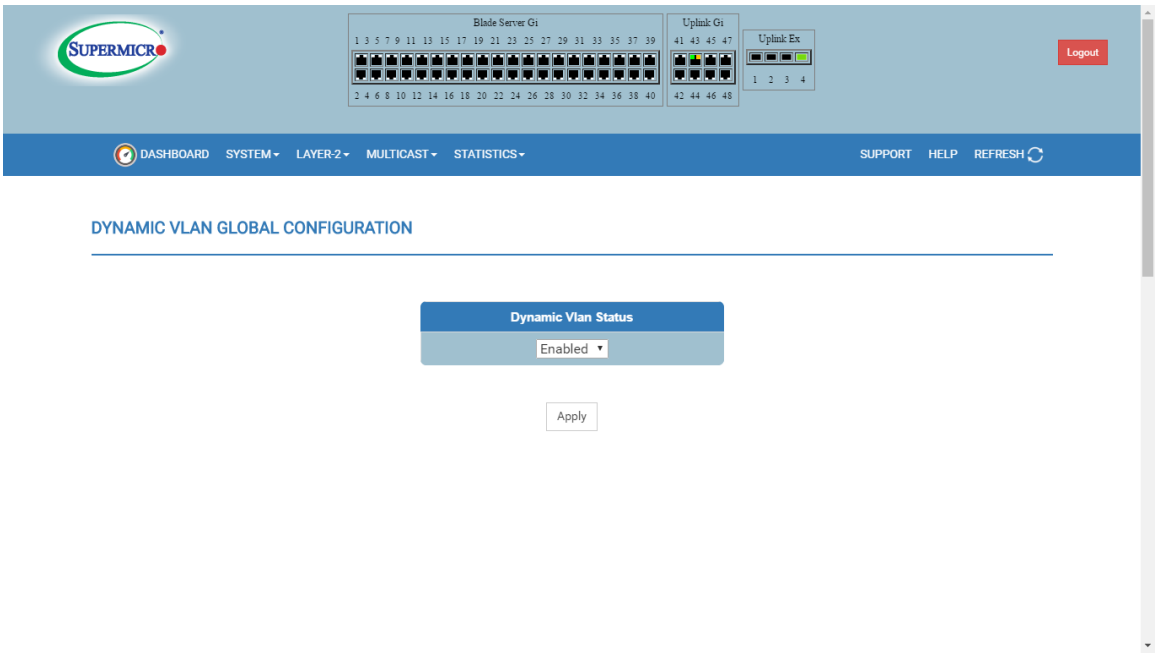


Fig: Dynamic Vlan

This page allows user to enable or disable Dynamic Vlan.

4.6.1 Port Configuration

The *Port Settings* link opens the **GVRP Configuration** page. You need to configure the following fields:

Port – Specifies the Interface index.

GVRP Status – Allows enabling / disabling GVRP Status in the switch.

Restricted VLAN Registration - Allows enabling / disabling of Restricted VLAN Registration.

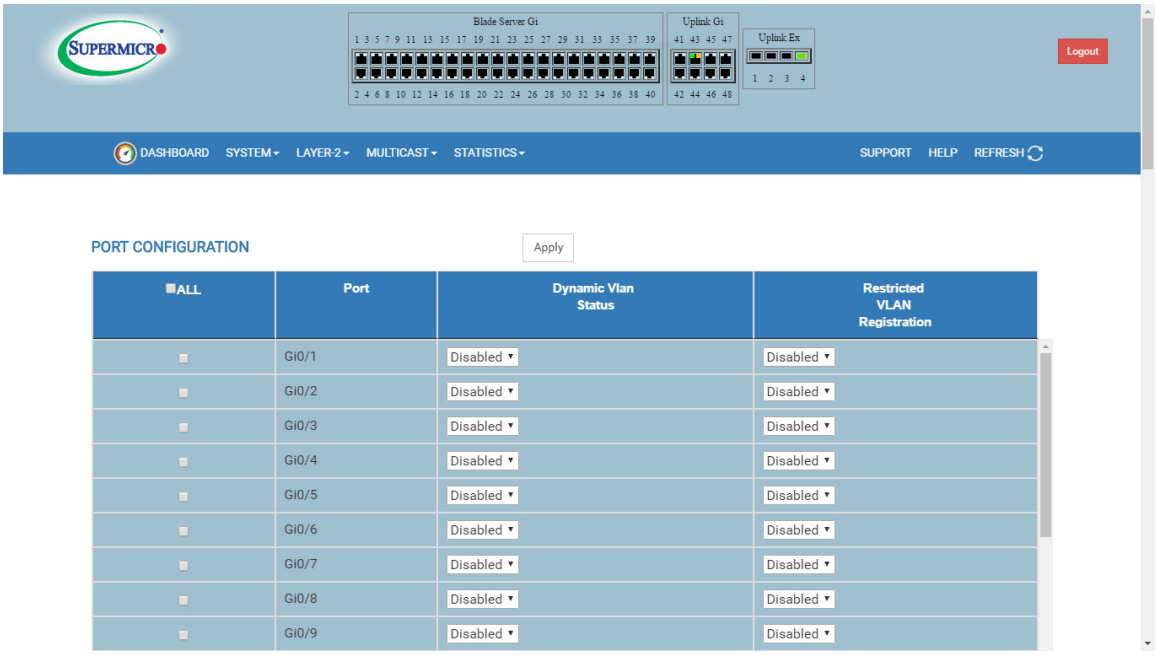


Fig: Dynamic Vlan Port Configuration

4.6.2 GARP Timers

Garp Timers Configuration page allows to configure the values for timers associated with GARP protocol for every port.

Port No - Port number

Garp Join Time - Configures GARP join time in milli seconds. The value ranges between 1 to 1073741810. The default value is 200 milli seconds.

Garp Leave Time - Configures GARP leave time in milli seconds. The value ranges between 1 to 2147483630.The default value is 600 milli seconds.

Garp LeaveAll Time - Configures GARP leave all time in milli seconds. The value ranges between 1 to 2147483640.The default value is 10000 milli seconds.

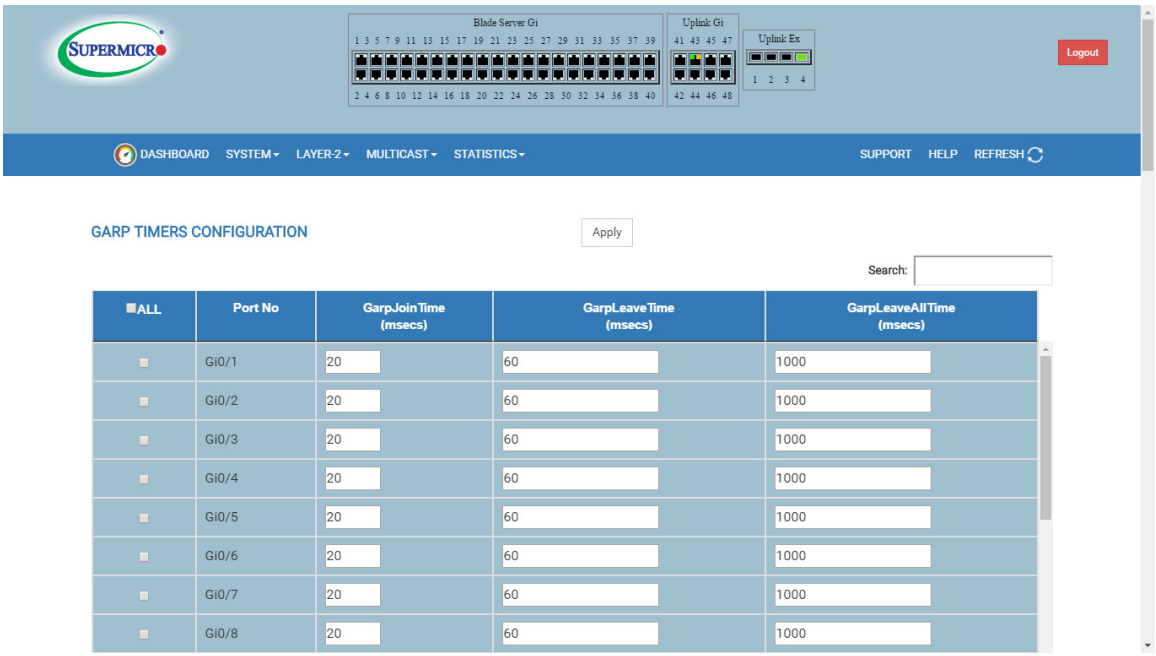


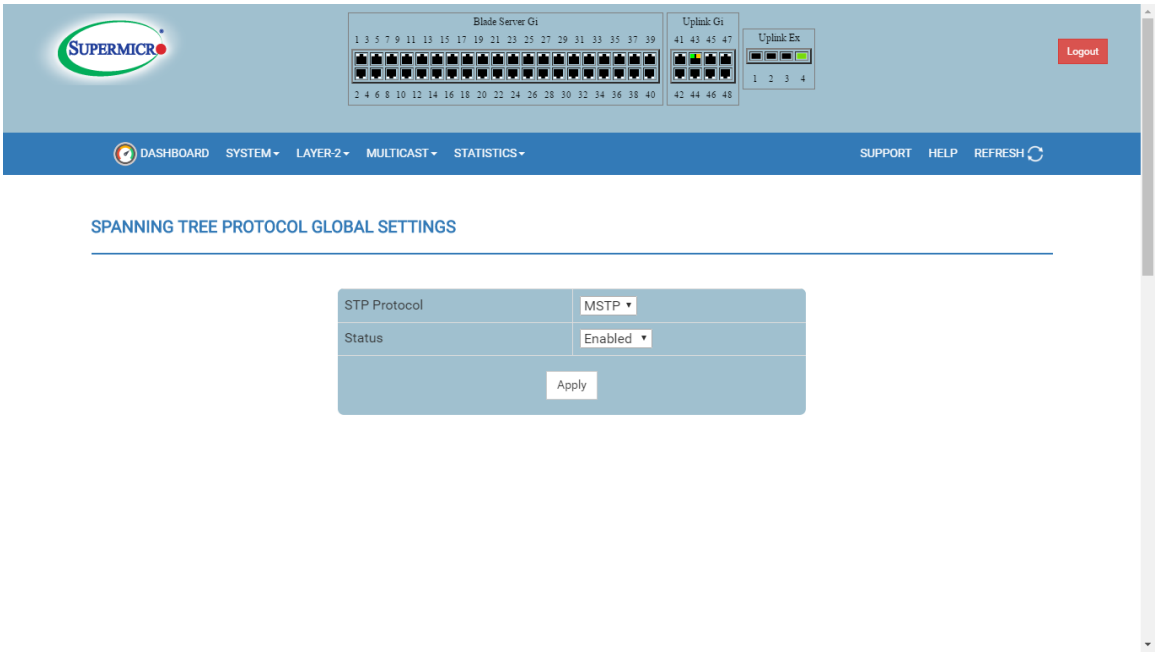
Fig: GARP Timers

4.7 Spanning Tree

Spanning Tree Protocol(STP) supports to configure RSTP or MSTP.

STP Protocol – User can modify the protocol RSTP or MSTP

Status – Enable or Disable the spanning tree protocol status.



The *RSTP* link provides links to the following configuration pages:

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

4.7.1 RSTP Global Settings

RSTP Global Configuration allows to configure RSTP global parameters.

Bridge Priority – Specifies the Priority value assigned to the bridge that is used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768

Path Cost Type – This allows user to configure the type 16 Bit or 32 Bit.

Protocol Version – This allows user to configure the version as RSTP or MSTP.

Dynamic Path Cost Calculation – Enable or disable dynamic path cost calculation.

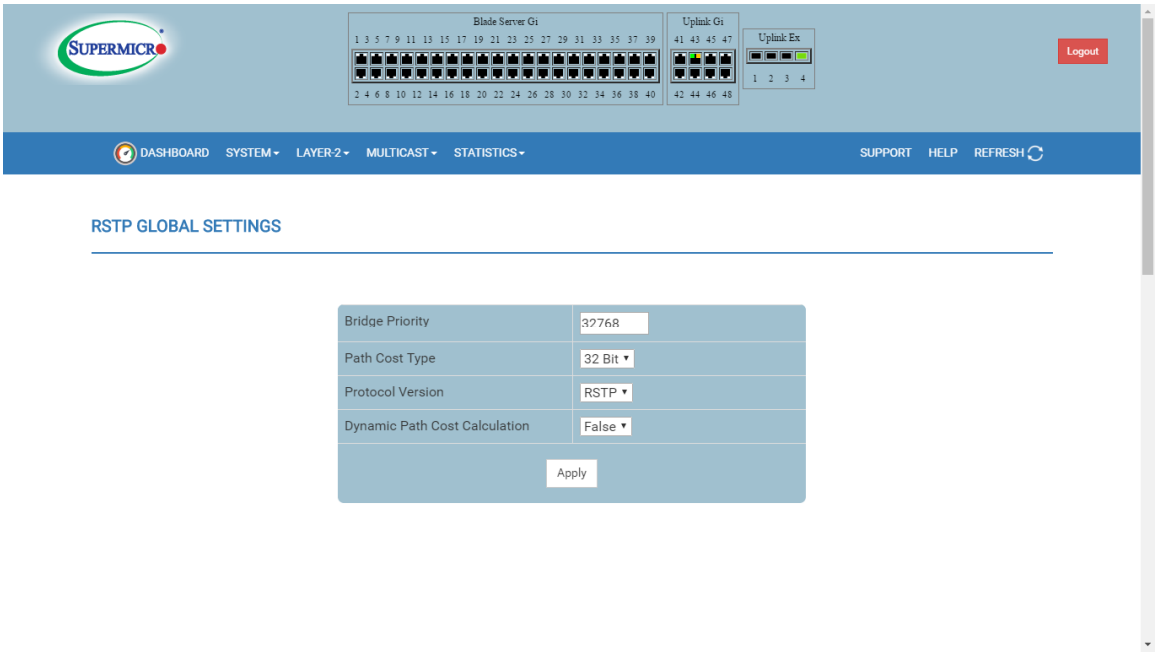


Fig: RSTP Global Settings

4.7.2 RSTP Basic Settings

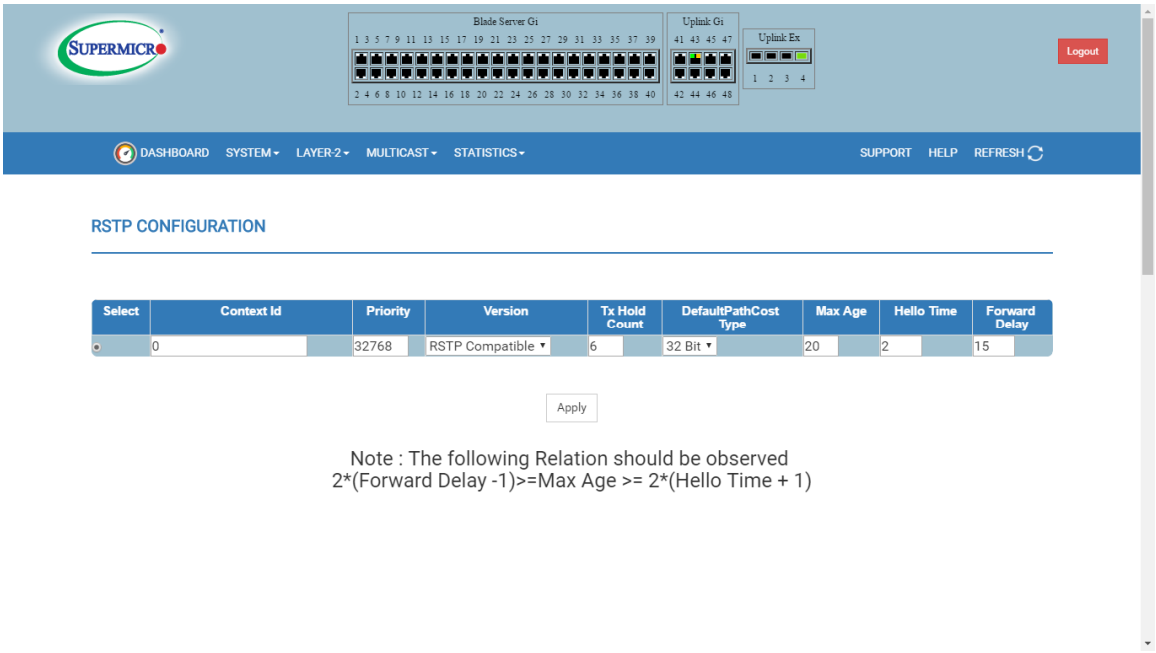


Fig: RSTP Basic Settings

The *Basic Settings* link opens the **RSTP Basic Settings** page.

This page includes the following fields:

Context Id - Specifies the context identifier***.***

Version - You can choose to run the protocol in RSTP or STP compatible version.

Priority – Specifies the Bridge priority, which can be used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768.

Transmit Hold Count – Specifies the maximum number of packets that can be sent in a given interval. This is configured to avoid flooding. Transmit hold count value may be from 1 to 10. The default value is 6.

Default Path Cost Type - 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.

Maximum Age (Seconds) – Specifies the time period for which the information received in the RSTP BDPU is valid. The max age values from 6 to 40 seconds. The default value is 20.

Hello Time - Specifies administrative value of hello time for the port. Hello time may be 1 or 2 seconds. The default value is 2.

Forward Delay (Seconds) - Specifies how fast a port changes its spanning state when moving towards the Forwarding state. Forwarding time values from 4 to 30 seconds. The default value is 15.

4.7.3 RSTP Port Settings

The *Port Settings* link opens the **RSTP Port Settings** page. The configuration per port related to RSTP can be done through this page. You are allowed to configure the following:

Port – Specifies the port identifier.

Port Role - Specifies the Port's Current Role, which can be enabled or disabled.

Port Priority – Specifies the port priority used in role selection. Port priority values from 0 to 240. The default priority value is 128.

RSTP Status – Specifies the RSTP protocol status that can be enabled/disabled on the particular port.

Path Cost – Specifies the path cost associated with this port. Port priority values from 0 to 200000000. The default path cost is calculated based on the port speed.

Protocol Migration - This is to control 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 - Edge port or non-edge port.

Admin Point-to-Point -You can configure ports explicitly as point-to-point (Force true), or Non-point-to-point or leave the decision to be made dynamically (from AL or MAC layer).

Auto Edge Detection - Enable or disable the automatically detection of auto edge.

Restricted Role – Specifies the Restricted role status of the port.

Restricted TCN – Indicates the Restricted TCN status of the port.

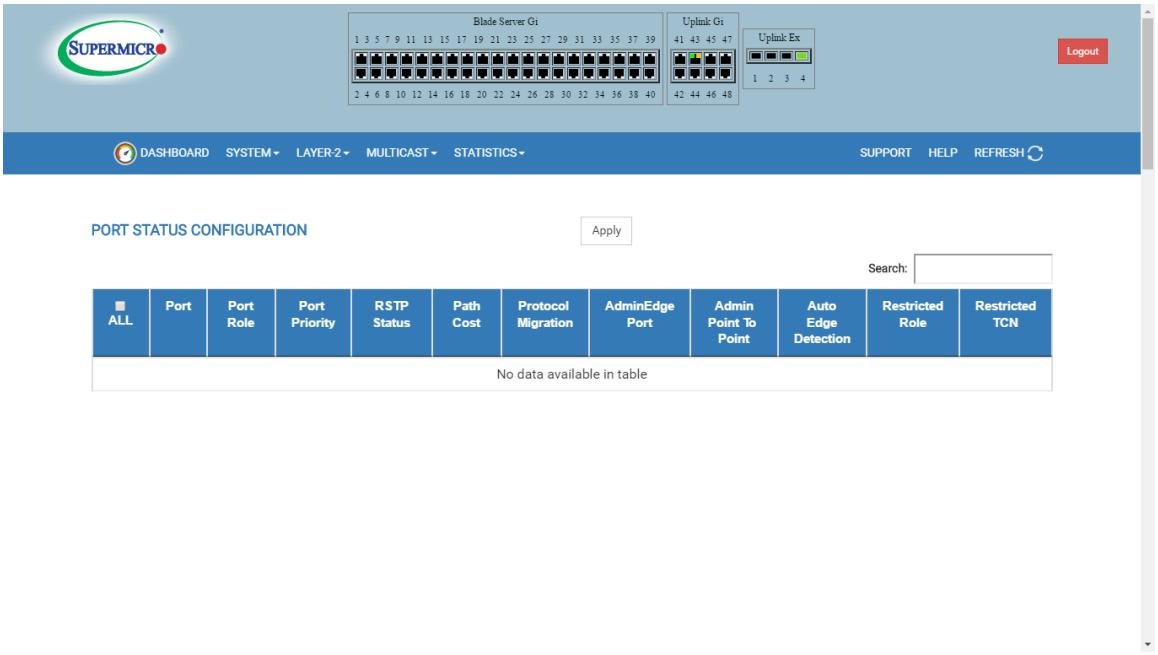


Fig: RSTP Port Settings

4.7.4 RSTP Port Status

The *Port Status* link opens the **RSTP Port Status** page.

This page displays RSTP port specific information. You need to configure the following:

Port – Port number.

Designated Root: Specifies the unique Bridge Identifier of the Bridge recorded as the Root for the segment to which the port is attached.

Designated Cost: Specifies the path cost of the Designated Port of the segment connected to this port.

Designated Bridge: Specifies the Bridge Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.

Designated Port: Specifies the Port Identifier of the port on the Designated Bridge for this port's segment.

Type: 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: Specifies the Port's Current Role as defined by Spanning Tree Protocol.

Port State: The port's current state as defined by application of the Spanning Tree Protocol.

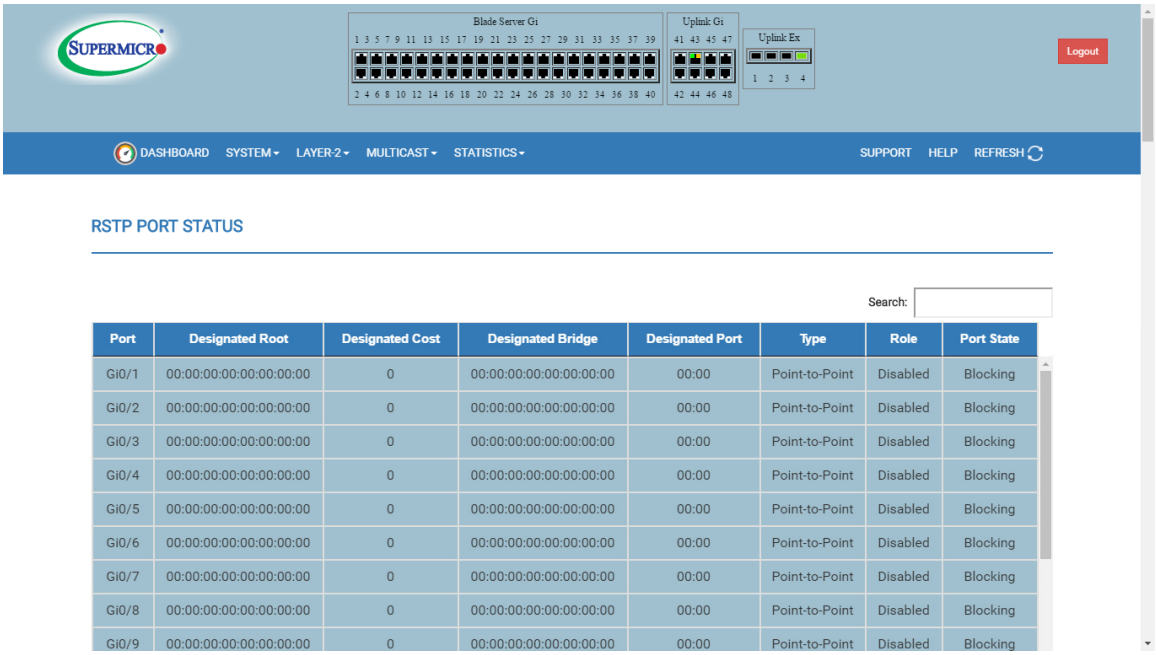


Fig: RSTP Port Status

MSTP:

The *MSTP* link leads you to the following configuration pages:

- Basic Settings
- Timers
- Port configuration
- VLAN Mapping
- Port Settings
- CIST Port Status

4.7.5 MSTP Basic Settings

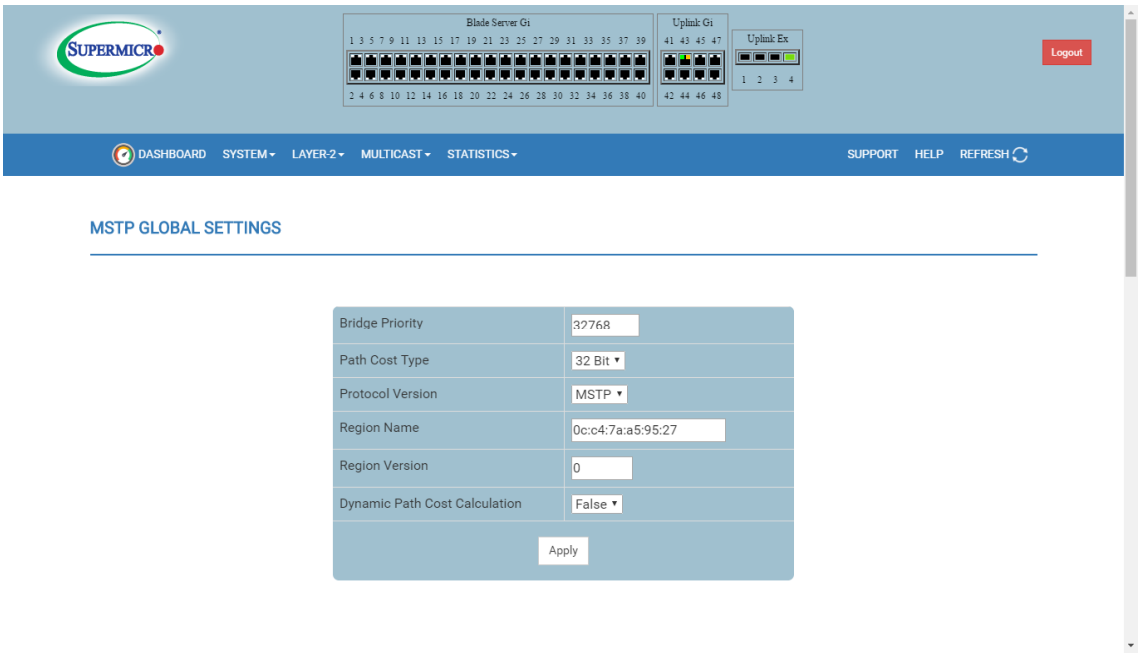


Fig: MSTP Basic settings

The *Basic Settings* link opens the **MSTP Basic Settings** page. The MSTP global configuration can be accessed through this page. You need to configure the following:

Bridge Priority – Specifies the Priority value assigned to the bridge that is used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768.

Path Cost Type – Specifies the type 16 Bit or 32 Bit.

Protocol Version – User can choose to run the protocol in RSTP or MSTP.

Region Name – Specifies the name for the Region's configuration. By default, the region name will be equal to the Bridge MAC Address.

Region Version – Specifies the version number of the configuration to be used. The allowed value ranges from 0 to 65535. The default priority value is 0.

Dynamic Path Cost Calculation – Enable or disable dynamic path cost calculation.

4.7.6 MSTP Timers

The timers are configurable for maximum hop count, forward delay, maximum age, transmit hold age and hello time.

Maximum Hop Count – MSTP uses a hop count to decide the validity of the BPDU messages. The root switch sends a BPDU with a hops count as the max hops. Every switch decrements the hops count while forwarding the BPDU. When this hops count reaches zero, the switch discards the BPDU message. The allowed value ranges from 6 to 40. The default value is 20.

Max Age – Switches maintain the BPDU information for every port for a maximum age period. If BPDU configuration messages are not received on any ports within the max age time, the switch will reconfigure those ports. The allowed value ranges from 6 to 40. The default value is 20.

Forward Delay – A switch will wait for the of forwarding time interval on listening and learning states before going to aforwarding state.The allowed value ranges from 4 to 30. The default value is 15.

Transmit Hold Count – Transmit hold count helps to control the BPDU burst traffic.The allowed value ranges from 1 to 10. The default value is 3.

Hello Time - The root switch periodically sends the BPDU messages on every port for every hello time interval. The allowed value is 1 or 2 seconds. The default value is 2 seconds.

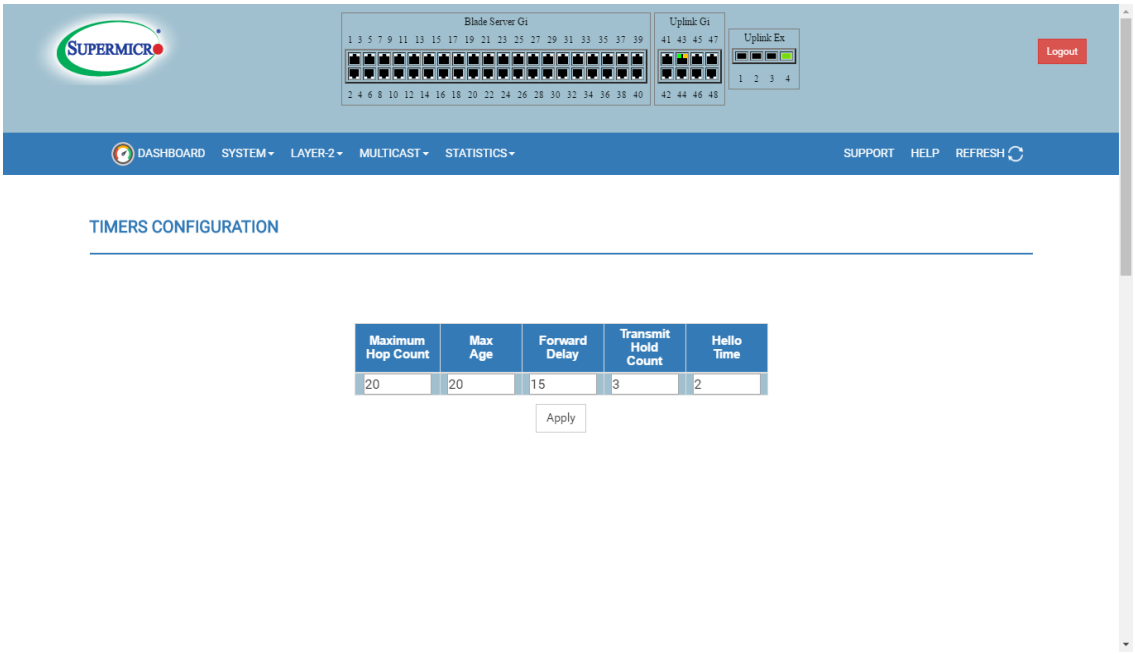


Fig: MSTP Timers

4.7.7 MSTP Port Configuration

The *CIST Settings* link opens the **CIST Settings** page. The configuration per Port related to MSTP can be done through this page. You are allowed to configure the following:

Port – Specifies the port identifier.

Path Cost – Specifies the path cost associated with this port. Path cost values from 0 to 200000000. The default path cost is calculated based on the port speed.

Priority – Specifies the port priority used in role selection. Port priority values from 0 to 240. The default priority value is 128.

Point-to-Point Status- User can configure the ports explicitly as point-to-point (Force true), or Non-point-to-point port or leave the decision to be made dynamically (from AL or MAC layer).

Edge Port - This must be configured, if the corresponding port is an edge port.

MSTP Status – Specifies the MSTP protocol status that can be enabled/disabled on the particular port.

Protocol Migration - This is to control the migration among MSTP, RSTP and STP protocols, if the other side of the switch runs a different mode. Migration takes place only if this is enabled.

Hello Time (Seconds) - Specifies administrative value of hello time for the port. Hello time may be 1 or 2 seconds. The default value is 2.

Auto Edge Status - If set to true, the edge port status will be dynamically calculated.

Restricted Role – Specifies the Restricted role status of the port.

Restricted TCN – Indicates the Restricted TCN status of the port.

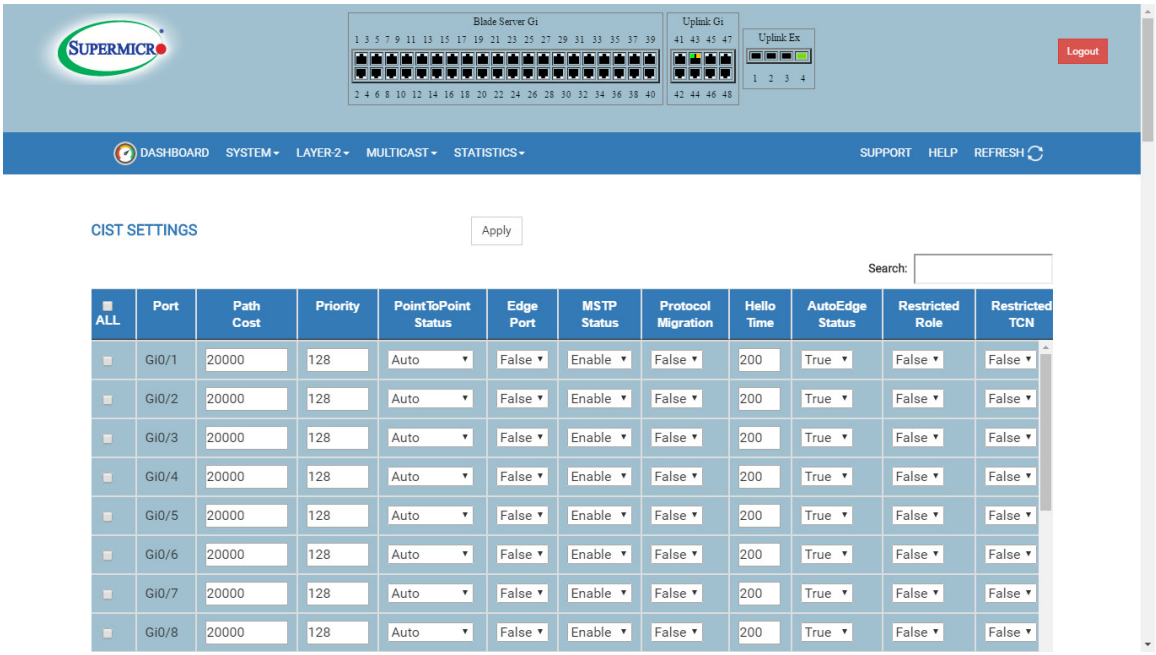


Fig: MSTP CIST settings

4.7.8 MSTP VLAN Mapping

The *VLAN Mapping* link opens the **VLAN Mapping** page. This table contains one entry for each instance of MSTP. You are allowed to configure the following:

MSTP Instance ID – Specifies the Instance ID, which is the index of the table. The allowed value ranges from 1 to 16.

Bridge Priority – Specifies the Priority value assigned to the bridge that is used to select the root bridge. The allowed value ranges from 0 to 61440. The default priority value is 32768

Add VLAN – Specifies the list of VLANs to be mapped to this instance of the spanning tree.

Delete VLAN – Specifies the list of VLANs to be unmapped from this instance of the spanning tree.

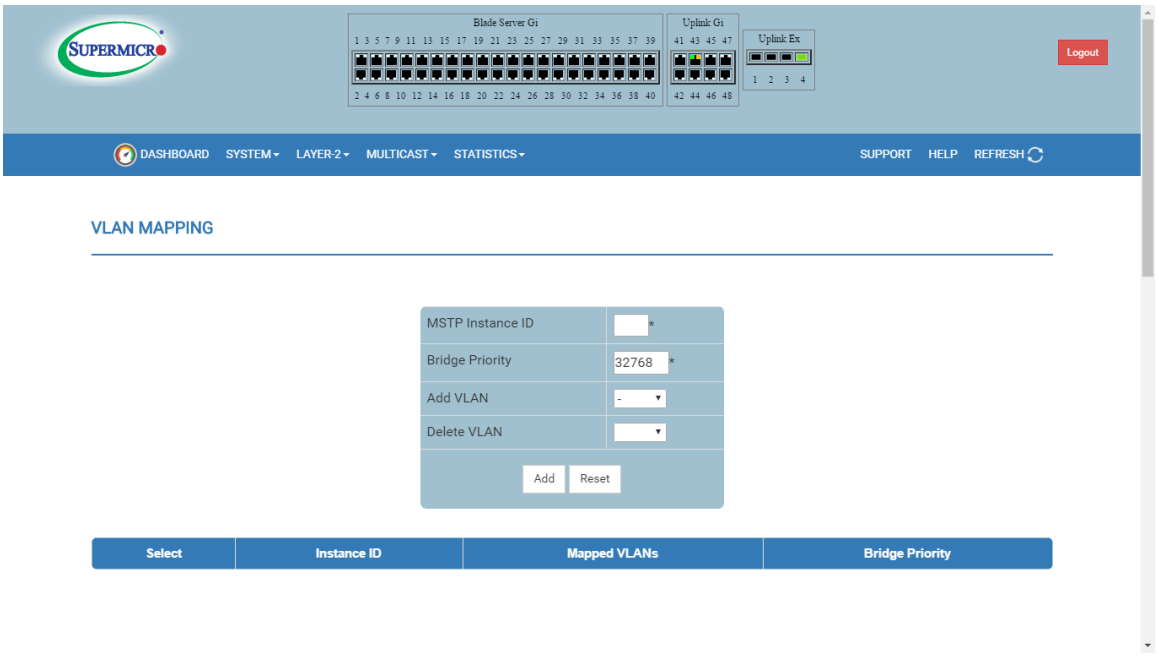


Fig: VLAN Mapping

4.7.9 MSTP Port Settings

The *Port Settings* link opens the **Port Settings** page. You are allowed to configure the following:

Port – Specifies the interface index of the port on which MSTP is being run.

MSTP Instance ID – Specifies the instance ID of the STP that is associated with this instance.

Port State – Specifies the current state of the port.

Priority – Specifies the priority related to this port.

Cost – Specifies the cost associated with this port, which will be added to the cost of any path that includes this port.

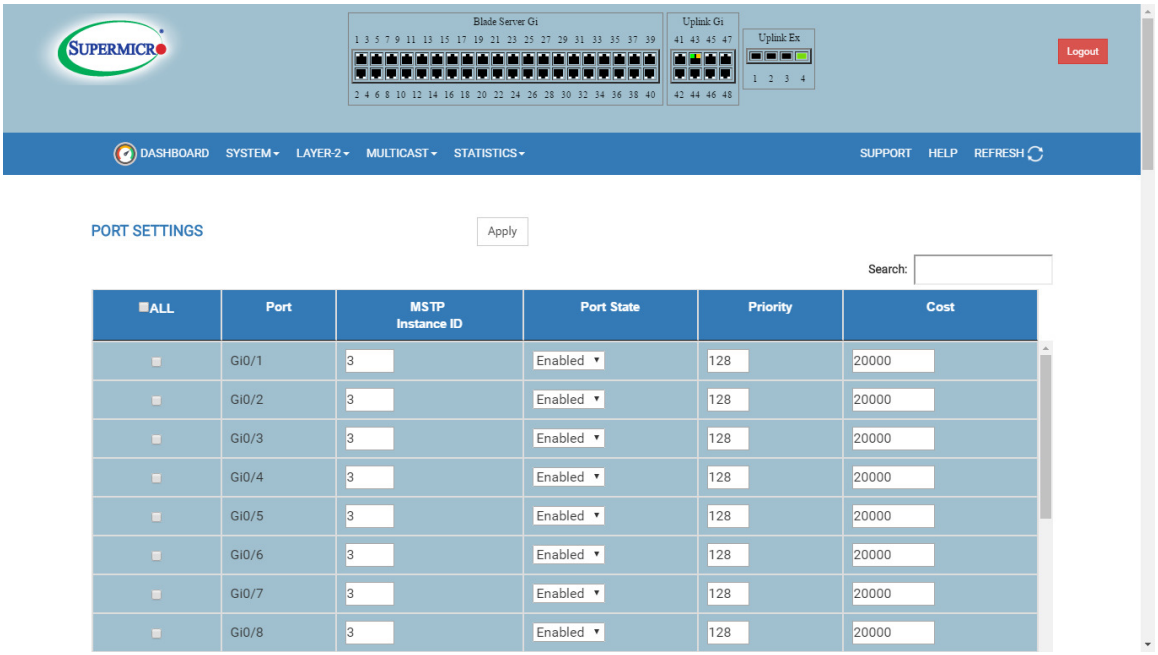


Fig: MSTP Port settings

4.7.10 MSTP CIST Port Status

The *CIST Port Status* link opens the **MSTP CIST Port Status** page. This page displays MSTP CIST port specific information. You need to configure the following:

Port – Port number.

Designated Root - Specifies the unique Bridge Identifier of the Bridge recorded as the Root for the segment to which the port is attached.

Root Priority - Specifies the priority related to this designated root.

Designated Bridge - Specifies the Bridge Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.

Designated Port - Specifies the Port Identifier of the port on the Designated Bridge for this port's segment.

Designated Cost - Specifies the path cost of the Designated Port of the segment connected to this port.

Regional Root - Specifies the unique Bridge Identifier of the bridge recorded as the CIST Regional Root Identifier in the configuration BPDUs transmitted.

Regional Root Priority - Specifies the priority related to this regional root.

Regional Path Cost - Specifies the contribution of this port to the path cost of paths towards the CIST Regional Root, which includes this port.

Type - 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 - Specifies the Ports Current Role as defined by Spanning Tree Protocol.

Port State - Specifies the port's current state as defined by application of the Spanning Tree Protocol.

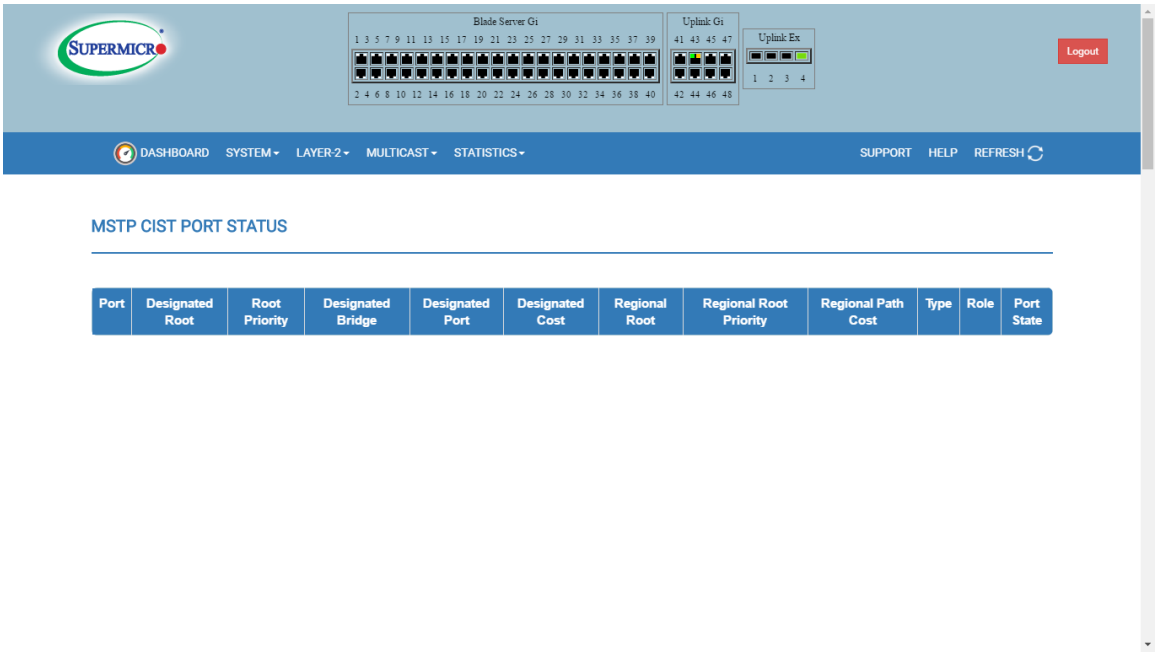


Fig: MSTP CIST Port Status

4.8 LA

The *LA* link provides links to the following configuration pages:

- Basic Settings
- Interface settings
- Port Settings
- MLAG Configuration

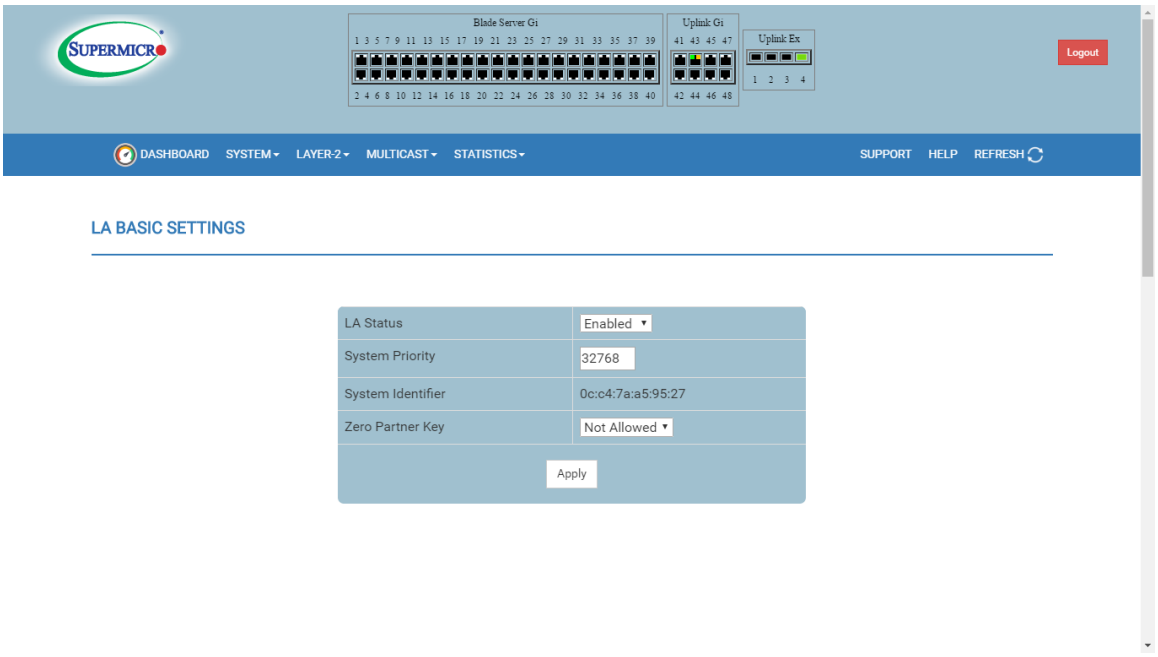


Fig: LA Basic Settings

The *Basic Settings* link opens the **LA Basic Settings** page. The following parameters are configured through this page:

LA Status - This is used to enable/disable LA in the switch.

System Priority – Specifies the priority value associated with the Actor's system ID. The allowed value ranges from 0 to 65535. The default value is 32768.

System ID – Specifies the Bridge MAC Address that is displayed. This is a read-only parameter.

Zero Partner Key - This is used to choose the partner key as Allowed or Not Allowed.

4.8.1 Interface Settings

Port Channel Interface Basic Settings page allows to configure port channels.

Port Channel ID - Specifies the identifier of the port channel interface. The valid values are between 1 to 65535.

Port List – Displays the port list.

No of ports – Displays the number of ports configured in LA.

Admin State – Displays administratively make port channel Up or Down.

Oper State – Displays operational status for port, Up or Down.

MLAG Status - This is used to enable or disable MLAG status for port channel. This filed is available in MLAG supported switch model.

Strom Control :

Below fields are under Storm Control:

- **DLF level pps** - User can specify Destination lookup failure(DLF) limit in packets per second..
- **Broadcast level pps** - User can specify Broadcast limit in packets per second.
- **Multicast level pps** - User can specify Multicast limit in packets per second.

MTU – MTU value for this port channel. The allowed values from 1500 to 9216. The defaul value is 1500.

Switch port mode – Specifies the switch port mode, Access or Trunk or Hybrid for port channel.

Load balancing – User can either choose to Source MAC Address Based or Destination MAC Address Based or Source and Destination MAC Address Based or Source IP Address Based or Destination IP Address Based or Source and Destination IP Address Based.

Description – Specifies interface description string for this port channel.

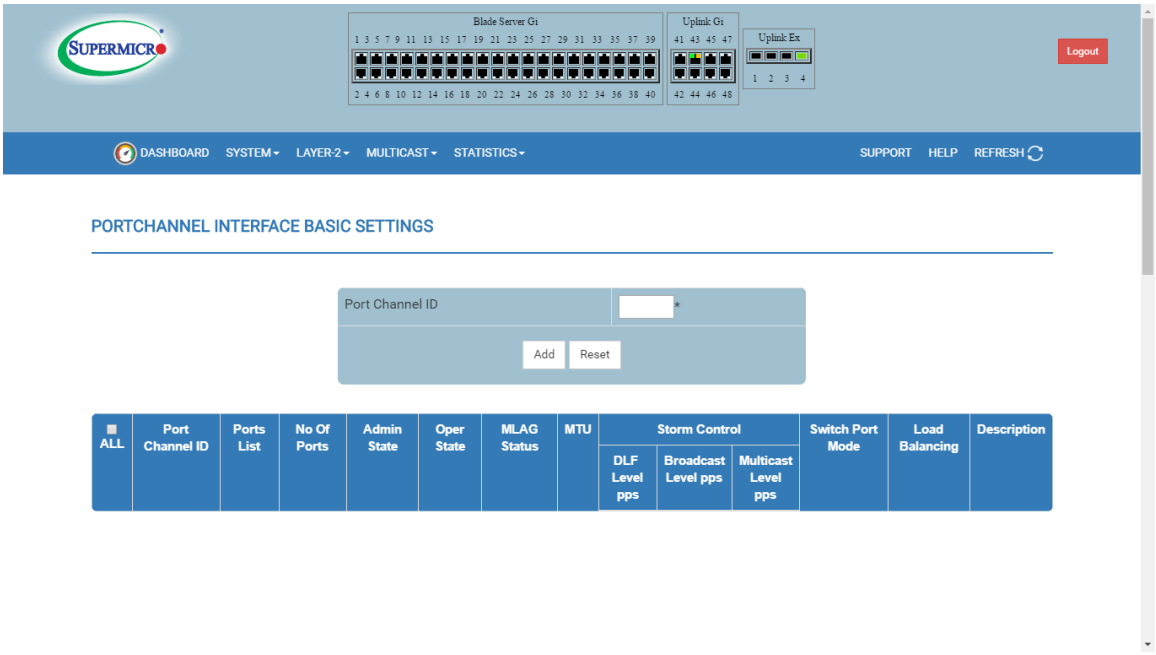


Fig: Interface Settings

4.8.2 Port Settings

The *Port Settings* link opens the **LA Port Settings** page. You can configure the following LA properties at per-port level in this page:

Port - Specifies the Interface Index.

Port Channel – Specifies the port Channel, Configured or Not Configured.

Mode - Specifies the various Port Modes, such as, On , Active or Passive .

Port Priority - Specifies the Priority value of the Port. The allowed values are from 0 to 65535. The default is 128.

Timeout – Sets the time within which LACP PDUs must be received on a port to avoid timing out of the Aggregated Link. If “long” timeout is chosen then the ports will time out of the Port Channel in 90 seconds. If “short” timeout is chosen then the ports will time out of the Port Channel in 3 seconds.

Wait Time– Configures the waiting time for a port after receiving Partner information and before entering aggregation. The allowed values are from 0 to 10. The default value is 2.

Port State - Indicates the current state of the port with respect to Link Aggregation. The possible states are

- Up in Bundle - The Port is an active member of the Port Channel.
- Up Individual - The Port is not a member of any Port Channel but its Oper-Status is Up.
- Standby - The Port is a member of the Port Channel but is currently in standby state.
- Down - The Ports Oper-Status is Down.

Aggregation State – Specifies the state whether static or dynamic.

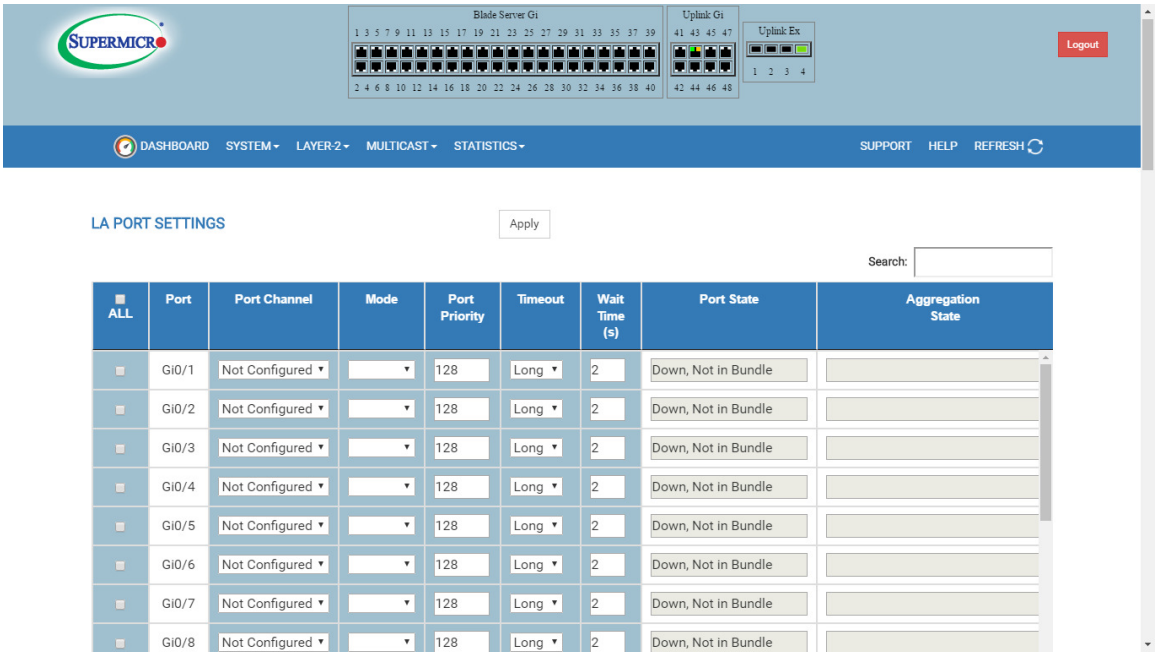


Fig: LA Port Settings

4.8.3 MLAG Configuration

The MLAG Configuration page allows to configure following parameters:

System Identifier – Specifies the system ID in MAC Address format.

System Priority – Specifies the priority value associated with the Actor's system ID. The allowed value ranges from 0 to 65535. The default value is 32768.

Keep Alive Time - Specifies the keep alive time in seconds. The allowed value ranges from 3 to 90. Default value is 3.

IPL Interface - Specifies the configured Port Channel number for IPL.

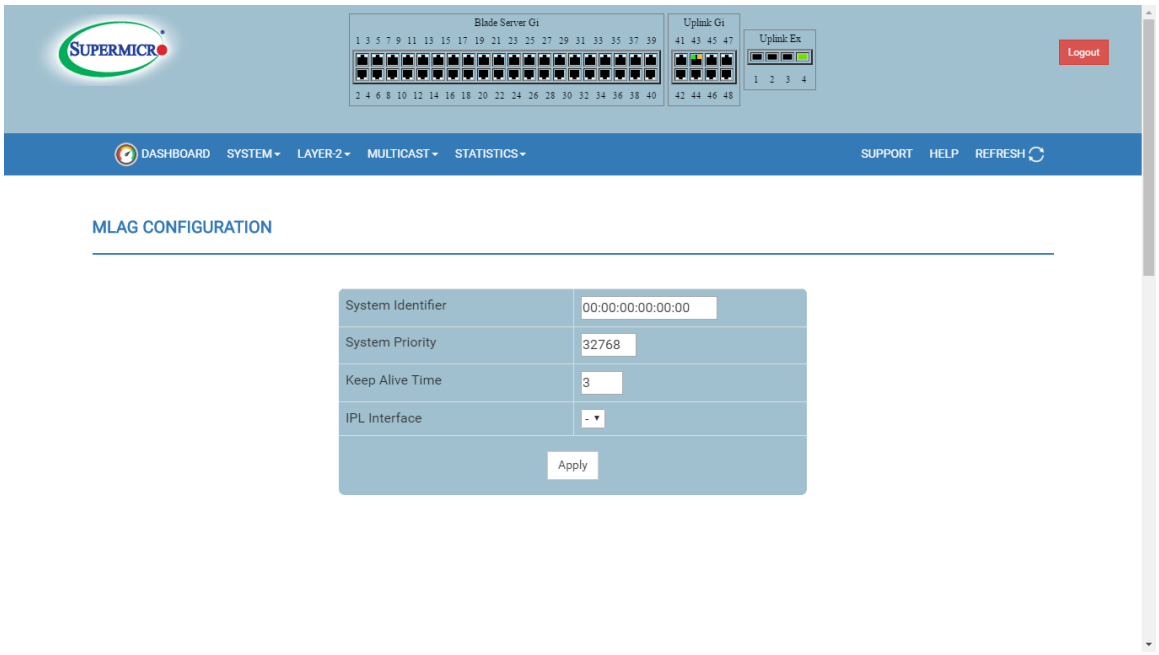


Fig: MLAG Configuration

4.9 LLDP

The LLDP link has the following configuration pages:

- Global Settings
- Interface Settings

4.9.1 Global settings

This page helps user to configure the LLDP global parameters.

LLDP Status – Enable or disable the LLDP status.

Transmit Interval – Specifies the transmission frequency of LLDP updates in seconds. The allowed values are from 5 to 32768. The default is 30 seconds..

Holdtime Multiplier - Specifies the multiplier value (value which is used to calculate the Time-To-Live for the LLDP advertisements). The allowed values are from 2 to 10. The default value is 4.

Reinitialization Delay – Specifies the re-initialization delay (delay time taken by LLDP to re-initialize on any interface). The allowed values are from 1 to 10. The default is 2 seconds.

Transmit Delay - Specifies the transmit delay (minimum amount of delay between successive LLDP frame transmissions). The allowed values are from 1 to 8192. The default is 2 seconds

Notification Interval - Specifies the notification interval (interval at which LLDP notifications are sent to NMS). The allowed values are from 5 to 3600. The default is 5 seconds.

Chassis-id Subtype – User can either choose chassis-id subtype as Chassis component or Port component or MAC address or Network address or Interface name or Locally assigned.

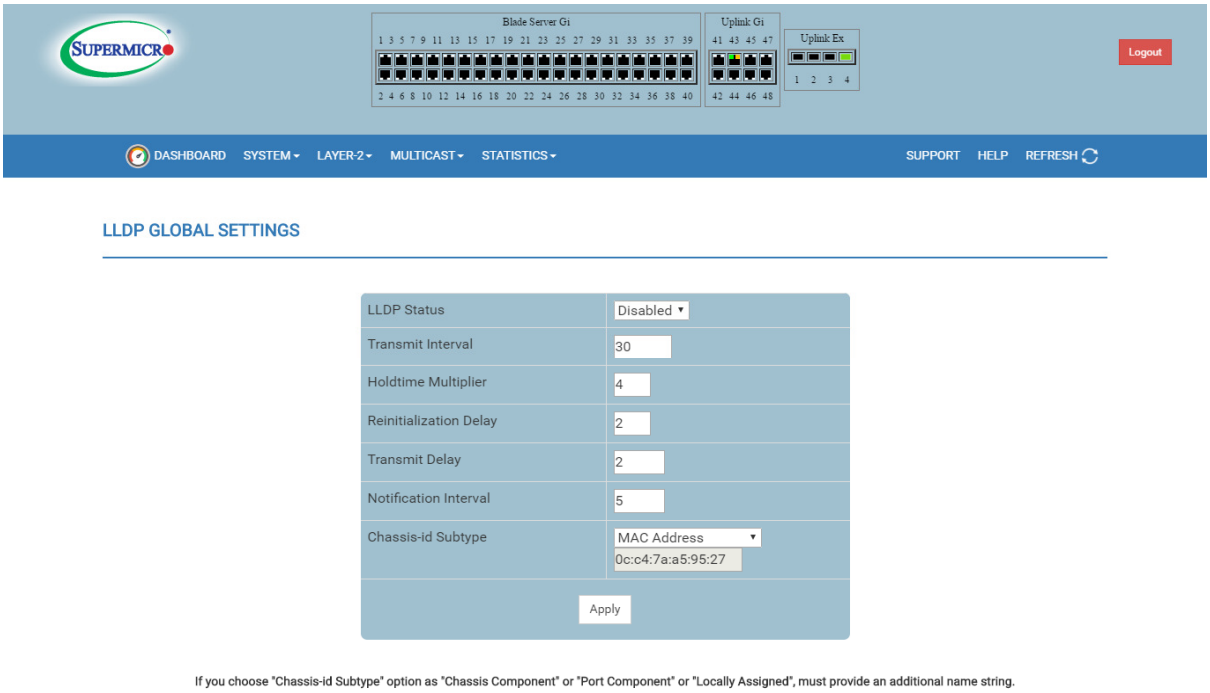


Fig: LLDP Global Settings

4.9.2 Interface Settings

This page helps user to configure the LLDP interface information. User can configure the following:

Port – Port number

Tx/Rx – This helps to configure either Transmit and Receive(Tx+Rx) or Transmit(Tx) or Receive (Rx) or none.

Notification – This helps to configure either Disabled or Remote change or Mis config or both.

Port Id Subtype – This helps either to choose PortId subtype as Interface alias or Port component or MAC address or Interface name or Locally assigned.

Below fields are under **Basis TLV**.

Port – Specifies the port “yes” or “none”.

SysName – Specifies the system name “yes” or “none”.

SysDesc – Specifies the system description “yes” or “none”.

SysCapab – Specifies the system capability “yes” or “none”.

MgmtAddr – Specifies the management address “All” or “IPV4”.

Below fields are under **Dot1 TLV VLAN**.

Port – Specifies the port “yes” or “none”.

Protocol – Specifies the protocol All or Vlan Id.

Name – Specifies the name All or Vlan Id.

Below fields are under **Dot3 TLV**.

MAC Phy – Specifies the MAC “yes” or “none”.

Link Agg – Specifies the link aggregation “yes” or “none”.

Max Frame – Specifies the maximum frame “yes” or ‘none”.

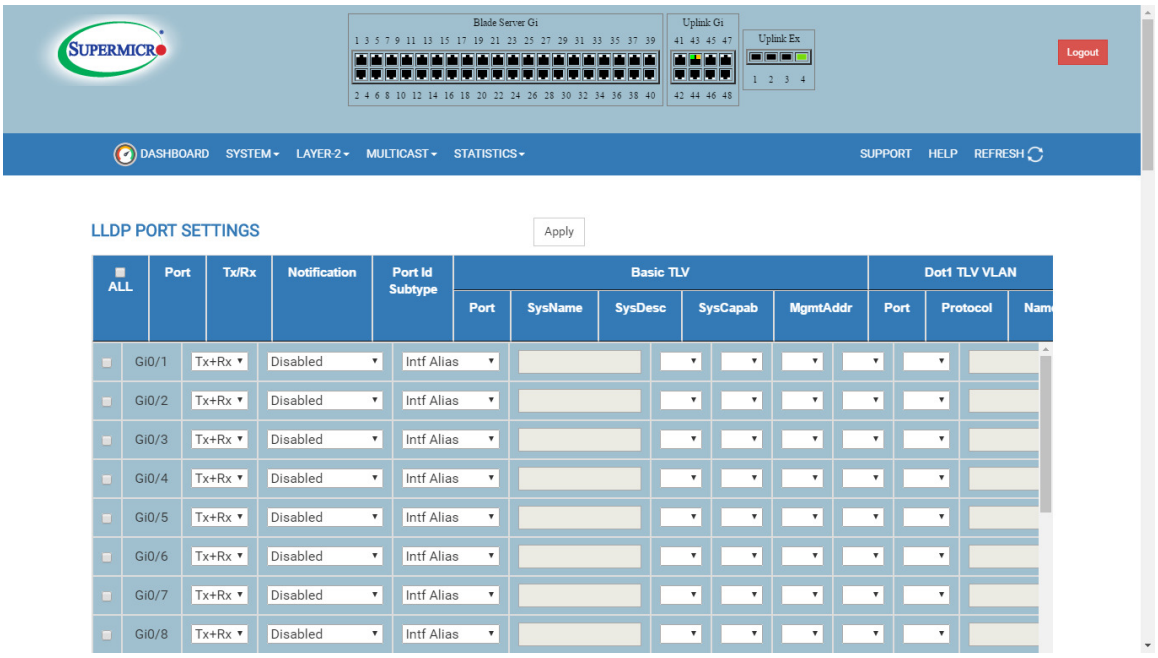


Fig: LLDP Port Settings

4.10 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

4.10.1 Unicast Filters

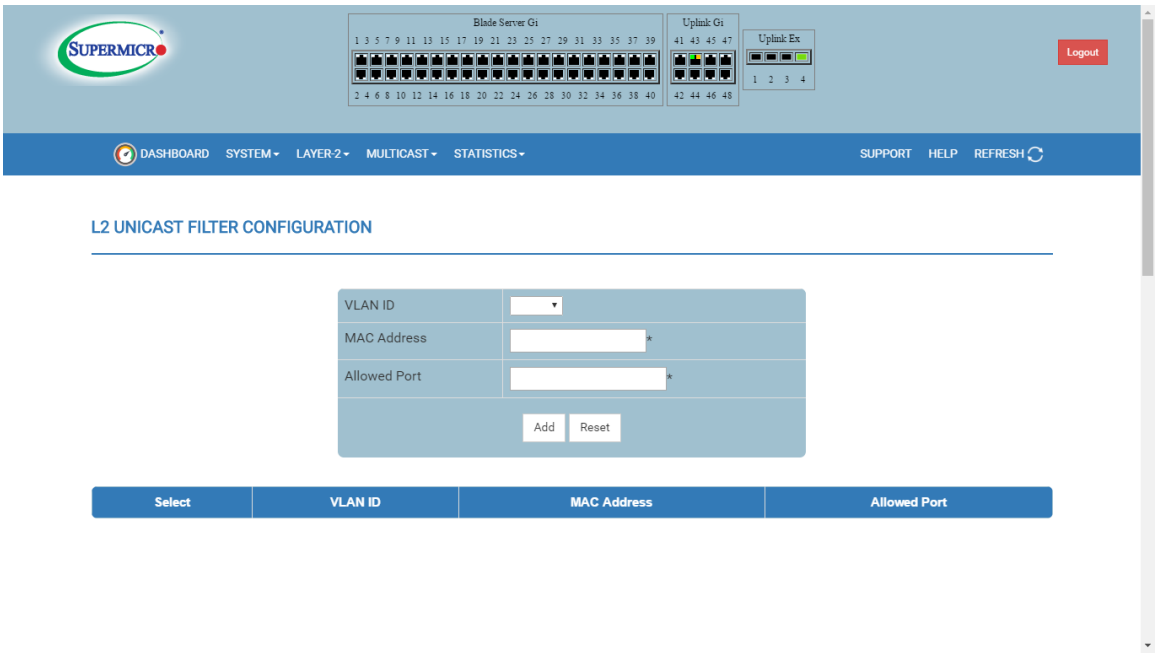


Fig: Unicast Filter

The *Unicast Filters* link opens the **L2 Unicast Filter Configuration** page. Using this page, you can set the filter configuration to control the unicast packets that the switch needs to process. Following are the fields that need to be configured:

VLAN ID – Specifies the Vlan Identifier .

MAC Address – Specifies the destination MAC address of the received packet.

Allowed Ports – Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) can be forwarded.

4.10.2 Multicast Filters

The *Multicast Filters* link opens the **L2 Multicast Filter Configuration** page.

This page allows you to set the filter configuration to control the multicast packets that the switch needs to process. Following are the fields that needs to be configured:

VLAN ID – Specifies the VLAN ID.

MAC Address – Specifies the destination MAC address of the received packet.

Allowed Ports – Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) can be forwarded.

Forbidden Ports – Specifies the list of ports on which the received packet (with the above set MAC address and if received from the configured port) must NOT be forwarded.

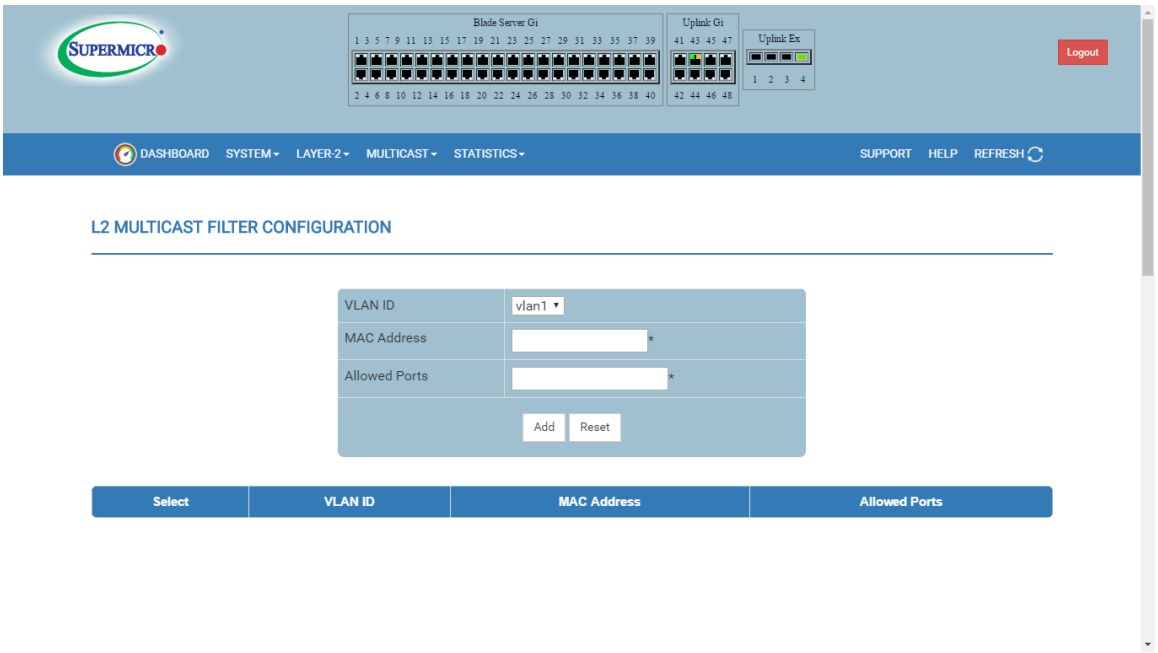


Fig: Multicast filter

5 Multicast

Multicast menu has links to multicast features.

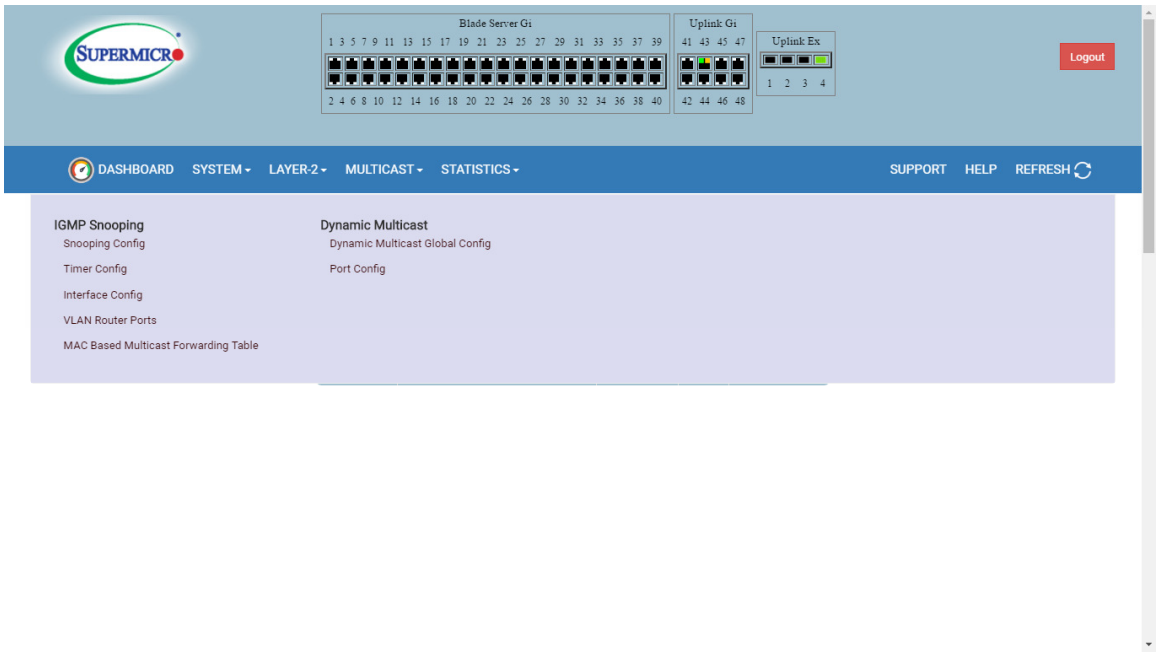


Fig: Multicast

5.1 IGMP Snooping

5.1.1 IGMP Snooping Configuration

IGMP Snooping Configuration page helps configuring the following IGMP snooping parameters.

System Control - Starts/Shutsdown IGS in switch.

IGMP Snooping Status - Enables / disables IGMP snooping globally in the switch. To enable IGS, GMRP status must be disabled.

Operational Status - Enables / disables IGMP snooping operationally in the switch. To enable IGS, GMRP status must be disabled.

Proxy Reporting - Indicates whether the proxy reporting in the IGMP snooping switch is to be enabled / disabled.

Report Forwarding - Specifies whether the IGMP reports are forwarded on all ports or only on router ports.

Retry Count - Specifies the maximum number of group specific queries sent on a port on reception of an IGMPv2 leave message. The allowed ranges from 1 to 5. The default value is 2.

Query Transmit On TC - Enable or disable query transmit when topology changes.

Multicast Filtering - Enable or disable the multicast filtering.

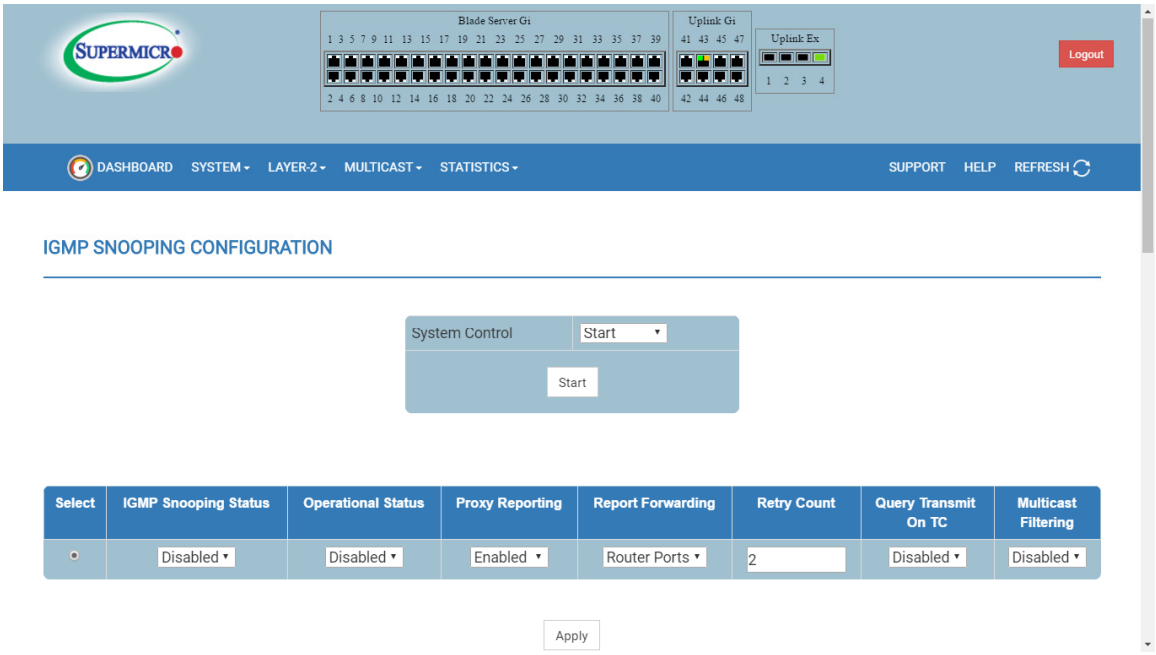


Fig: IGMP Snooping

5.1.2 IGMP Snooping Timer

IGMP Snooping Timer Configuration page helps configuring the following IGMP snooping timers.

Router Port PurgeInterval (Secs) - Specifies the interval for which the learnt router port will be purged. The allowed value range from 60 to 600.The default value is 125 seconds.

Group-Member Port Purge Interval (Secs) - Specifies the interval after which a port gets deleted, if IGMP reports are not received on a port. The allowed value ranges from 130 to1225. The default value is 260 seconds.

Report Forward Interval (Secs) - Specifies the interval within which the next report messages for the same multicast group will not be forwarded. The value ranges between 1 to 25.The default value is 5 seconds.

Group Query Interval (Secs) - Specifies the interval within which the switch sends a group specific query on a port when an IGMPv2 leave message is received. The value ranges between 1 to 5. The default value is 2 seconds.

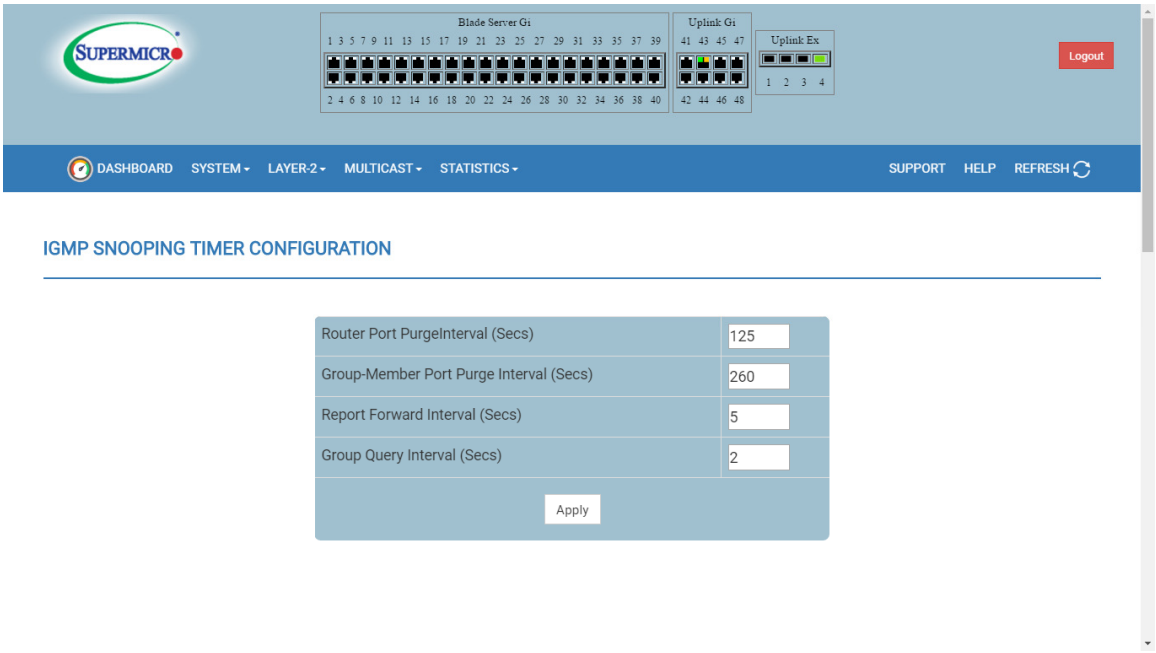


Fig : IGMP Snooping Timer Configuration

5.1.3 IGMP Snooping Interface

IGMP Snooping Interface Configuration page helps configuring the following IGMP snooping interface specific parameters.

VLAN ID - Specifies the VLAN ID for which the configuration is to be performed.

IGMP Snooping Status - Specifies the status of IGMP snooping in the Switch, which can be enabled / disabled for a specific VLAN.

Operating Version - Specifies the operating version of the IGMP snooping switch for a specific VLAN, is to be version 1 or version 2 or version3

Fast Leave - Indicates whether the fast leave processing for a specific VLAN, is to be enabled/disabled.

Querier Status - Specifies whether the IGMP snooping switch is enabled / disabled as a querier for a specific VLAN.

Querier Interval(secs) - Specifies the time period for which general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN. The value ranges between 60 to 600.

Router Port List - Specifies the router port list for a specific VLAN.

Configured Version – This displays the configured IGMP operating Version on the given VLAN.

Current Version - The working IGMP Version on the given VLAN.

Configured Querier Status – This displays the configured Querier status, which can be enabled or disabled.

Current Querier Status - The current status of Querier.

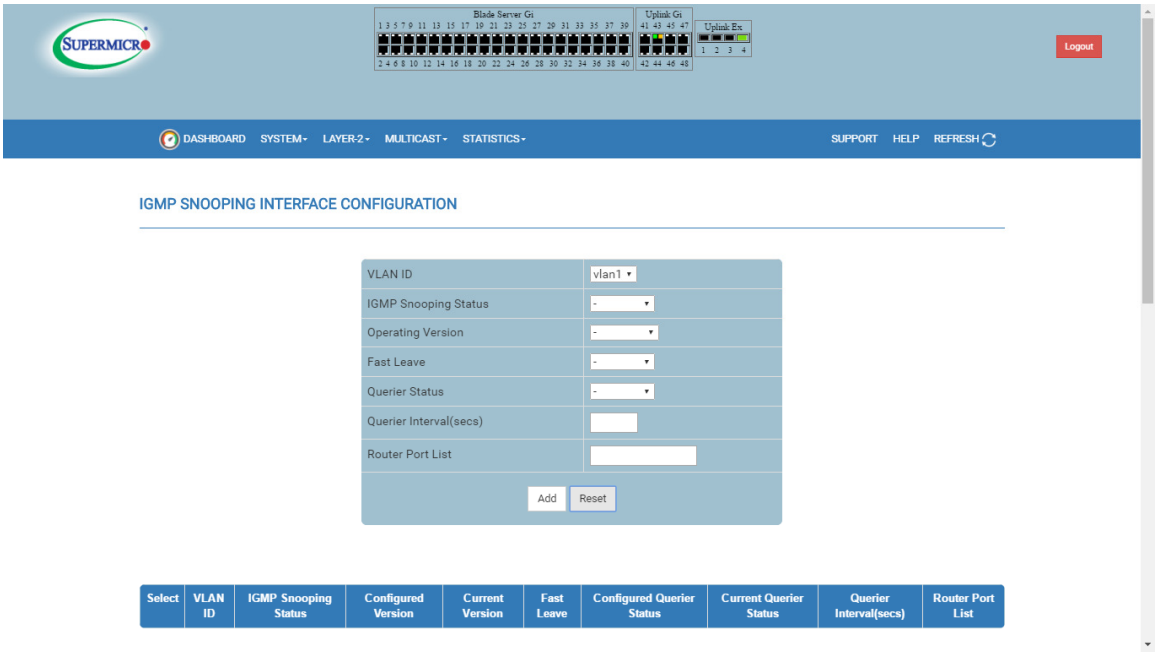


Fig: IGMP Snooping Interface

5.1.4 IGMP Snooping Vlan Router

IGMP Snooping VLAN Router Ports page displays the Router Port List table with the following fields.

VLAN ID - Specifies the VLAN ID.

Port List - Specifies the ports on which routers are connected for a specific VLAN.

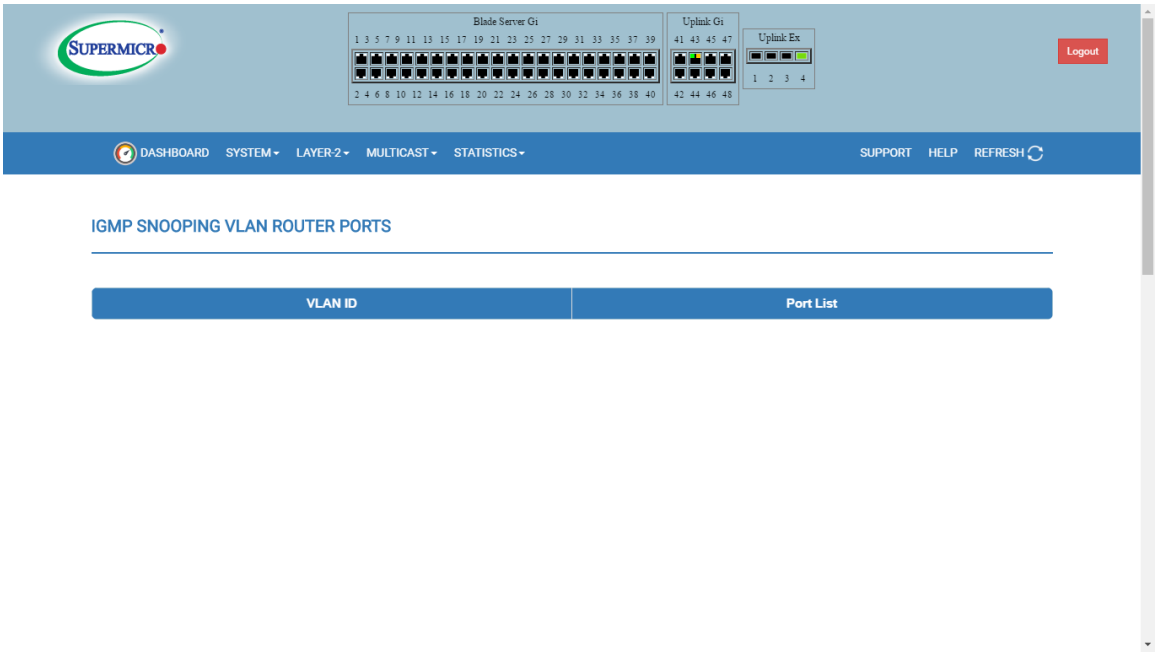


Fig: IGMP snooping Vlan

5.1.5 IGMP MAC Forwarding

MAC Based Multicast Forwarding Table page displays either the IP Based or the MAC Based Multicast Forwarding Table depending upon the configuration of the forwarding mode.

VLAN ID - Specifies the VLAN ID pertaining to the MAC based multicast forwarding entry.

Group MAC Address - Specifies the Group MAC Multicast address that is learnt.

Port List - Specifies the learnt ports.

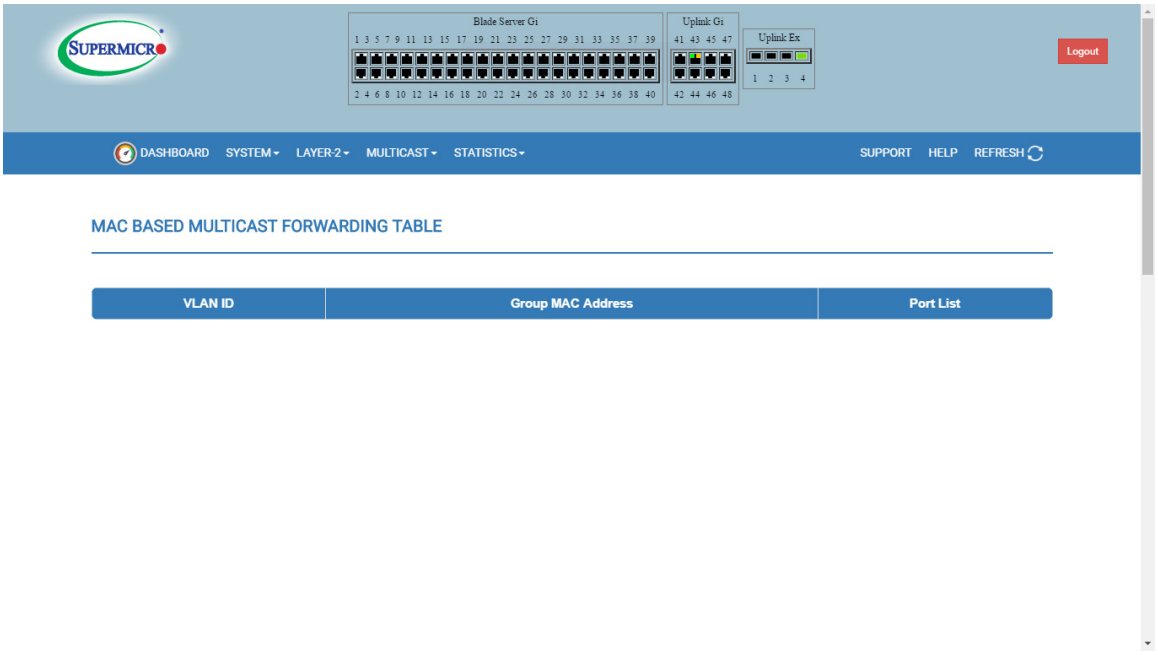


Fig: IGMP Snooping Mac

5.2 Dynamic Multicast

5.2.1 Global Configuration

Dynamic Multicast Global Configuration page helps enabling or disabling dynamic multicast feature.

Context – Displays the context identifier, which is a read only field.

Dynamic Multicast Status - Enable or disable dynamic multicast.

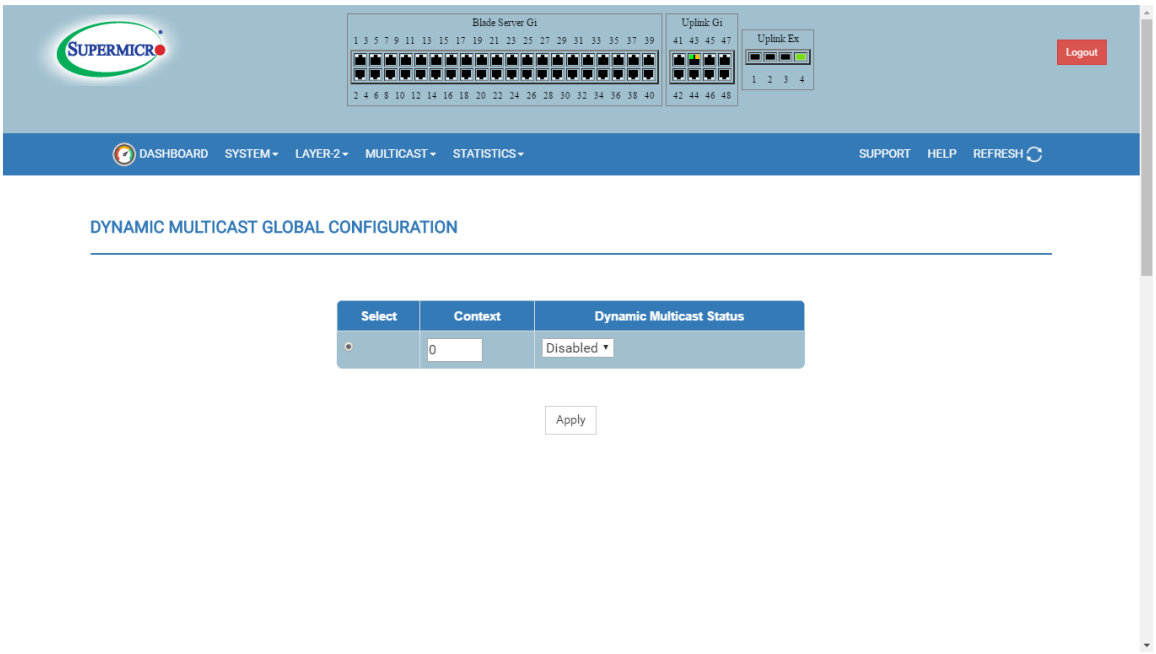


Fig: Dynamic Multicast

5.2.2 Dynamic Multicast Port config

Dynamic Multicast Port Configuration page helps configuring dynamic multicast at port level.

Port - Port index.

Dynamic Multicast Status - Enable or disable dynamic multicast on this port.

Restricted Group Registration - Enable or disable Restricted Group Registration on this port.

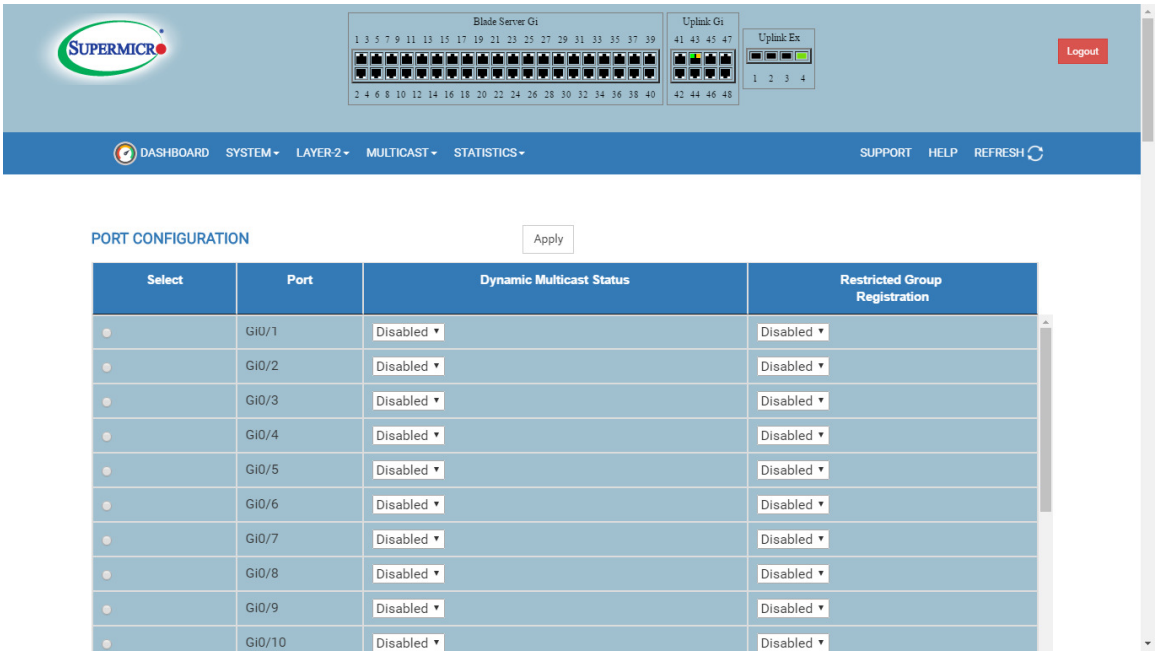


Fig: Dynamic Multicast Port configuration

6 Statistics

Statistics menu has links to all statistical information all features.

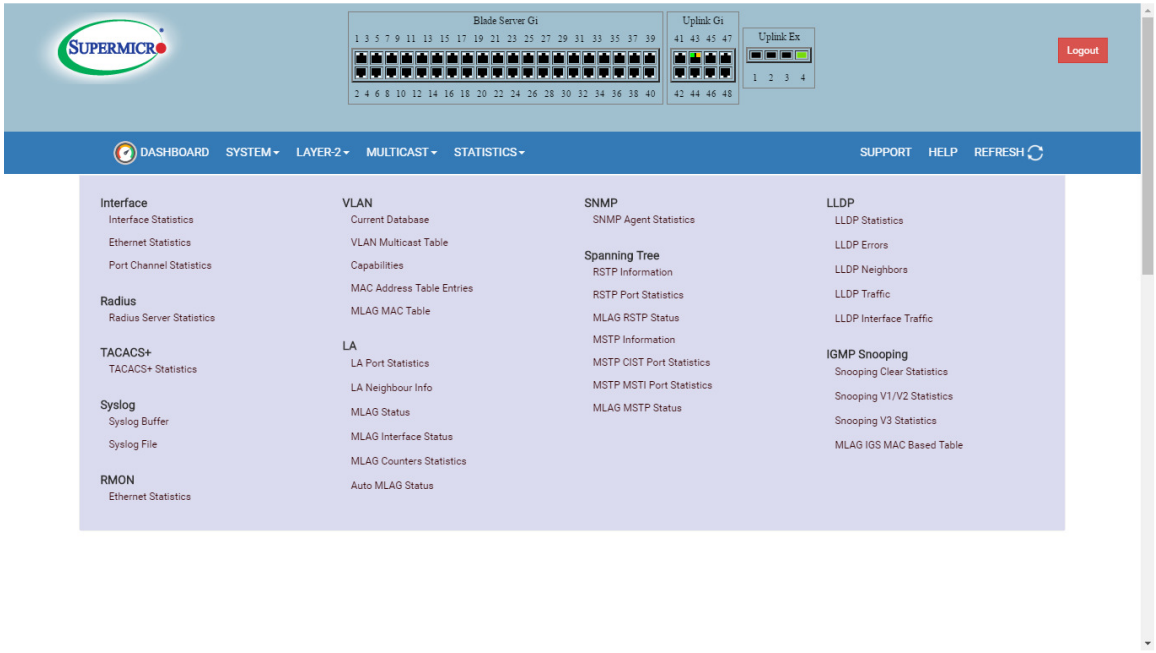


Fig: Statistics

6.1 Interface

6.1.1 Interface Statistics

Interface Statistics page displays the port statistics.

Interface - Port interface.

MTU - Max Transfer Unit bytes.

Speed (Bits Per Second) - Port speed in bits per second.

Received Octets - Number of bytes received.

Received Unicast Packets - Number of unicast packets received.

Received Unicast Packets Rate - Number of unicast packets rate received

Received Broadcast Packets - Number of broadcast packets received.

Received Broadcast Packets Rate - Number of broadcast packets rate received.

Received Multicast Packets - Number of multicast packets received.

Received Multicast Packets Rate - Number of multicast packets rate received.

Received Total Packets Rate - Number of total packets rate received.

Received Pause - Number of pause packets received.

Received Undersize Packets - Number of packets received with size lesser than minimum accepted Ethernet frame size.

Oversize Packets – Number of packets received with size greater than maximum accepted frame size of this interface.

Received CRC – Number of packets received with CRC errors.

Received Discards - Number of packets discarded due to errors.

Received Errors - Number of packets received with errors.

Received Unknown Protocols - Number of packets received with unknown protocol.

Transmitted Octets - Number of bytes transmitted.

Transmitted Unicast Packets - Number of unicast packets transmitted.

Transmitted Unicast Packets Rate - Number of unicast packets rate transmitted.

Transmitted Broadcast Packets - Number of broadcast packets transmitted.

Transmitted Broadcast Packets Rate - Number of broadcast packets rate transmitted.

Transmitted Multicast Packets - Number of multicast packets transmitted.

Transmitted Multicast Packets Rate - Number of multicast packets rate transmitted.

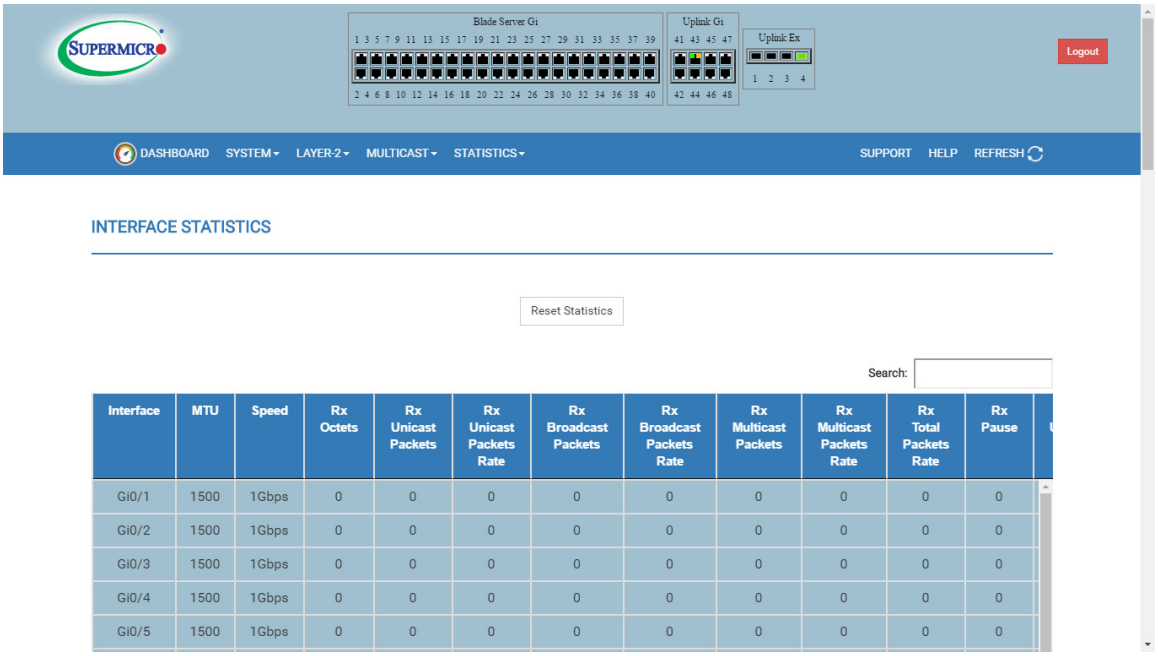
Transmitted Total Packets Rate - Number of total packets rate transmitted.

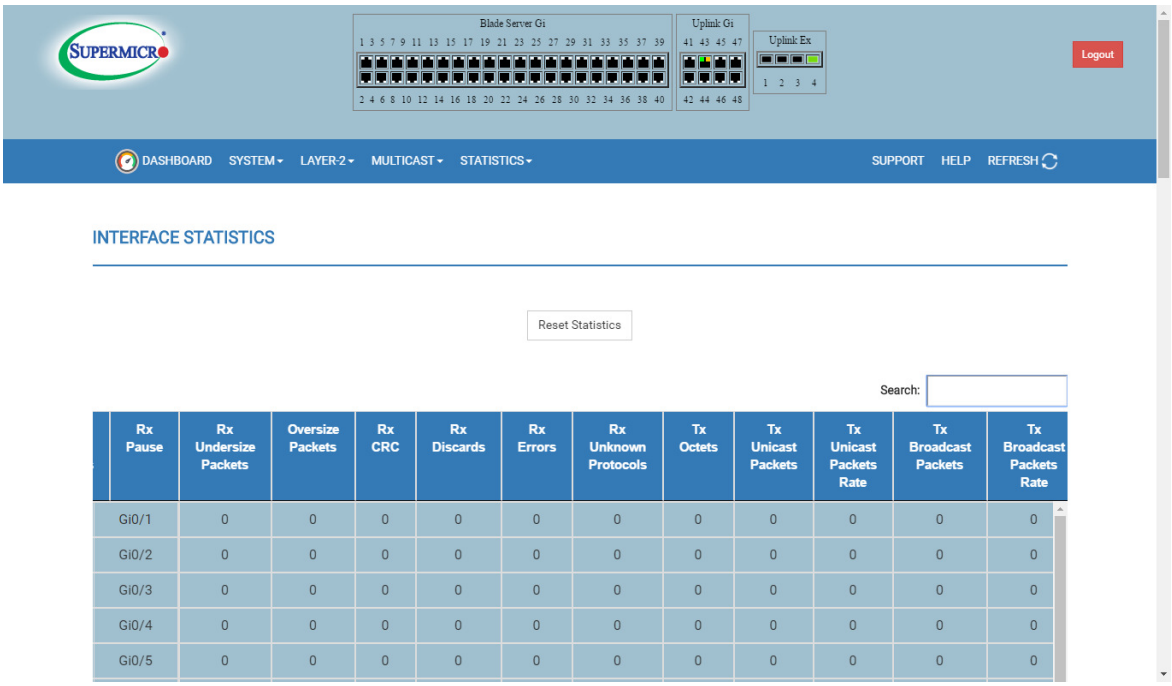
Transmitted Pause - Number of pause packets transmitted.

Transmitted Discards - Number of packets discarded due to transmit errors.

Transmitted Errors - Number of transmit errors.

Reset Statistics – This button used to reset the received and transmitted packet counter values to 0.





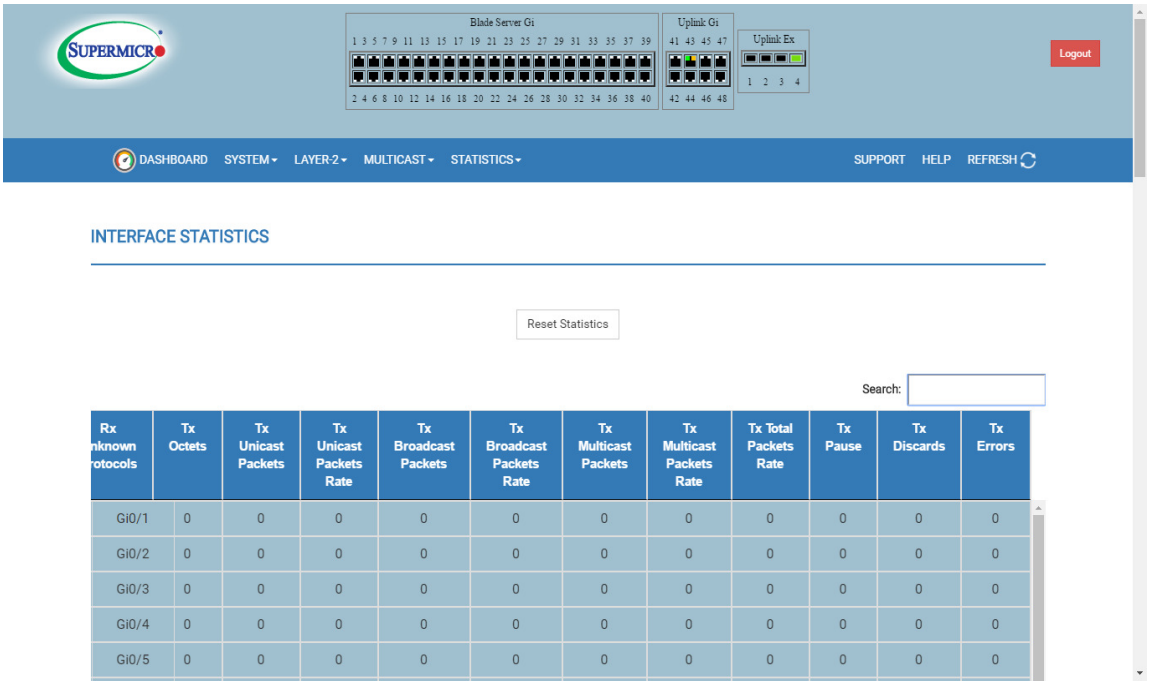


Fig: Interface statistics

6.1.2 Ethernet Statistics

Ethernet Statistics page displays the Ethernet statistics.

Index - Port index.

Alignment Errors - Number of alignment errors. Alignment errors generally indicate improper byte-alignment for Ethernet packets.

FCS Errors - Number of packets received with checksum errors.

Single Collision Frames - Number of frames received with a collision.

Multiple Collision Frames - Number of frames received with multiple collisions.

SQE Test Errors - Number of Signal Quality Errors occurred.

Deferred Transmissions - Number of frames deferred for transmissions due to network sense.

Late Collisions - Number of frames faced late collisions. A collision is considered late if the jam occurs after 512 bit-times, or 64 bytes.

Excess Collisions - Number of excess collisions detected. Excessive Collisions describe the situation where a station has tried 16 times to transmit without success and discards the frame. This means that there is excessive traffic on the network and this must be reduced.

Transmitted Internal MAC Errors - Number of MAC transmit errors.

Carrier Sense Errors - Number of carrier sense errors.

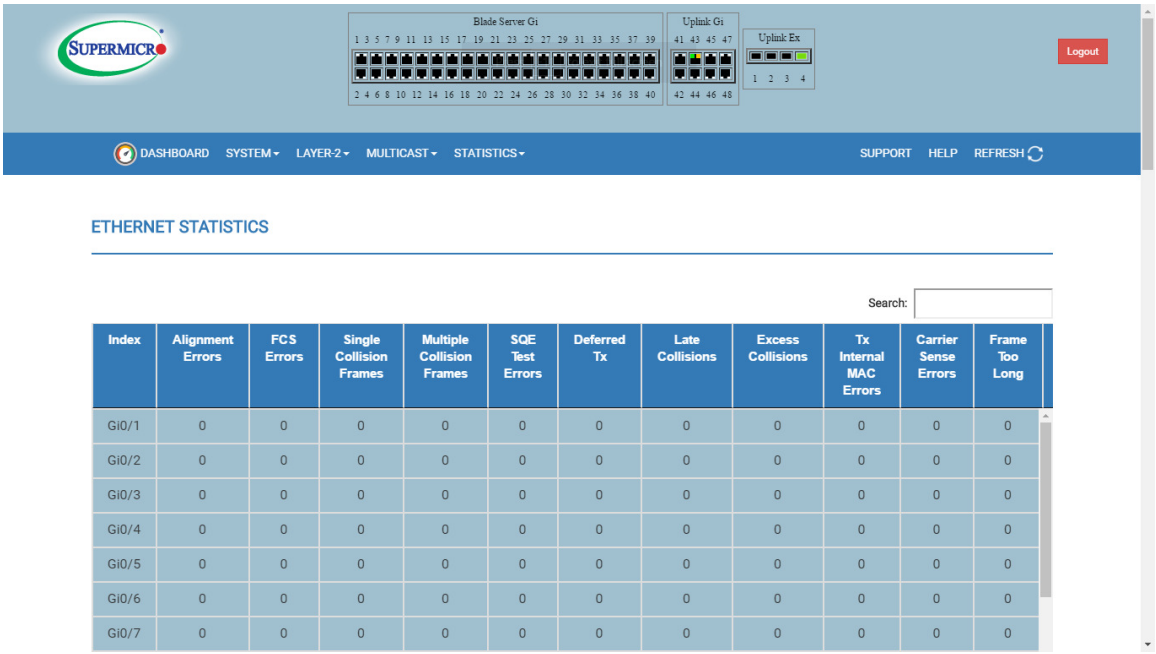
Frame Too Long - Number of too long frames received for transmission.

Received Internal MAC Errors - Number of MAC receive errors.

Ether ChipSet – - Number of ethernet chip set value**.**

Symbol Errors - Number of symbol errors.

Duplex Status - Current status of duplex.



Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Tx	Late Collisions	Excess Collisions	Tx Internal MAC Errors	Carrier Sense Errors	Frame Too Long
Gi0/1	0	0	0	0	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0	0	0	0	0

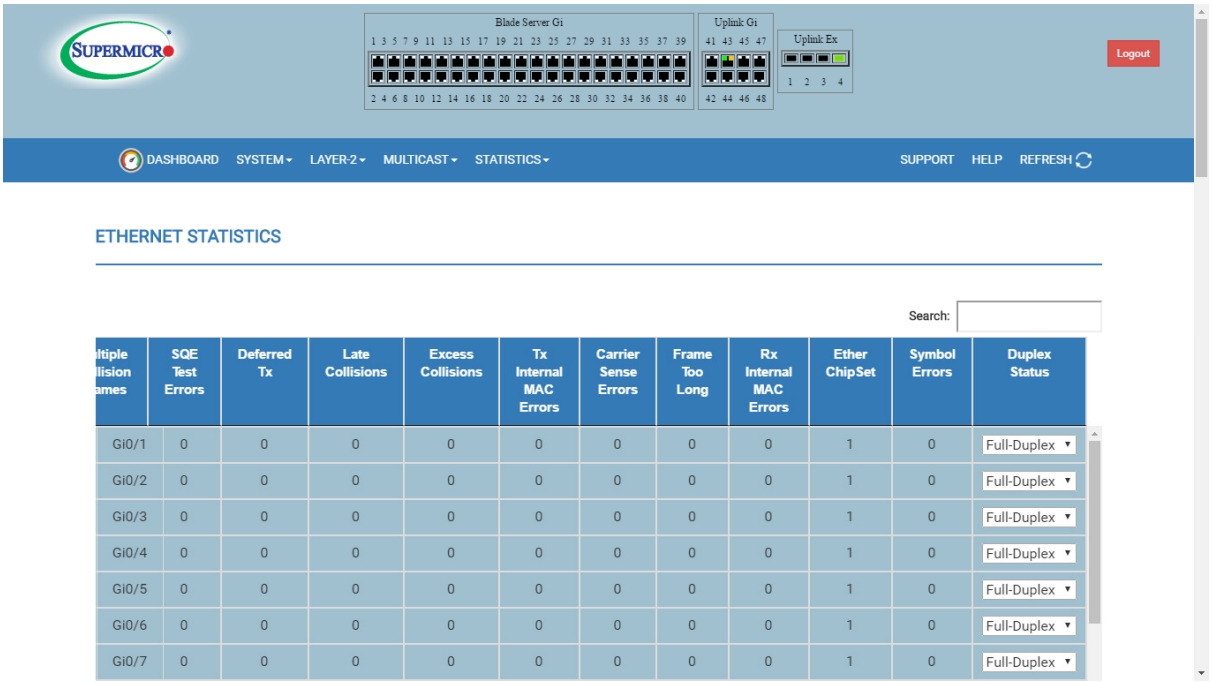


Fig: Ethernet Statistics

6.1.3 Port Channel Statistics

Port Channel Statistics page displays the port statistics.

Interface - Port interface.

MTU - Max Transfer Unit bytes.

Received Octets - Number of bytes received.

Received Unicast Packets - Number of unicast packets received.

Received Unicast Packets Rate - Number of unicast packets rate received.

Received Broadcast Packets - Number of broadcast packets received.

Received Broadcast Packets Rate - Number of broadcast packets rate received.

Received Multicast Packets - Number of multicast packets received.

Received Multicast Packets Rate - Number of multicast packets rate received.

Received Total Packets Rate - Number of total packets rate received.

Received Pause - Number of pause packets received.

Received Undersize Packets - Number of packets received with size lesser than minimum accepted Ethernet frame size.

Oversize Packets – Number of packets received with size greater than maximum accepted Ethernet frame size.

Received CRC – Number of packets received with CRC errors.

Received Discards - Number of packets discarded due to errors.

Received Errors - Number of packets received with errors.

Received Unknown Protocols - Number of packets received with unknown protocol.

Transmitted Octets - Number of bytes transmitted.

Transmitted Unicast Packets - Number of unicast packets transmitted.

Transmitted Unicast Packets Rate - Number of unicast packets rate transmitted.

Transmitted Multicast Packets - Number of multicast packets transmitted.

Transmitted Multicast Packets Rate - Number of multicast packets rate transmitted.

Transmitted Broadcast Packets - Number of broadcast packets transmitted.

Transmitted Broadcast Packets Rate - Number of broadcast packets rate transmitted.

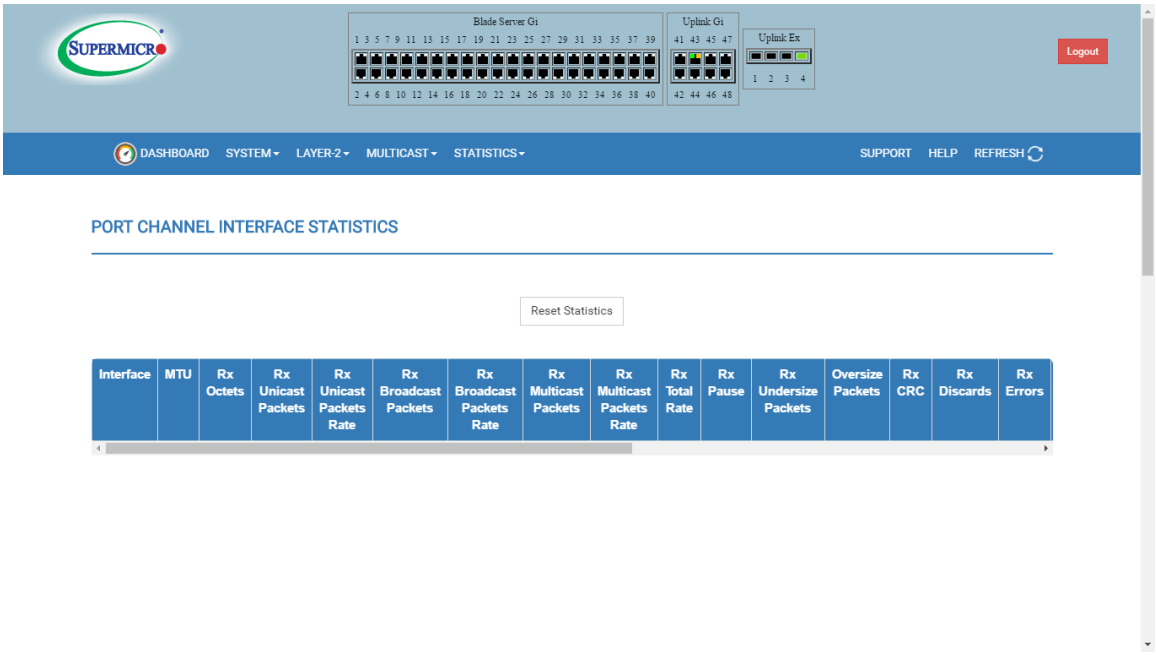
Transmitted Total Packets Rate - Number of total packets rate transmitted.

Transmitted Pause - Number of pause packets transmitted.

Transmitted Discards - Number of packets discarded due to transmit errors.

Transmitted Errors - Number of transmit errors.

Reset Statistics – This button used to reset the received and transmitted packet counter values to 0.



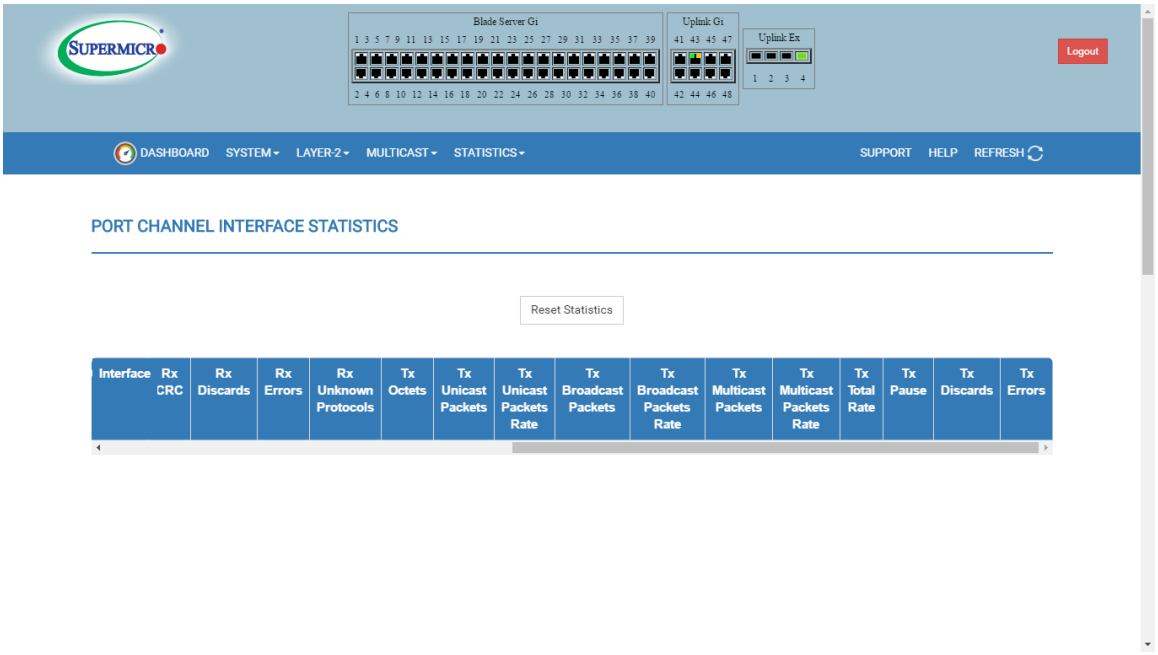


Fig: Port Channel Statistics

6.2 Radius Statistics

Radius Server Statistics page displays the following information about Radius server.

Index – Port index.

Radius Server Address – Address of the radius server.

UDP Port Number – Port number.

Round Trip Time - Round Trip Time in seconds.

No of Request Packets - Number of request packets transmitted.

No of Retransmitted Packets - Number of packets retransmitted.

No of Access-Accept Packets - Number of accept packets.

No of Access-Reject Packets - Number of reject packets.

No of Access-Challenge Packets - Number of challenge packets.

No of Malformed Access Responses - Number of invalid access responses received.

No of Bad Authenticators - Number of failed authentications.

No of Pending Requests - Number of currently pending requests.

No of Time Outs - Number of time outs happened.

No of Unknown Types - Number of unknown types received.

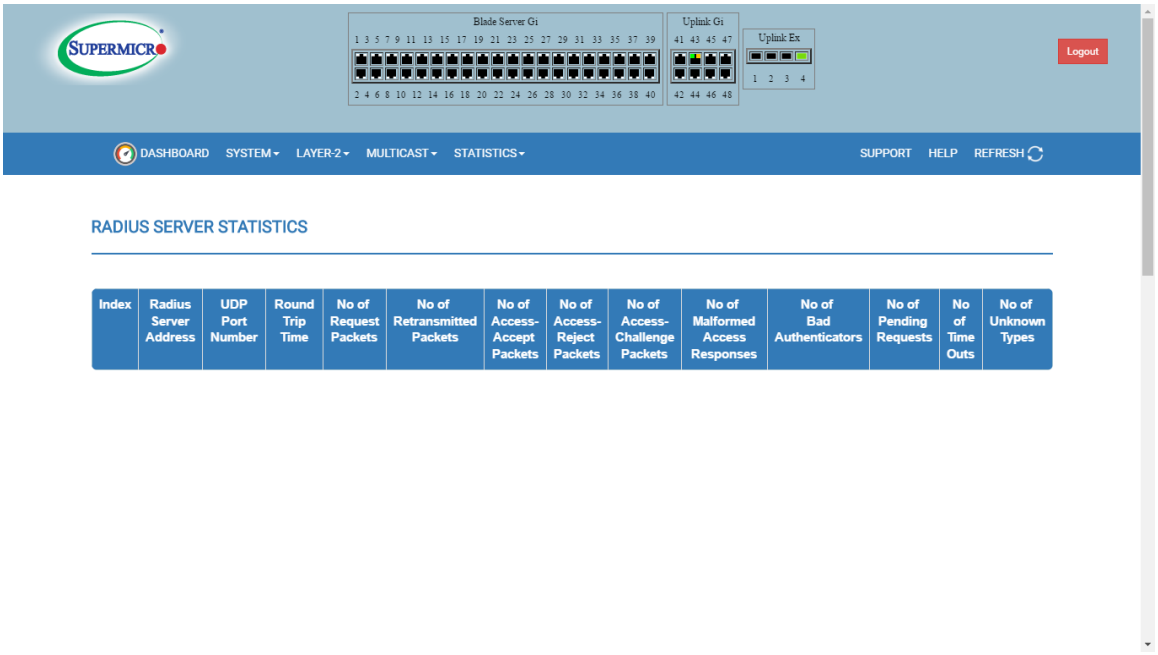


Fig: Radius Statistics

6.3 TACACS+ Statistics

TACACS+ Statistics page displays the following information about TACACS.

Authentication Starts Request - Number of authentication start request packets received.

Authentication Continues Request - Number of authentication continue request packets received.

Authentication Enables Request - Number of authentication enable request packets received.

Authentication Aborts Request - Number of authentication abort request packets received.

Authentication Pass Received - Number of authentication pass packets received.

Authentication Fails Received - Number of authentication fail packets received.

Authentication Get User Received - Number of authentication get user packets received.

Authentication Get Pass Received - Number of authentication get pass packets received.

Authentication Get Data Received - Number of authentication get data packets received.

Authentication Errors Received - Number of authentication error packets received.

Authentication Follows Received - Number of authentication follow packets received.

Authentication Restart Received - Number of authentication restart packets received.

Authentication Session Timeouts - Number of authentication session timeout packets received.

Authorization Requests - Number of authorization request packets received.

Authorization Pass Add Received - Number of authorization pass add packets received.

Authorization Pass Reply Received - Number of authorization pass reply packets received.

Authorization Fails Received - Number of authorization fail packets received.

Authorization Errors Received - Number of authorization error packets received.

Authorization Follows Received - Number of authorization follow packets received.

Authorization Session Timeouts - Number of authorization session timeout packets received.

Accounting Start Requests - Number of accounting start packets received.

Accounting WD Requests - Number of accounting WD request received.

Accounting Stop Requests - Number of accounting stop packets received.

Accounting Success Received - Number of accounting success packets.

Accounting Errors Received - Number of accounting error packets received.

Accounting Follows Received - Number of accounting follow packets received.

Accounting Session Timeouts - Number of accounting session timeout packets received.

Malformed Packets Received - Number of malformed packets received.

Socket Failures - Number of socket failure packets received.

Connection Failures - Number of connection failure packets received.

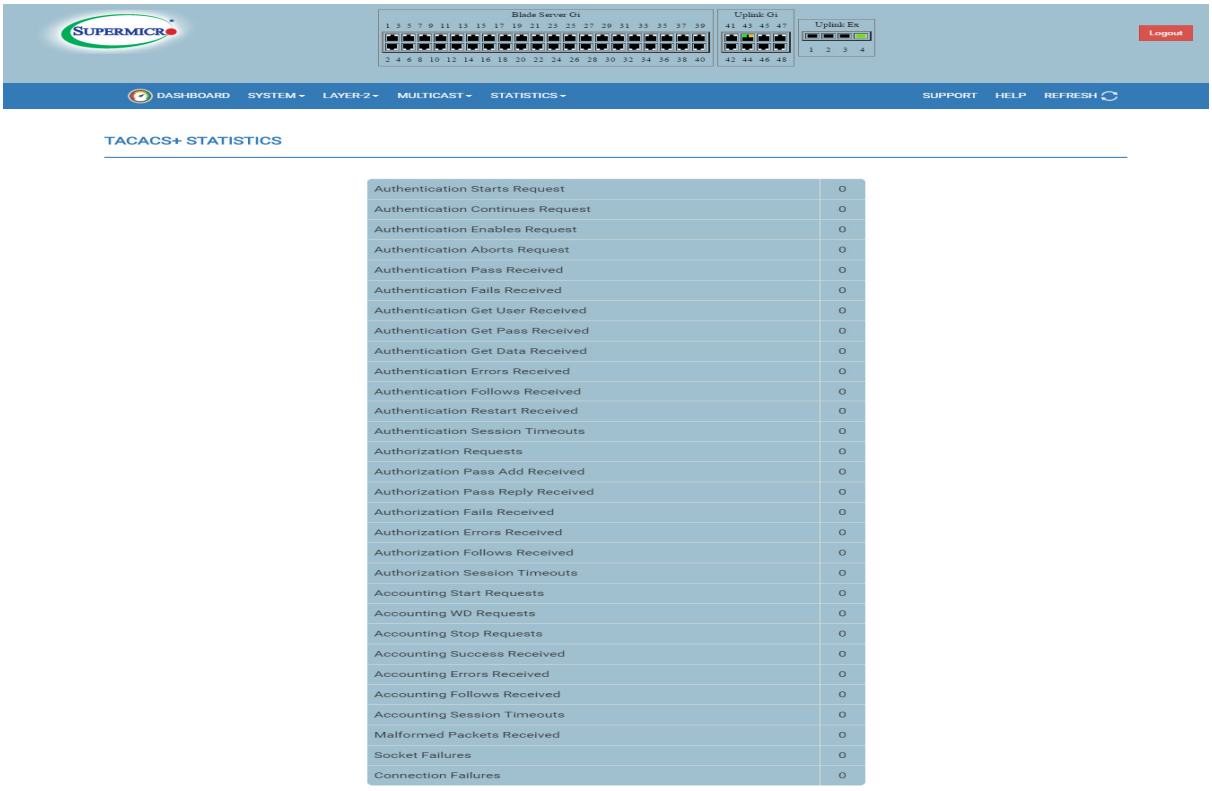


Fig: TACACS+ Statistics

6.4 Syslog Statistics

6.4.1 Syslog Buffer

This page displays syslog messages from syslog buffers in memory.

Clear Log Buffers button helps clearing all messages in syslog buffer memory.

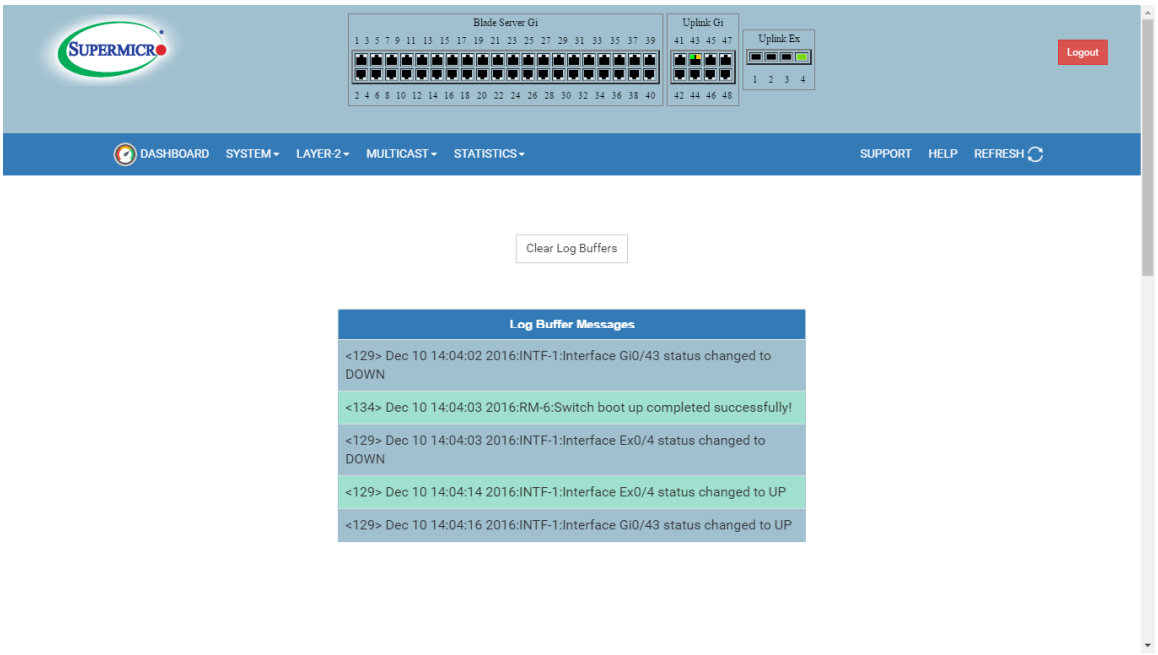


Fig: Syslog Buffer

6.4.2 Syslog File

This page displays syslog messages from syslog file in flash memory.

Clear Log File button helps removing all messages in current syslog file.

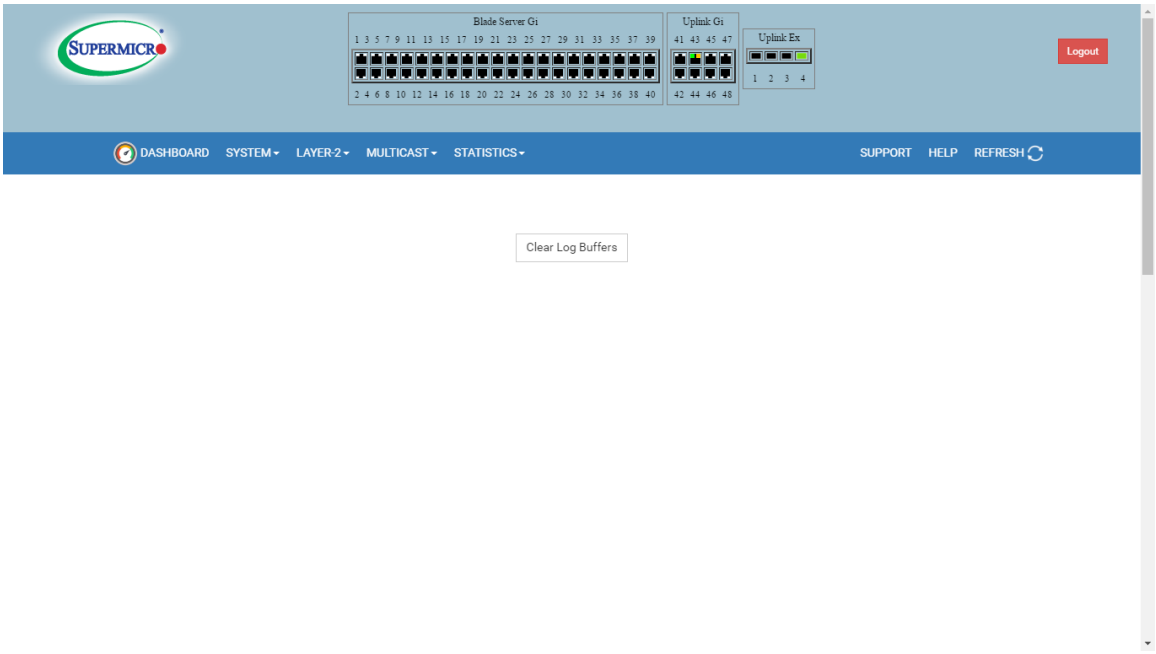


Fig: Syslog File

6.5 RMON Ethernet Statistics

RMON Ethernet Statistics page displays the following RMON Ethernet statistics information.

Index- Port index.

Data src – Number of data source received.

Drop Evts- Number of drop events received.

Packets - Number of packets received.

Broadcast Packets - Number of broadcast packets received.

Multicast Packets - Number of multicast packets received.

CRC Errors - Number of packets received with CRC errors.

Under Size Packets - Number of under size packets received.

Over Size Packets - Number of over size packets received.

Fragments - Number of fragments received.

Jabbers - Number of jabbers.

Collisions - Number of collisions.

64 Octets - Number of Ethernet packets received with size less than 64 bytes.

65-127 Octets - Number of Ethernet packets received with size between 65 to 127 bytes.

128-255 Octets - Number of Ethernet packets received with size between 128 to 255 bytes.

256-511 Octets - Number of Ethernet packets received with size between 256 to 511 bytes.

512-1023 Octets - Number of Ethernet packets received with size between 512 to 1023 bytes.

1024-1518 Octets - Number of Ethernet packets received with size between 1024 to 1518 bytes.

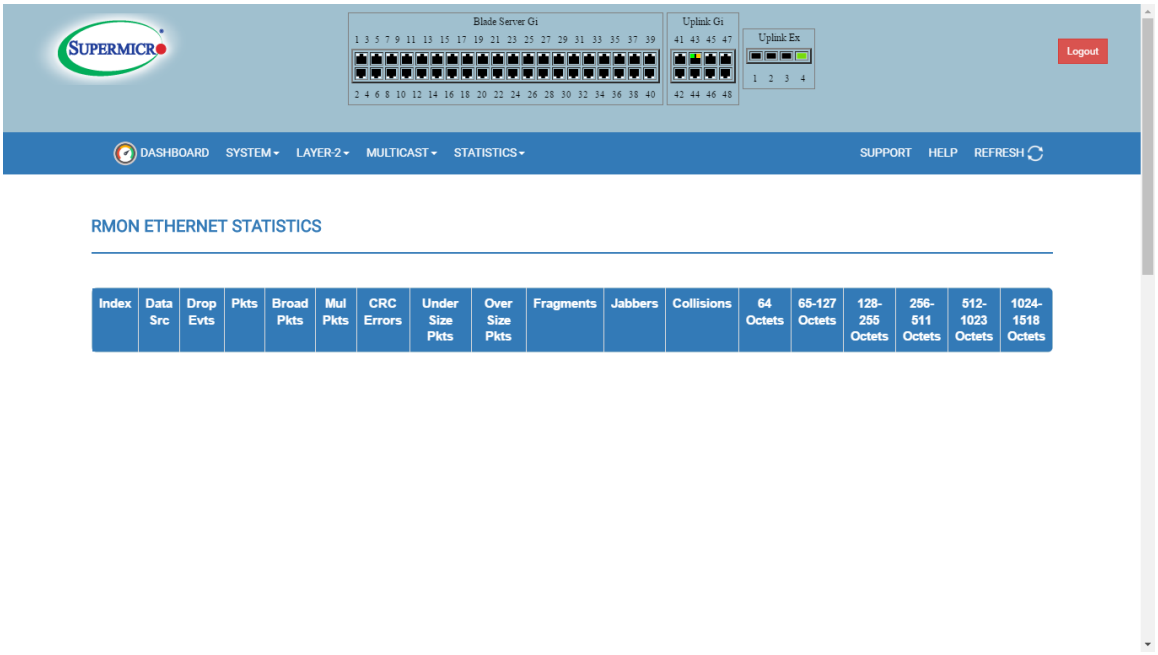


Fig: RMON Ethernet Statistics

6.6 VLAN Statistics

6.6.1 Current DB

VLAN Current Database page displays the VLAN database entries.

VLAN ID - VLAN identifier.

VLAN Name - VLAN filter database identifier.

Member Ports - Index of member ports.

Tagged Ports - Index of tagged member ports.

Untagged Ports - Index of untagged member ports.

Forbidden Ports - Index of forbidden member ports.

Access Ports - Index of access member ports.

Trunk Ports - Index of trunk member ports.

Status - VALN status.

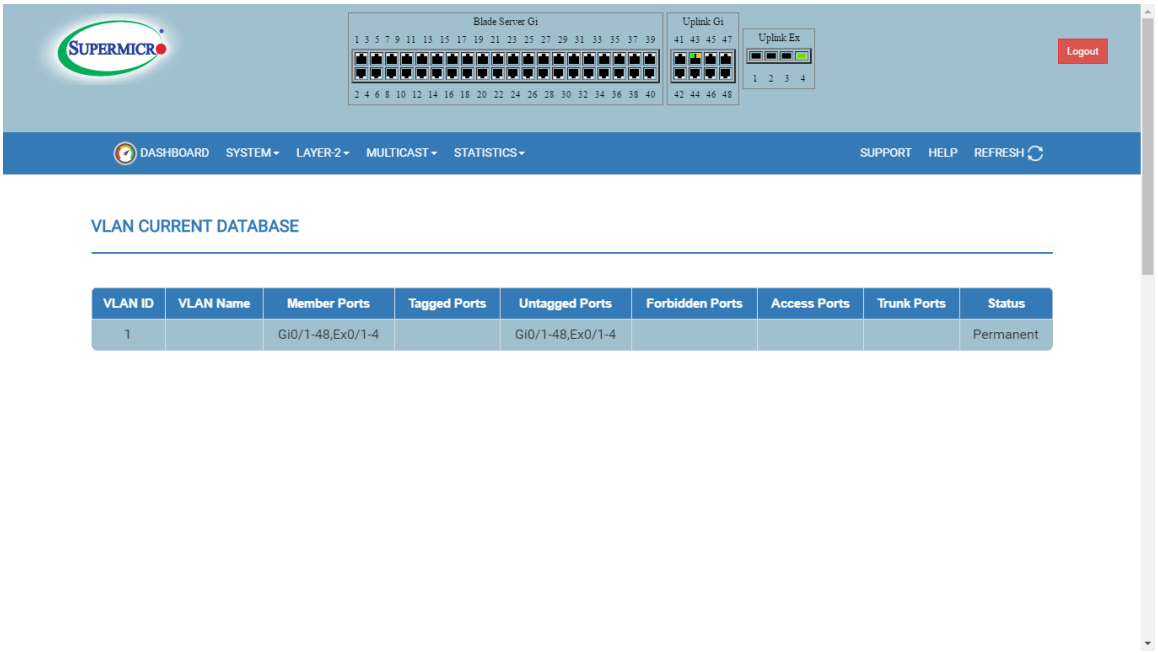


Fig: Vlan Current DB

6.6.2 VLAN Multicast Table

VLAN Multicast Table page displays the multicast VLAN information.

VLAN ID - VLAN identifier.

Address - VLAN address.

Egress Ports - Indexes of egress ports.

Ports Learnt - Indexes of ports on this VLAN is learned.

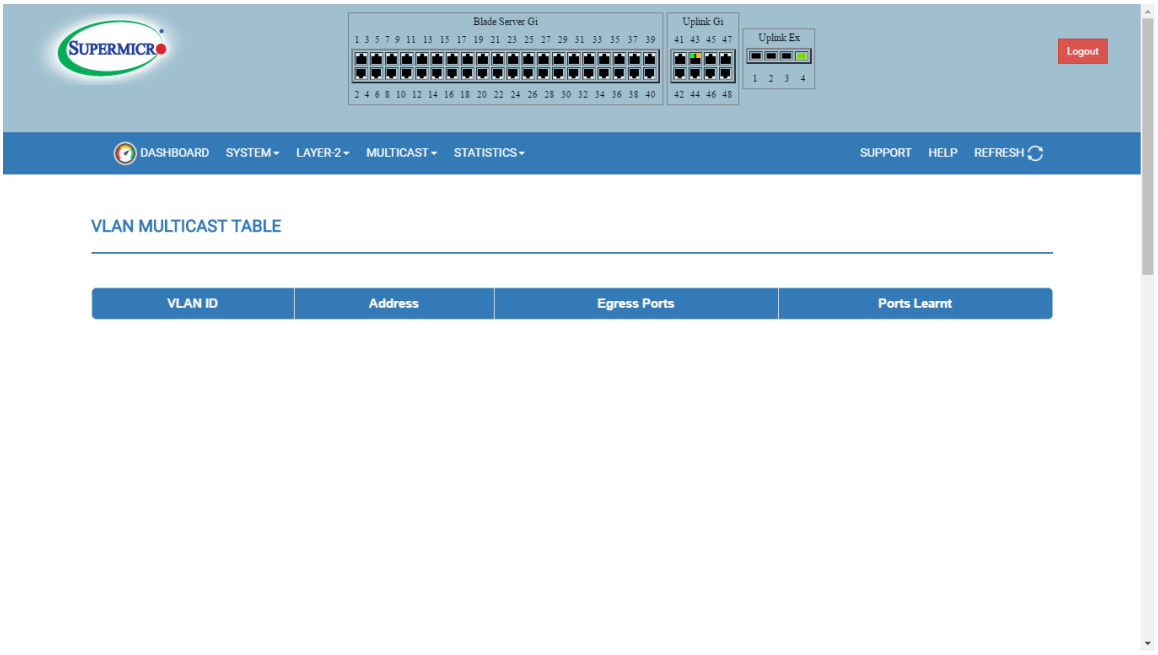


Fig: Vlan Multicast Table

6.6.3 VLAN Capabilities

VLAN Capabilities page displays the VLAN capabilities of switch.

Extended filtering services

Traffic classes

Static Entry Individual port

IVL capable

SVL capable

Hybrid capable

Configurable Pvid Tagging

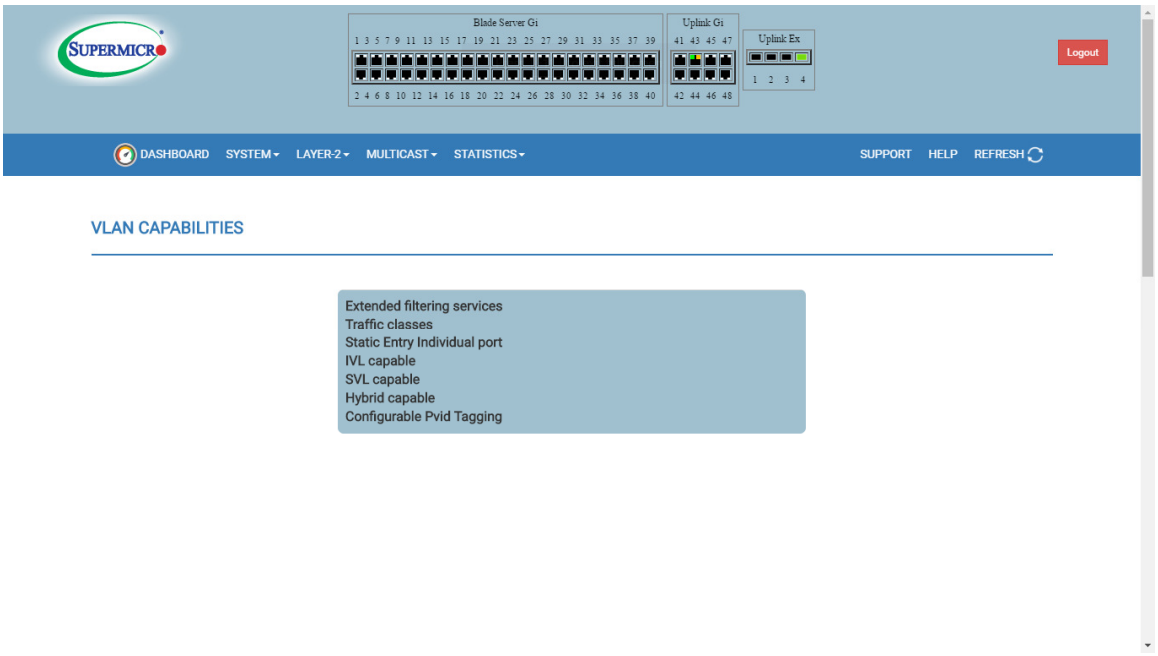


Fig: Vlan Capabilities

6.6.4 VLAN MAC Address Table Entries

VLAN MAC address table Entries page displays the VLAN Mac address entries.

VLAN ID - VLAN identifier.

MAC Address - MAC address learned.

Port - Index of port where this entry is learned.

All – User can choose this one, it displays the VLAN ID, MAC address and Port details .

Status - Status of this entry.

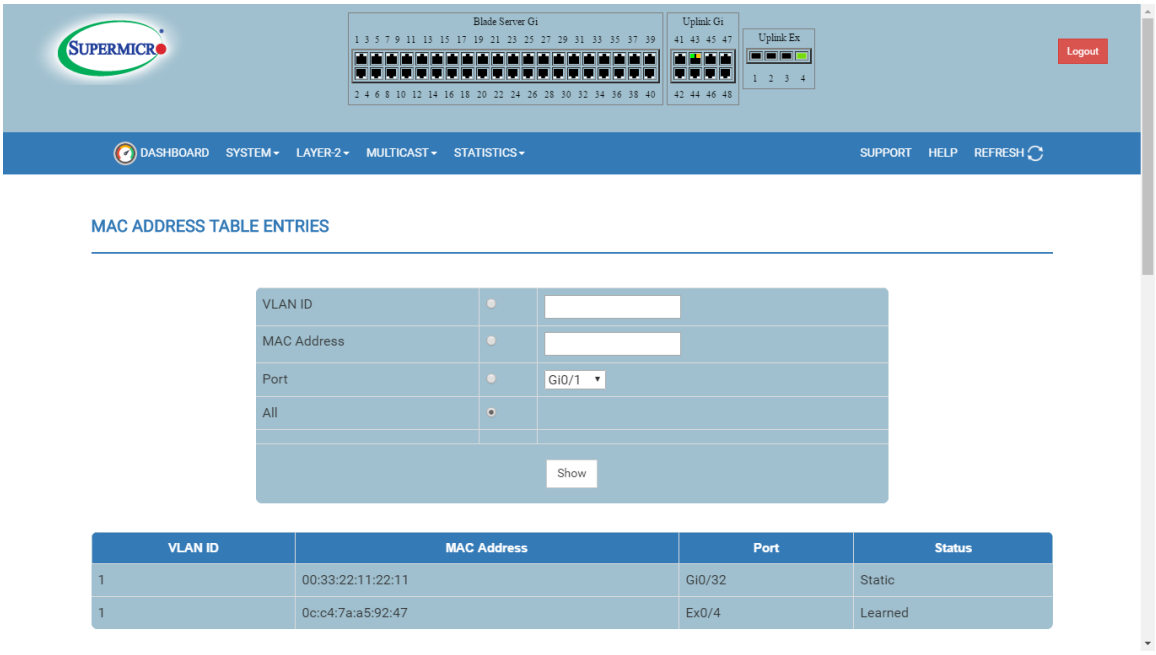


Fig: Vlan MAC Address Table Entries

6.6.5 MLAG MAC Table

MLAG MAC address table page displays the MLAG Mac entries.

VLAN - VLAN identifier.

MAC Address - Displays the learned MAC entry.

Ports - Displays the port channel index, where this entry is learned.

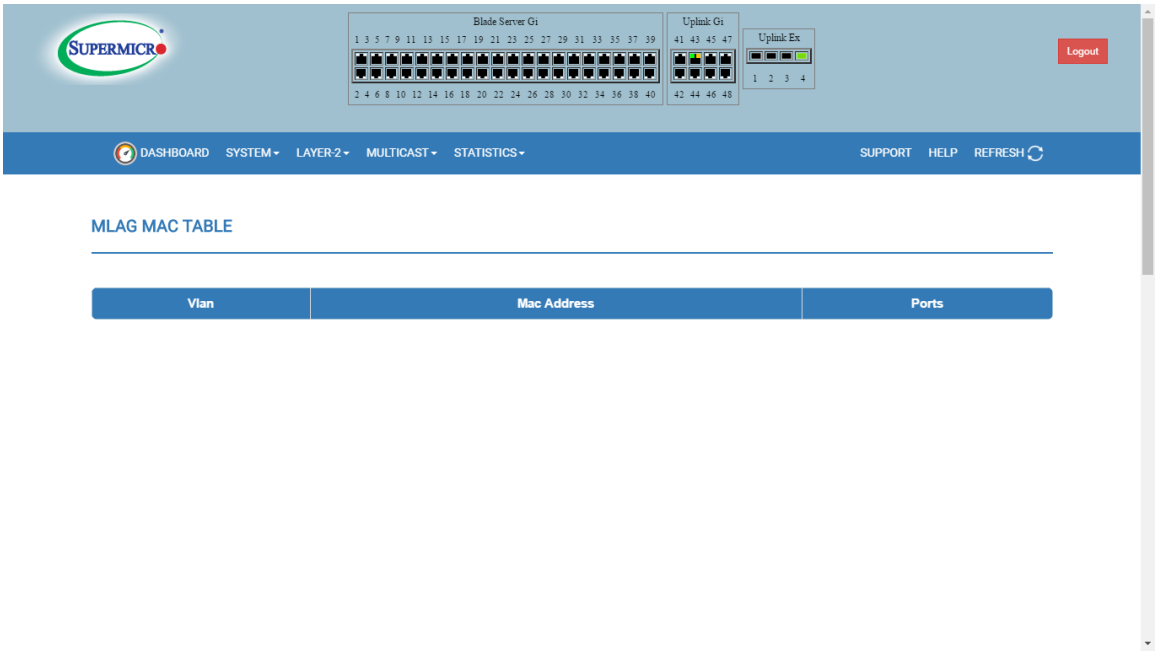


Fig: MLAG MAC Table

6.7 LA Statistics

6.7.1 LA Port Statistics

LA Port Statistics page displays the following LACP port level statistics.

Port - Port index.

Received PDUs - Number of LACP PDUs received.

Received Marker PDUs - Number of Marker PDUs received.

Received Marker Response - Number of Marker response PDUs received.

Received Unknown PDUs - Number of unknown PDUs received.

Received Illegal PDUs - Number of invalid PDUs received.

Transmitted PDUs - Number of LACP PDUs transmitted.

Transmitted Marker PDUs - Number of Marker PDUs transmitted.

Transmitted Marker Response - Number of Marker response PDUs transmitted.

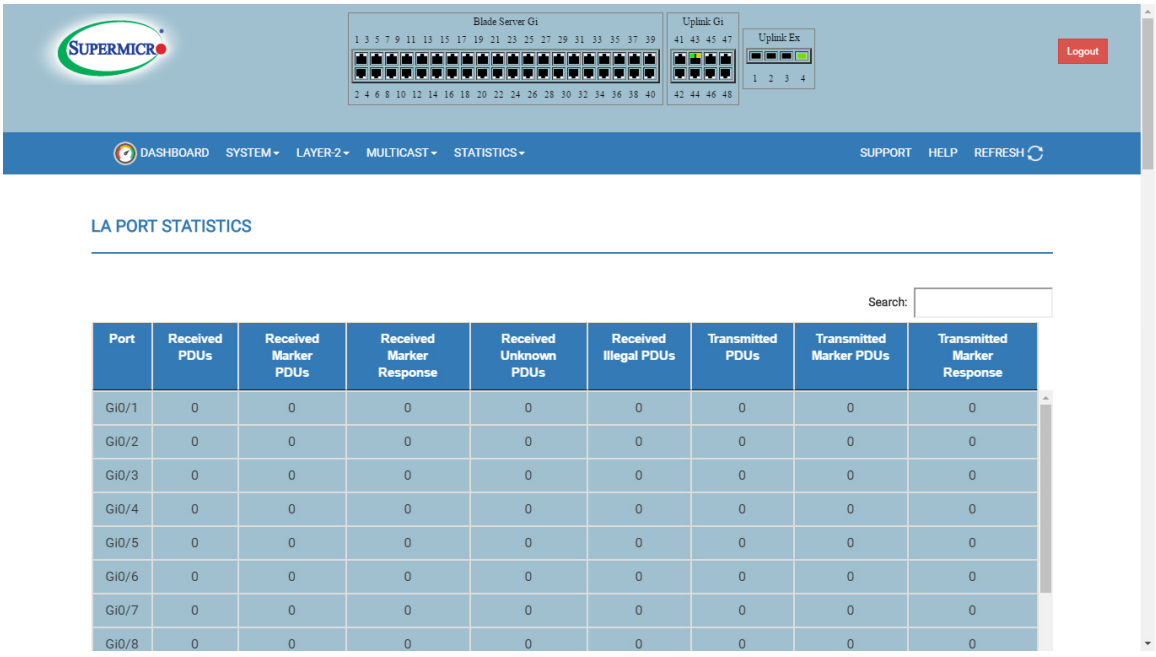


Fig: LA Port Statistics

6.7.2 LA neighbor Statistics

LA Neighbor Statistics Information page displays the following LACP neighbor statistics.

Port

Partner SystemID

Oper Key

Partner Port Priority

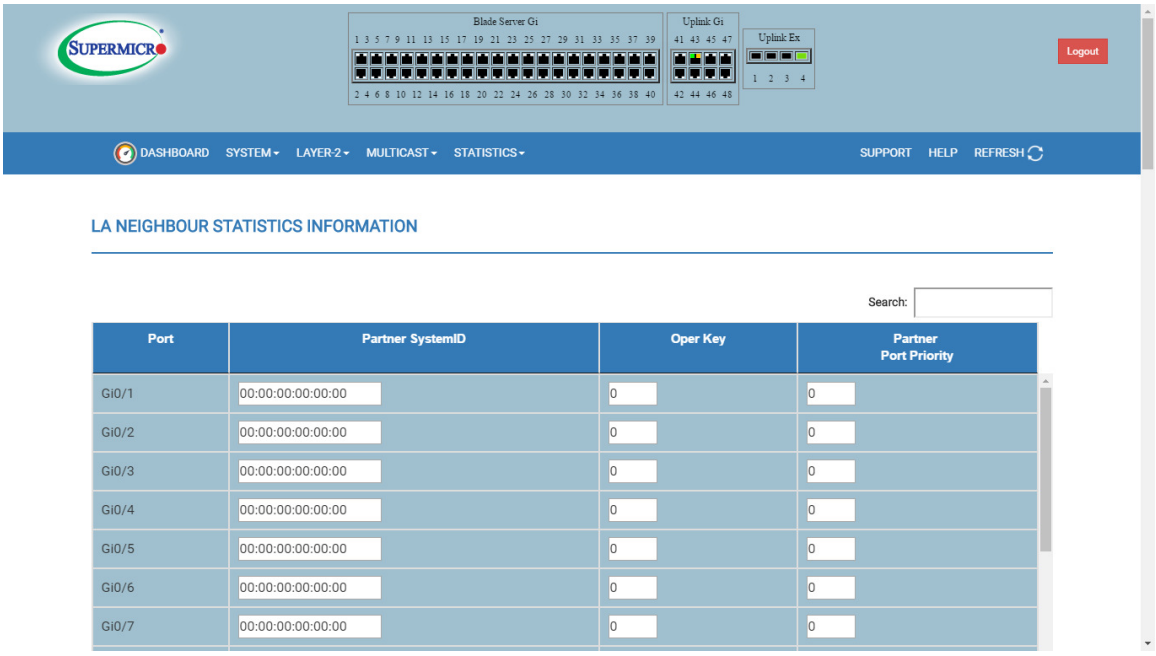


Fig: LA Neighbor Statistics

6.7.3 MLAG Status

MLAG status page displays the following MLAG information.

System ID - Displays the System ID for that MLAG, this is in MAC Address format.

System Priority - Displays the priority value.

Keep Alive Time - Time in seconds.

IPL Interface - Displays the configured IPL Port channel.

Peer System ID - Displays the Peer System ID for MLAG, this is in MAC Address format.

IPL Link Status - Up or Down.

Peer Connection State - Displays the state, which can be "Established" or "Not Established" or "Connection Error".

MLAG Role - Primary or Secondary.

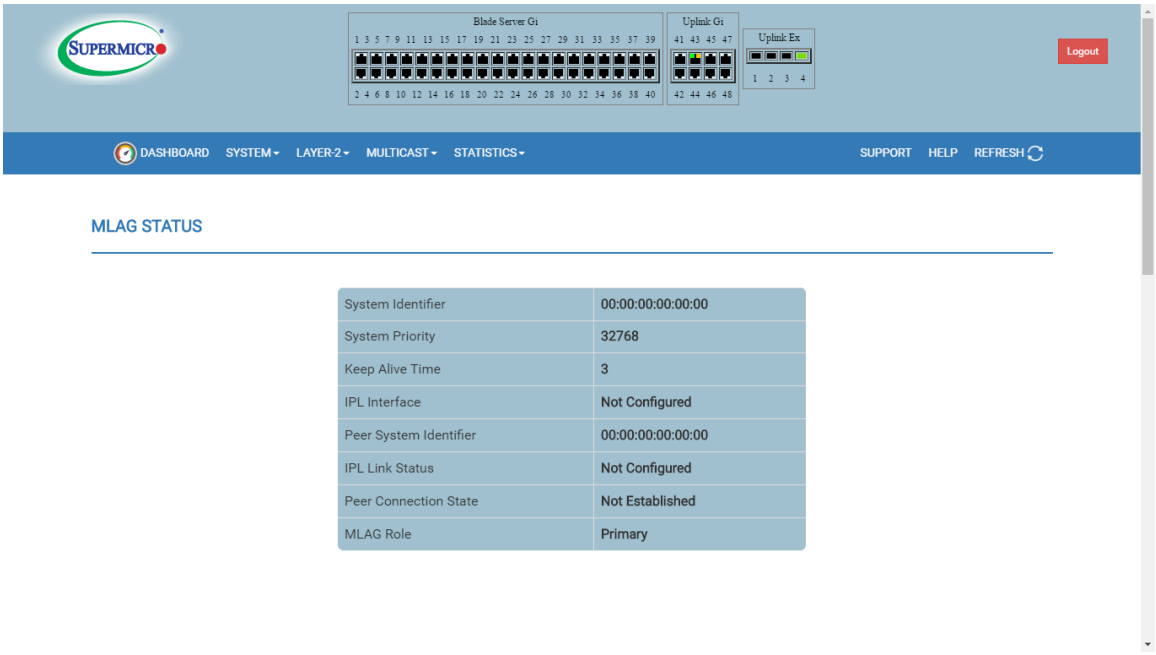


Fig: MLAG Status

6.7.4 MLAG Interface Status

MLAG Interface Status page displays the interface information.

MLAG Id - Displays the MLAG Port Channel Id.

Local Status - Displays the Local MLAG Port Channel.

Peer Status - Displays the Peer Switch MLAG Port Channel.

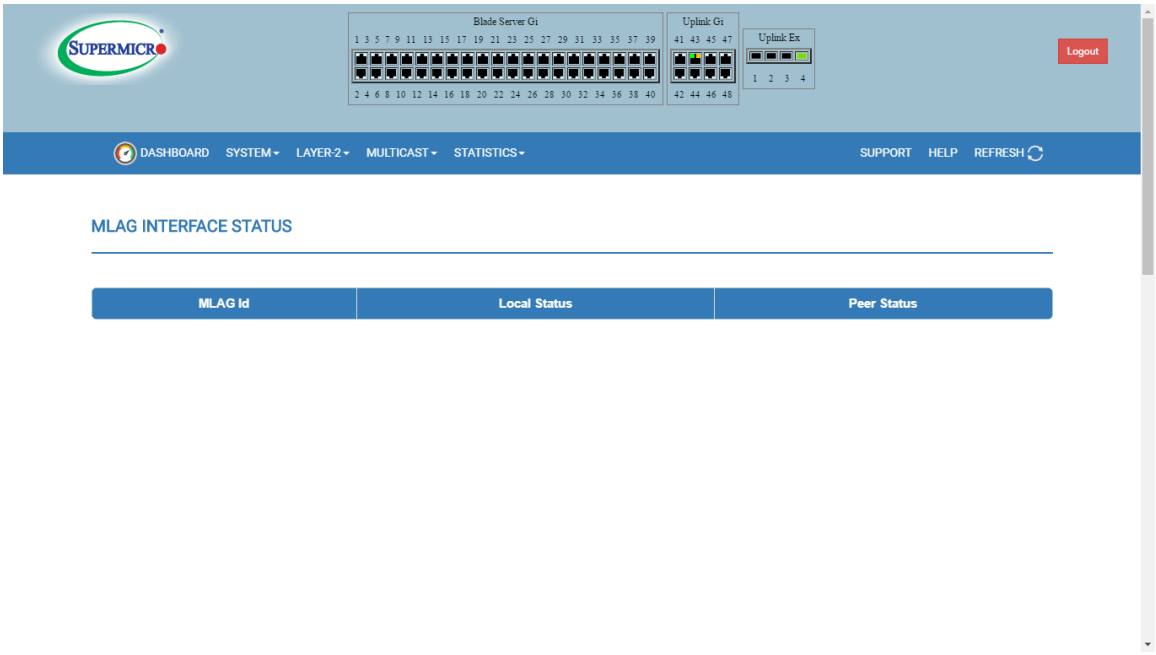


Fig: MLAG Interface Status

6.7.5 MLAG Counter Statistics

MLAG Counters Statistics page displays the sent and received packet information.

Received KeepAlive Packets - Number of KeepAlive packets received.
Received MLAG Status Packets - Number of MLAG Status packets received.
Received STP Packets - Number of STP packets received.
Received STP PortState Packets - Number of STP port state packets received.
Received MAC Packets - Number of MAC Sync packets received.
Received L3 MAC Packets - Number of layer3 MAC Sync packets received.
Received ARP Packets - Number of ARP packets received.
Received IGS Packets - Number of IGS packets received.
Transmitted KeepAlive Packets - Number of Keep Alive packets transmitted.
Transmitted MLAG Status Packets - Number of MLAG Status packets transmitted.
Transmitted STP Packets - Number of STP packets transmitted.
Transmitted STP PortState Packets - Number of STP Port State packets transmitted.
Transmitted MAC Packets - Number of MAC Sync packets transmitted.
Transmitted L3 MAC Packets - Number of layer3 MAC Sync packets transmitted.
Transmitted ARP Packets - Number of ARP packets transmitted.
Transmitted IGS Packets - Number of IGS packets transmitted.

Reset Statistics - This button is used to reset the all counter values.

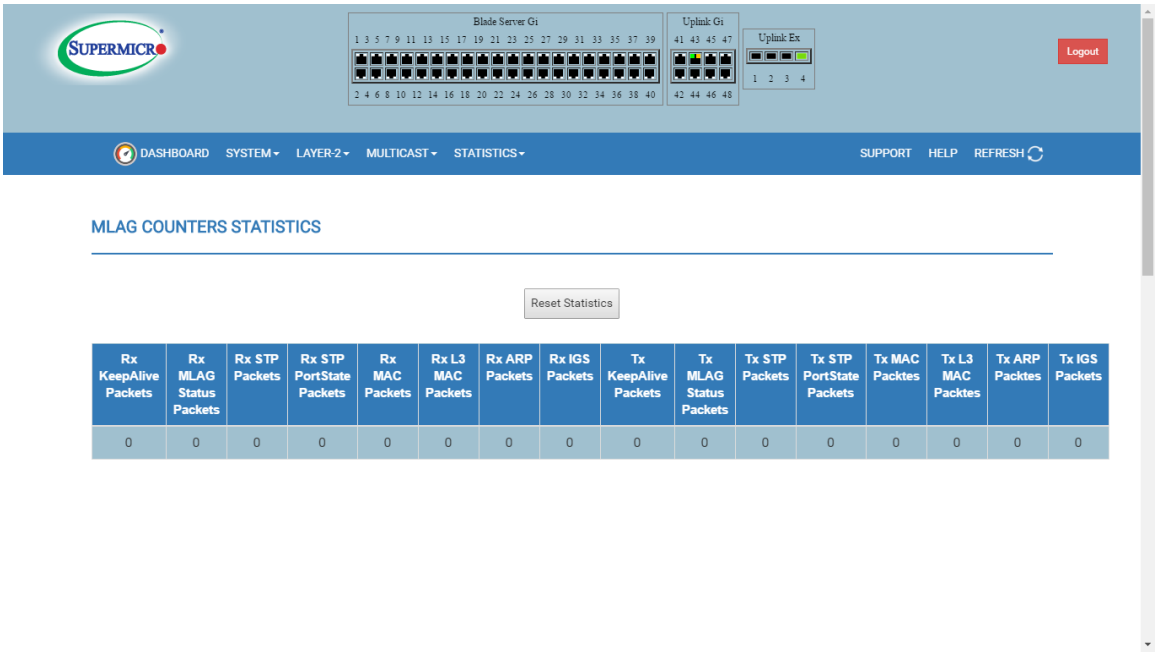


Fig: MLAG counter Statistics

6.8 SNMP Agent Statistics

SNMP Agent Statistics page displays the following SNMP statistics.

SNMP Packets Input

BAD SNMP Version Errors

SNMP Unknown Community Name

SNMP Get Request PDU's

SNMP Get Next PDU's

SNMP Set Request PDU's

SNMP Packet Output

SNMP Too Big Errors

SNMP No Such Name Errors

SNMP Bad Value Errors

SNMP General Errors

SNMP Trap PDU's

SNMP Manager-Role Output Packets

SNMP Inform Responses Received

SNMP Inform Request Generated

SNMP Inform Messages Dropped

SNMP Inform Requests awaiting Acknowledgement

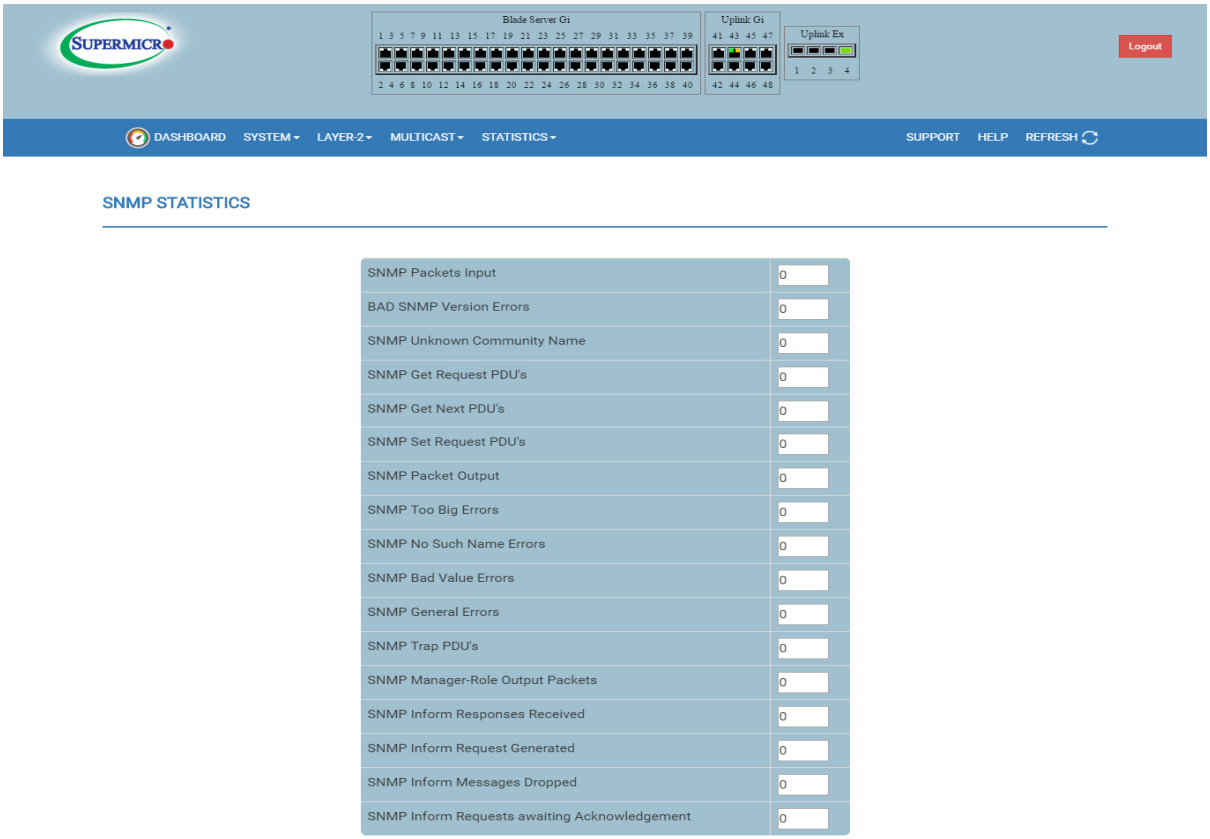


Fig: SNMP Agent

6.9 STP Statistics

6.9.1 RSTP Information

RSTP Information page displays the following RSTP statistics.

Context Id – Context identifier.

Protocol Specification – Protocol specification of the root.

Time Since Topology Change - Number of seconds since topology changed.

Designated Root - Designated root bridge address.

Root Brg Priority - Priority of root bridge.

Root Cost - Cost to root.

Root Port - Index of root port.

Max Age - Max age in seconds.

Hello Time - Hello time in seconds.

Hold Time - Hold time in seconds.

Forward Delay - Forward Delay in seconds.

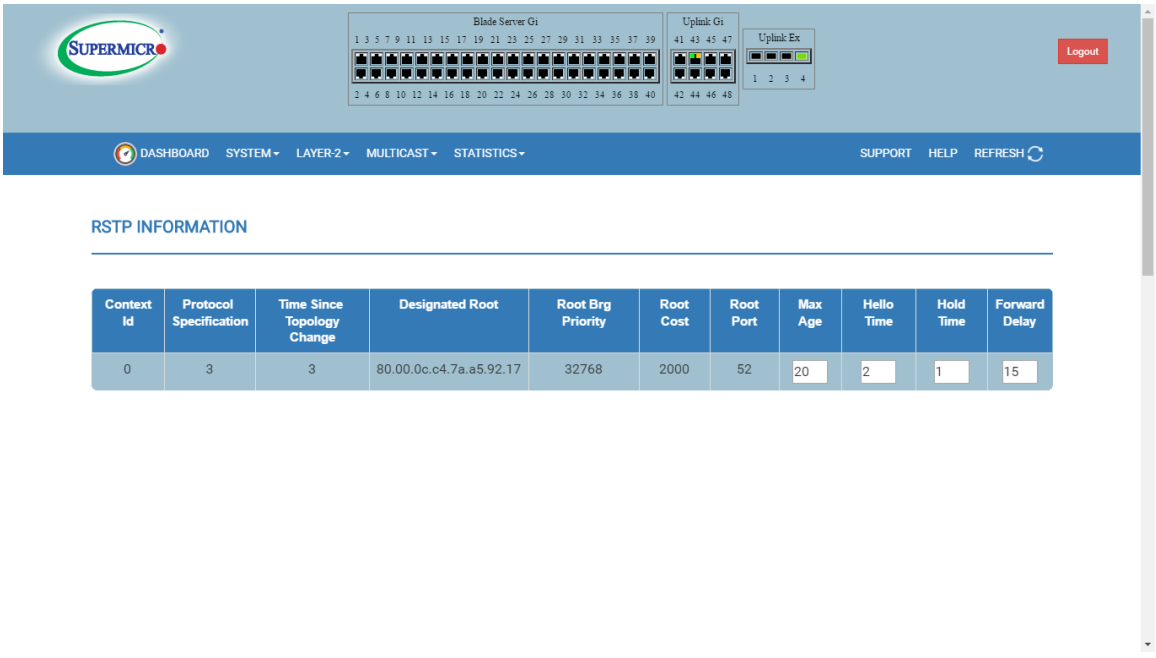


Fig: RSTP Statistics

6.9.2 RSTP Port Statistics

RSTP Port Statistics page displays the following RSTP port level statistics.

Port - Port index.

Received RST BPDUs - Number of RSTP BPDUs received.

Received Configuration BPDUs - Number of config BPDUs received.

Received TCN - Number of topology changed notifications received.

Transmitted RST BPDUs - Number of RSTP BPDUs transmitted.

Transmitted Configuration BPDUs - Number of config BPDUs transmitted.

Transmitted TCN - Number of topology change notifications transmitted.

Received Invalid RST BPDUs - Number of invalid RSTP BPDUs received.

Received Invalid Configuration BPDUs - Number of invalid configuration BPDUs received.

Received Invalid TCN BPDUs - Number of invalid topology change BPDUs received.

Protocol Migration Count - Number of times protocol migration happened.

Effective Port State –Enable or disable state.

EdgePort Oper Status - Operational status of edge port.

Link Type - Broadcast or Point to point.

Reset Statistics button used to set all field values to 0.

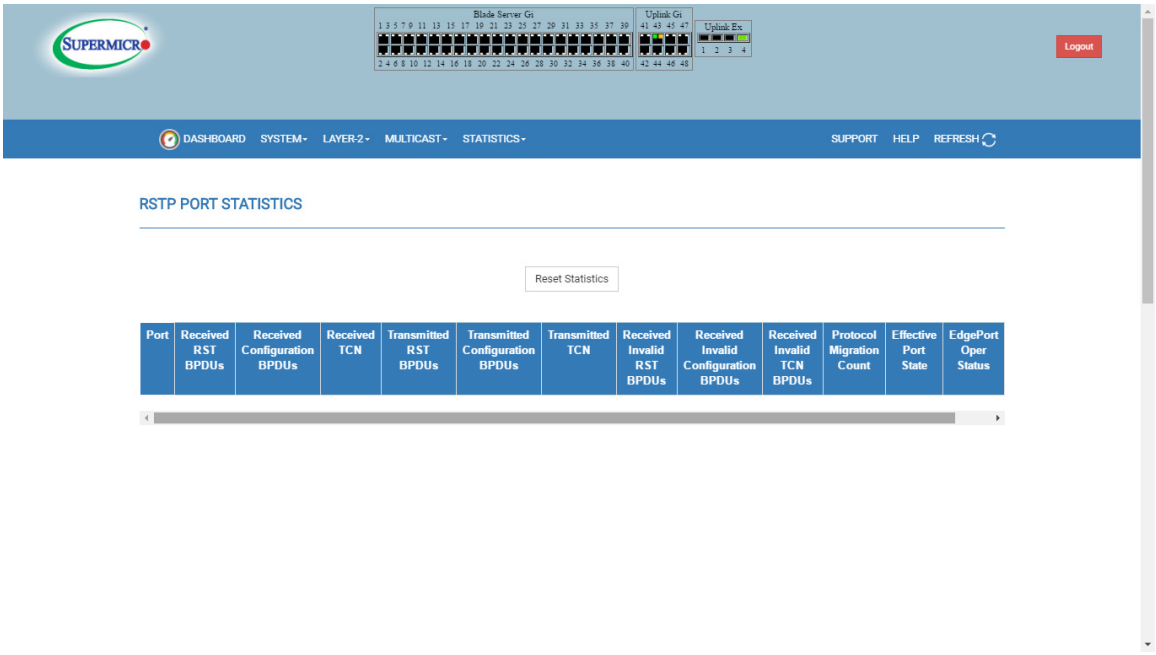


Fig: RSTP Port Statistics

6.9.3 MLAG RSTP Status

MLAG RSTP Status page displays the RSTP information w.r.t MLAG.

Interface - Displays the MLAG Port Channel in switch.

MLAG Role - Displays the MLAG Role as "PRIMARY" or "SECONDARY". MLAG Role was displayed empty, when MLAG not configured.

STP Role - Displays the port's current Role as defined by Spanning Tree Protocol.

State - Displays the port's current state as defined by Spanning Tree Protocol.

Reason - Reason of the interface as "Peer Runs STP" or "MLAG Detected Loop".

- Displays reason as "Peer Runs STP", when MLAG Role is SECONDARY.
- Displays reason as "MLAG Detected Loop", when MLAG Role is PRIMARY and MLAG interface is root blocked.
- Reason does not displayed, when MLAG Role is PRIMARY.

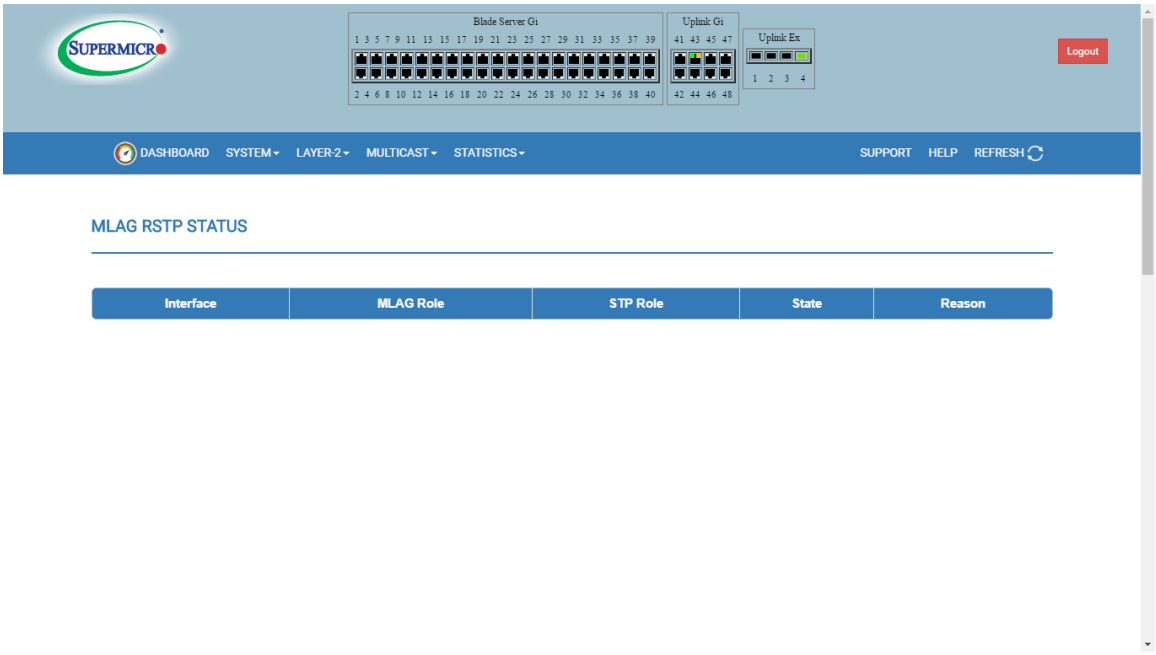


Fig: MLAG RSTP status

MSTP Statistics:

6.9.4 MSTP Information

MSTP Information page displays the following MSTP statistics.

Context Id –Context identifier.

Bridge Address- Address of the bridge.

CIST Root- CIST root address.

Regional Root- Regional root address.

CIST Root Cost- Cost to CIST root.

Regional Root Cost- Cost to regional root.

Root Port - Index of the root port.

Hold Time - Hold time in seconds.

Max Age - Maximum age in seconds.

Forward Delay - Forward delay in seconds.

CIST Time Since Topology Change - Number of seconds since topology last changed.

Topology Changes - Number of topology changes.

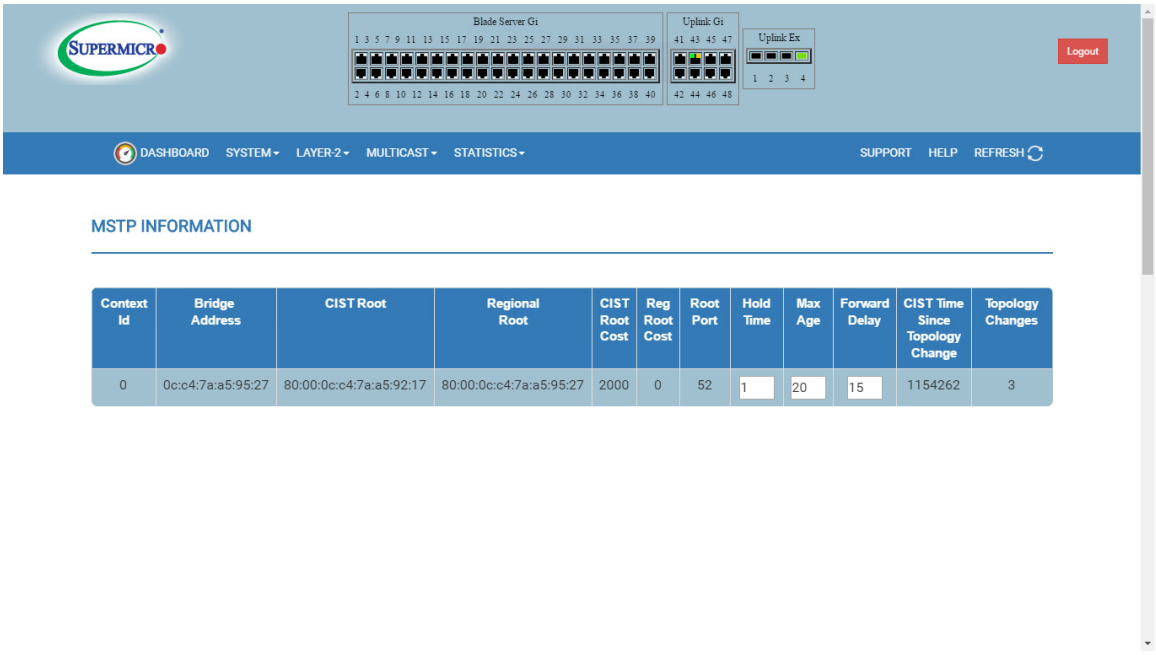


Fig: MSTP Statistics

6.9.5 MSTP CIST Statistics

MSTP CIST Port Statistics page displays the following MSTP CIST port level statistics.

Port –Port index.

Received MST BPDUs - Number of MSTP BPDUs received.

Received RST BPDUs - Number of RSTP BPDUs received.

Received Config BPDUs - Number of config BPDUs received.

Received TCN BPDUs - Number of topology change notification BPDUs received.

Transmitted MST BPDUs - Number of MSTP BPDUs transmitted.

Transmitted RST BPDUs - Number of RSTP BPDUs transmitted.

Transmitted Config BPDUs - Number of config BPDUs transmitted.

Transmitted TCN BPDUs - Number of topology change notification BPDUs transmitted.

Received Invalid MST BPDUs - Number of invalid MSTP BPDUs received.

Received Invalid RST BPDUs - Number of invalid RSTP BPDUs received.

Received Invalid Config BPDUs - Number of invalid config BPDUs received.

Received Invalid TCN BPDUs - Number of invalid TCN BPDUs received.

Protocol Migration Count - Number of times protocol migration happened.

Reset Statistics button used to set all field values to 0.

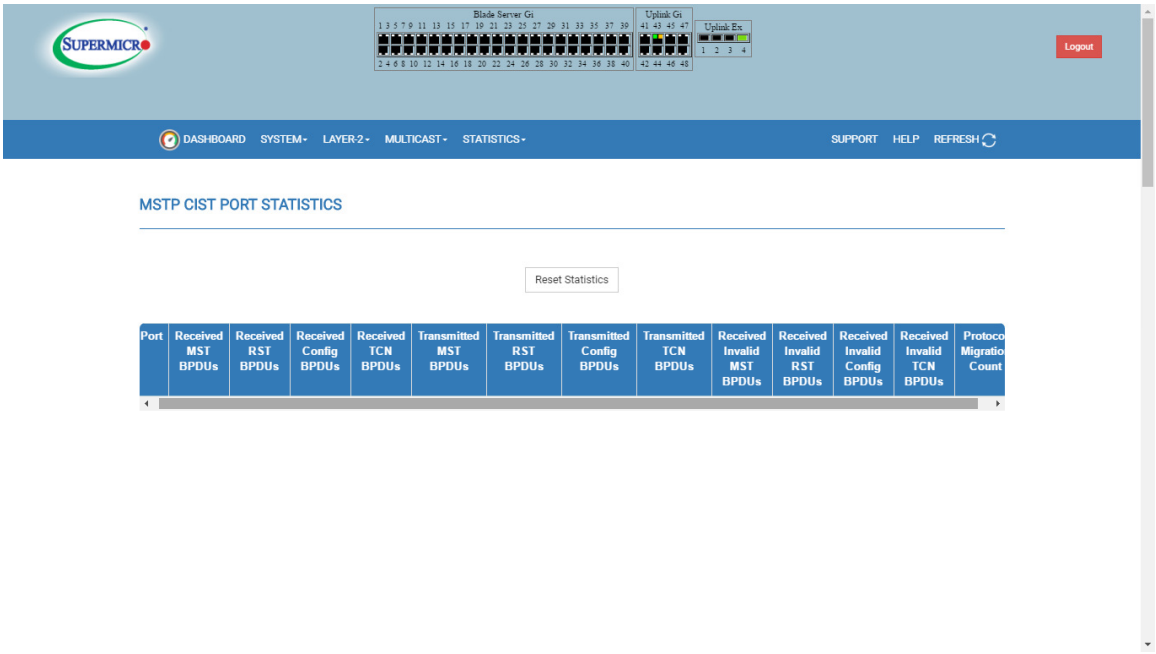


Fig: MSTP CIST Port Statistics

6.9.6 MSTP MSTI Port Statistics

MSTP MSTI Port Statistics page displays the following MSTP MSTI port level statistics.

Instance - MSTP instance Identifier.

Port - Port index.

Designated Root - Designated root bridge address.

Designated Bridge - Designated Bridge address.

Designated Port - Index of designated port for this MSTP instance.

State - Current state.

Forward Transitions- Number of forward transitions.

Received BPDUs - Number of BPDUs received.

Transmitted BPDUs - Number of BPDUs transmitted.

Invalid Received BPDUs - Number of invalid BPDUs received.

Designated Cost- Cost to designated root.

Role - Current role.

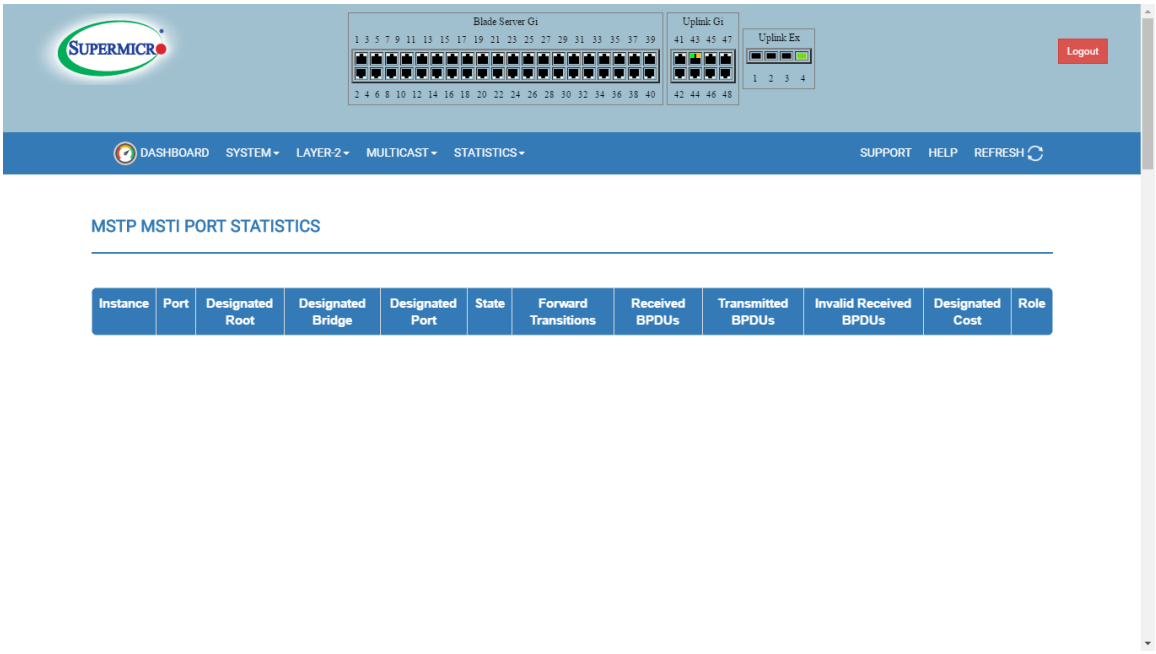


Fig: MSTP MSTI Port statistics

6.9.7 MLAG MSTP Status

MLAG MSTP Status page displays the MSTP information w.r.t MLAG.

Interface - Displays the MLAG Port Channel in switch.

MLAG Role - Displays the MLAG Role as "PRIMARY" or "SECONDARY". MLAG Role was displayed empty, when MLAG not configured.

STP Role - Displays the port's current Role as defined by Spanning Tree Protocol.

State - Displays the port's current state as defined by Spanning Tree Protocol.

Reason - Reason of the interface as "Peer Runs STP" or "MLAG Detected Loop".

- Displays reason as "Peer Runs STP", when MLAG Role is SECONDARY.
- Displays reason as "MLAG Detected Loop", when MLAG Role is PRIMARY and MLAG interface is root blocked.
- Reason does not displayed, when MLAG Role is PRIMARY.

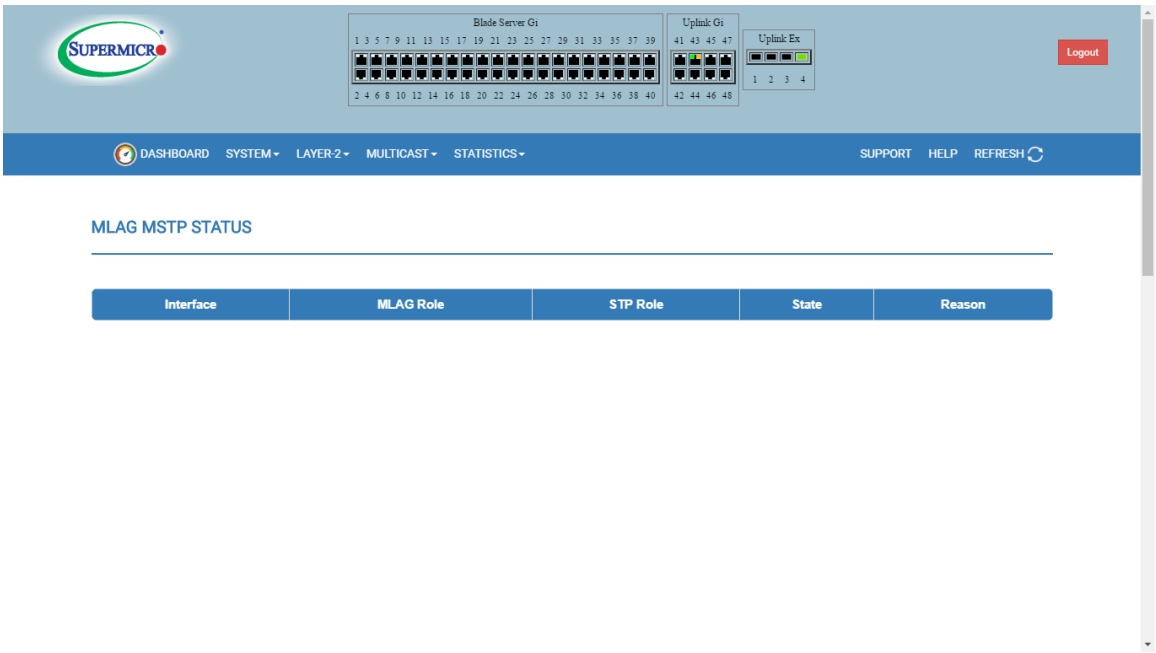


Fig: MLAG MSTP status

6.10 LLDP Statistics

6.10.1 LLDP Statistics

LLDP statistics page displays the LLDP statistics information.

Remote Table Last Change Time – The time since the last time remote LLDP information table got changed.

Remote Table Inserts – Number of inserts happened on remote information table.

Remote Table Deletes – Number of deletes happened on remote information table.

Remote Table Drops – Number of drops happened on remote information table.

Remote Table Ageouts – Number of ageouts happened on remote information table.

Remote Table Updates – Number of times remote information table got updated.

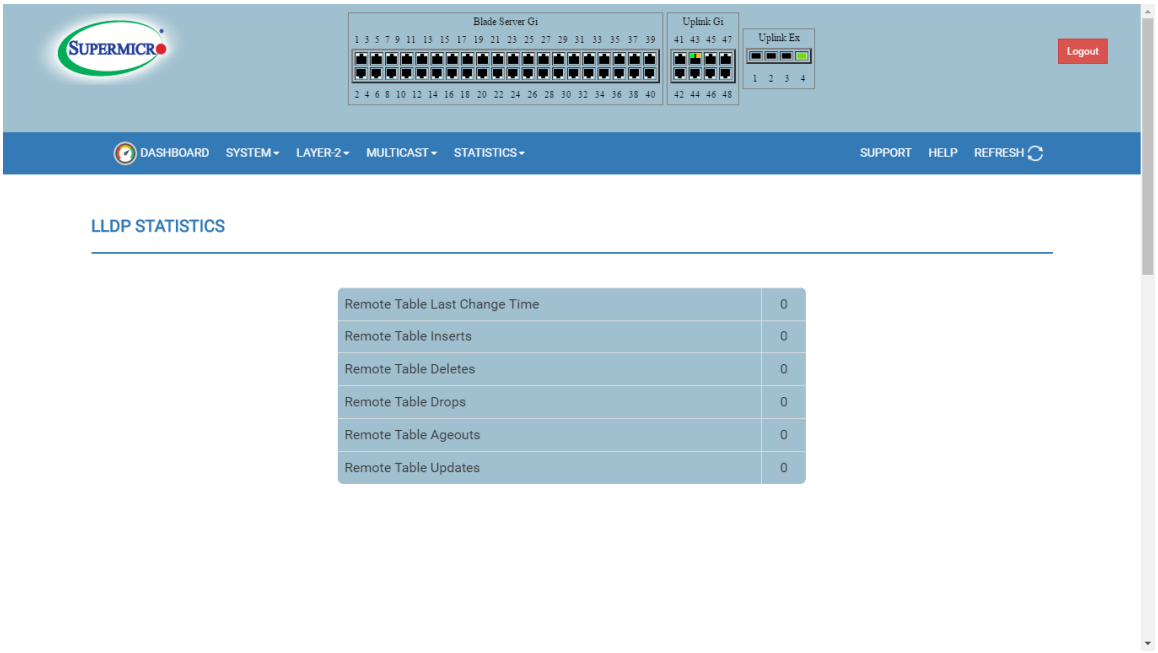


Fig: LLDP Statistics

6.10.2 LLDP Errors

LLDP Errors page displays the LLDP error information.

Total Memory Allocation Failures- The number of memory allocation failed in LLDP feature.

Total Input Queue Overflows- The number of times the LLDP input queue overflowed. **Total Table Overflows –** The number of times the LLDP remote table got overflowed.

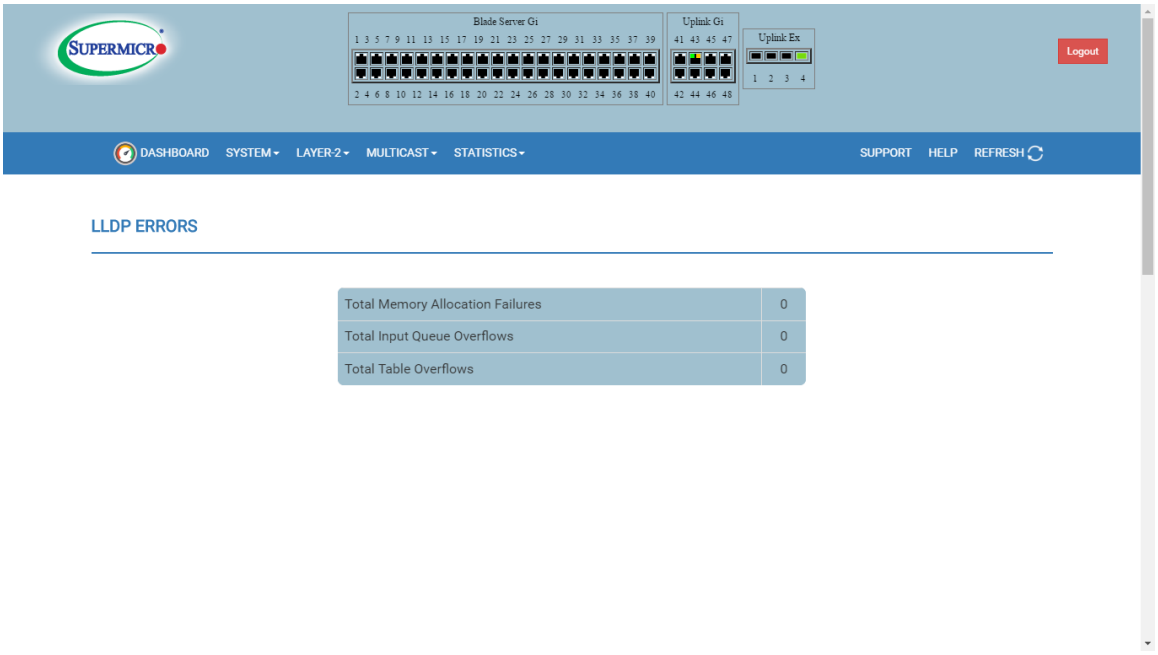


Fig: LLDP Errors

6.10.3 LLDP Neighbors

LLDP Neighbors page displays the LLDP neighbor information.

Neighbor List table has Interface and Chassis Id.

Interface - Interface name on which this neighbor is learned.

Chassis Id - The value of the chassis identifier.

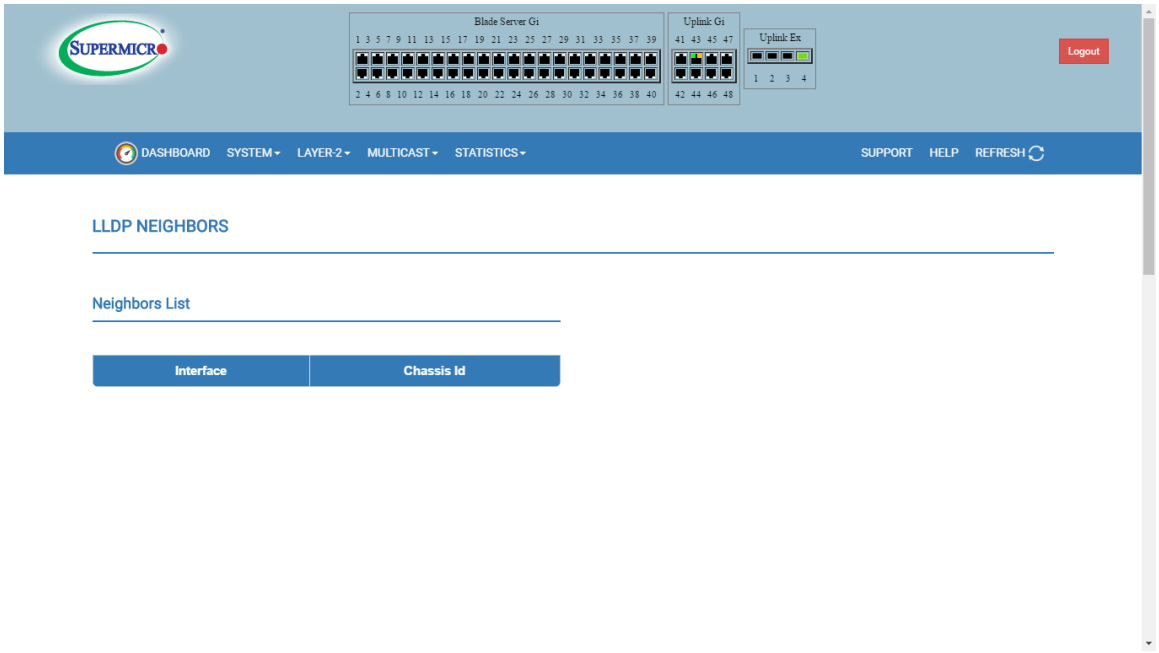


Fig:LLDP Neighbors

6.10.4 LLDP Traffic

LLDP Traffic page displays the LLDP traffic information.

Total Frames Out - The number of LLDP packets sent out from switch in all interfaces.

Total Entries Aged - The number of LLDP neighbor entries aged out.

Total Frames In - The number of LLDP packets received in by switch in all interfaces.

Total Frames Received In Error - The number of LLDP packets received with Error.

Total Frames Discarded - The number of LLDP packets discarded due to error and other failure conditions.

Total TLVS Unrecognized - The number of TLVs received could not recognized properly.

Total TLVs Discarded - The number of TLVs discarded due to invalidity.

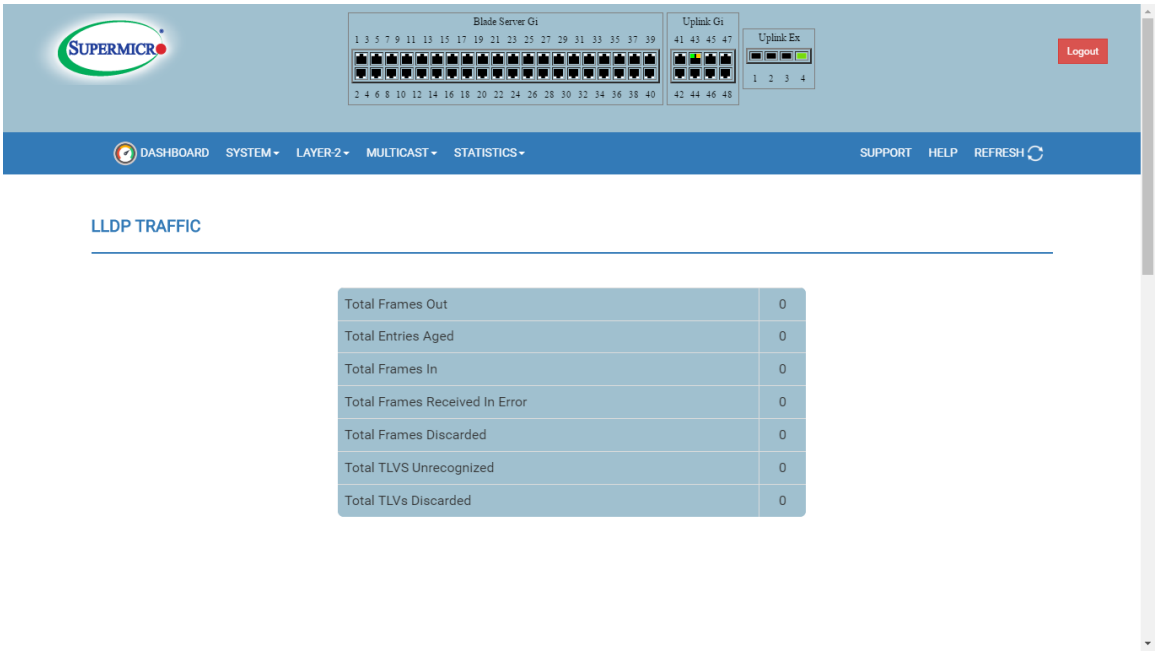


Fig : LLDP Traffic

6.10.5 LLDP Interface Traffic

LLDP Interface Traffic page displays the LLDP interface traffic information.

Interface – Interface index.

Total Frames Out - The number of LLDP packets sent out from switch in all interfaces.

Total Entries Aged - The number of LLDP neighbor entries aged out.

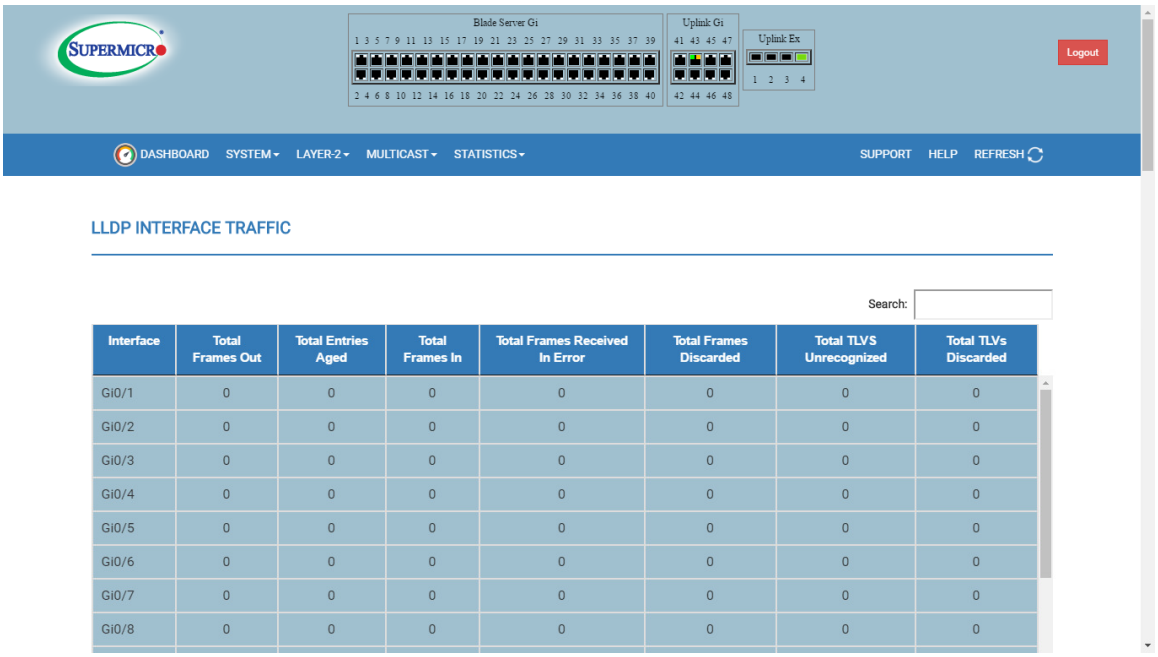
Total Frames In - The number of LLDP packets received in by switch in all interfaces.

Total Frames Received In Error - The number of LLDP packets received with Error.

Total Frames Discarded - The number of LLDP packets discarded due to error and other failure conditions.

Total TLVS Unrecognized - The number of TLVs received could not recognized properly.

Total TLVs Discarded - The number of TLVs discarded due to invalidity.



Interface	Total Frames Out	Total Entries Aged	Total Frames In	Total Frames Received In Error	Total Frames Discarded	Total TLVS Unrecognized	Total TLVs Discarded
Gi0/1	0	0	0	0	0	0	0
Gi0/2	0	0	0	0	0	0	0
Gi0/3	0	0	0	0	0	0	0
Gi0/4	0	0	0	0	0	0	0
Gi0/5	0	0	0	0	0	0	0
Gi0/6	0	0	0	0	0	0	0
Gi0/7	0	0	0	0	0	0	0
Gi0/8	0	0	0	0	0	0	0

Fig: LLDP Interface Traffic

6.11 IGMP Snooping Statistics

6.11.1 IGMP Snooping Clear statistics

IGMP Snooping Clear Statistics page helps clearing IGMP snooping statistics.

Clear Vlan Counters has two option “All” and “Vlan ID”. User can choose any one of the option to clear IGMP statistics.

All - Option to clear all the IGMP statistics.

Vlan ID - Option to clear IGMP statistics for particular VLAN.

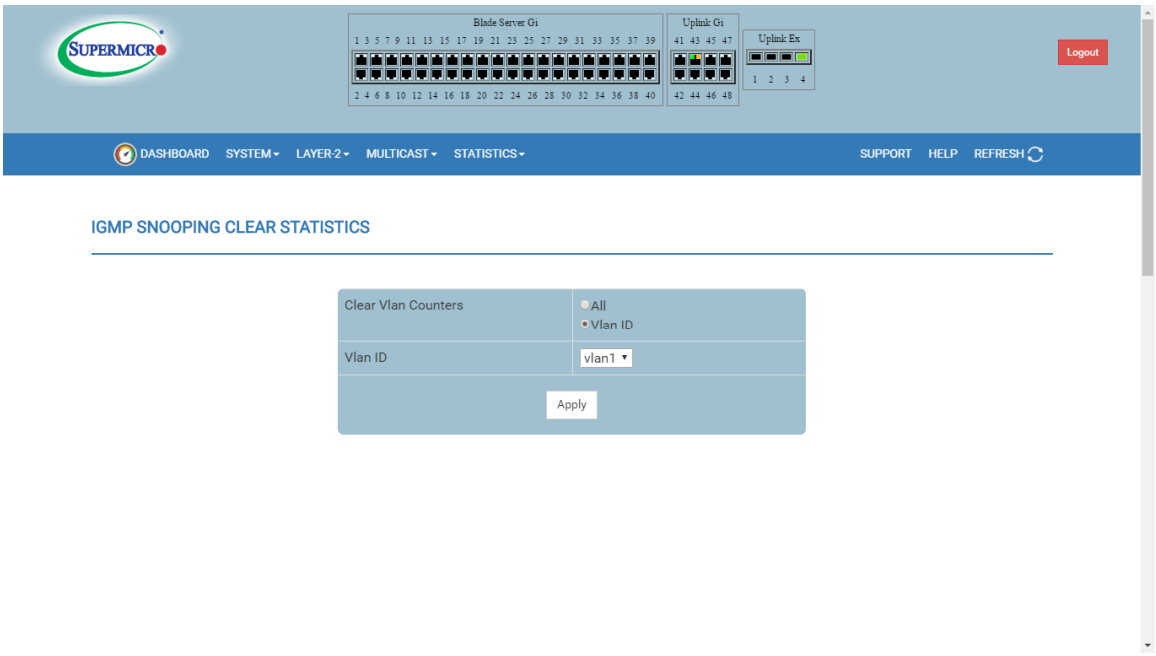


Fig: IGMP Snooping clear statistics

6.11.2 IGMP Snooping V1/V2 Statistics

IGMP Snooping V1/V2 Statistics page displays the following IGMP snooping statistics.

VLAN ID - VLAN identifier.

General Queries Received - Number of general query packets received

Group Queries Received - Number of group query packets received

Group and Source Queries Received - Number of group and source query packets received

IGMP Reports Received - Number of IGMP report packets received

IGMP Leaves Received - Number of IGMP leave packets received

IGMP Packets Dropped - Number of IGMP packets dropped

General Queries Transmitted - Number of general query packets transmitted

Group Queries Transmitted - Number of group query packets transmitted

IGMP Reports Transmitted - Number of IGMP report packets transmitted

IGMP Leaves Transmitted - Number of IGMP leave packets transmitted

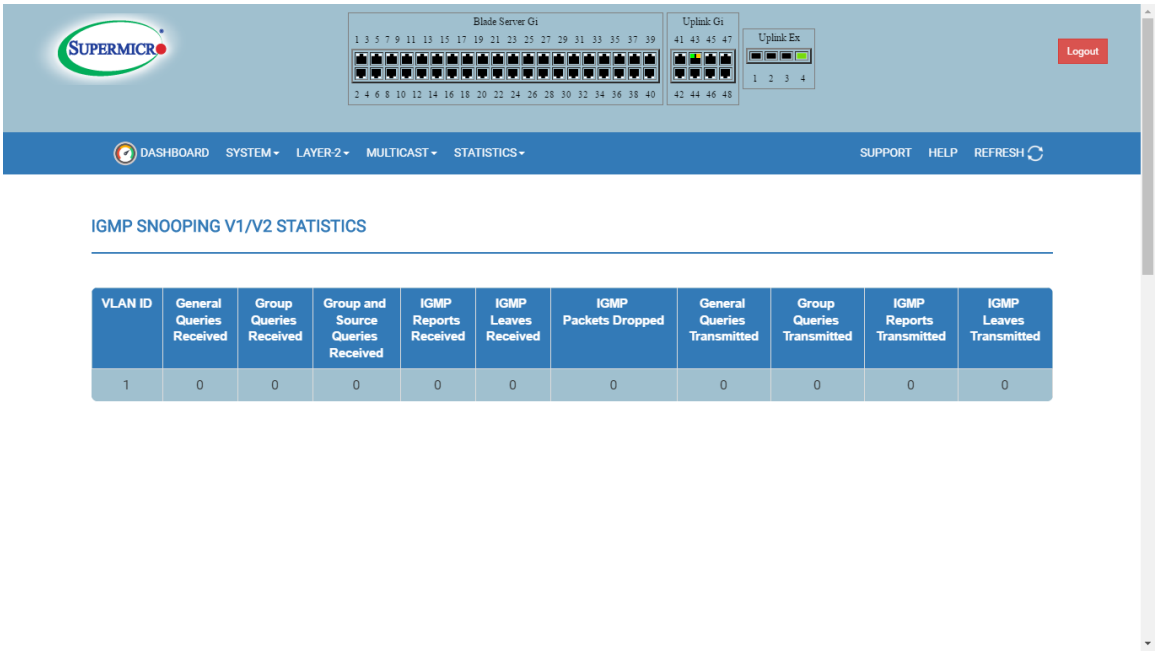


Fig: IGMP Snooping V1/V2 statistics

6.11.3 IGMP Snooping V3 statistics

IGMP Snooping V3 Statistics page displays the following statistics information.

VLAN ID - VLAN identifier.

V3 Reports Received - Number of Reports messages received

IS_INCL Messages Received - Number of messages received with is include field

IS_EXCL Messages Received - Number of messages received with is exclude field

TO_INCL Messages Received - Number of messages received with to include field

TO_EXCL Messages Received - Number of messages received with to exclude field

ALLOW Messages Received - Number of allow messages received

BLOCK Messages Received - Number of block messages received

V3 Reports Sent - Number of V3 reports transmitted

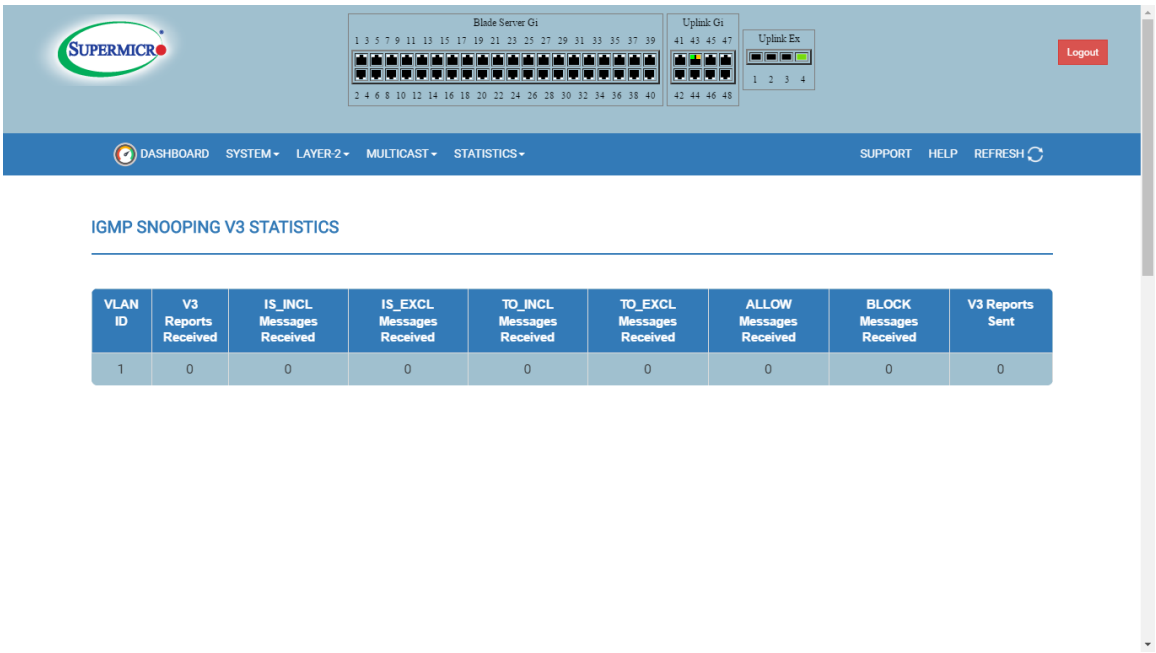


Fig: IGMP Snooping V3 Statistics

6.11.4 MLAG IGMP Snooping MAC Table

MLAG IGMP Snooping MAC Table page displays the following snooping information.

VLAN ID - VLAN identifier.

Group MAC - Displays the Group MAC address that is learnt.

Receiver Ports - Displays the learnt port or port list.

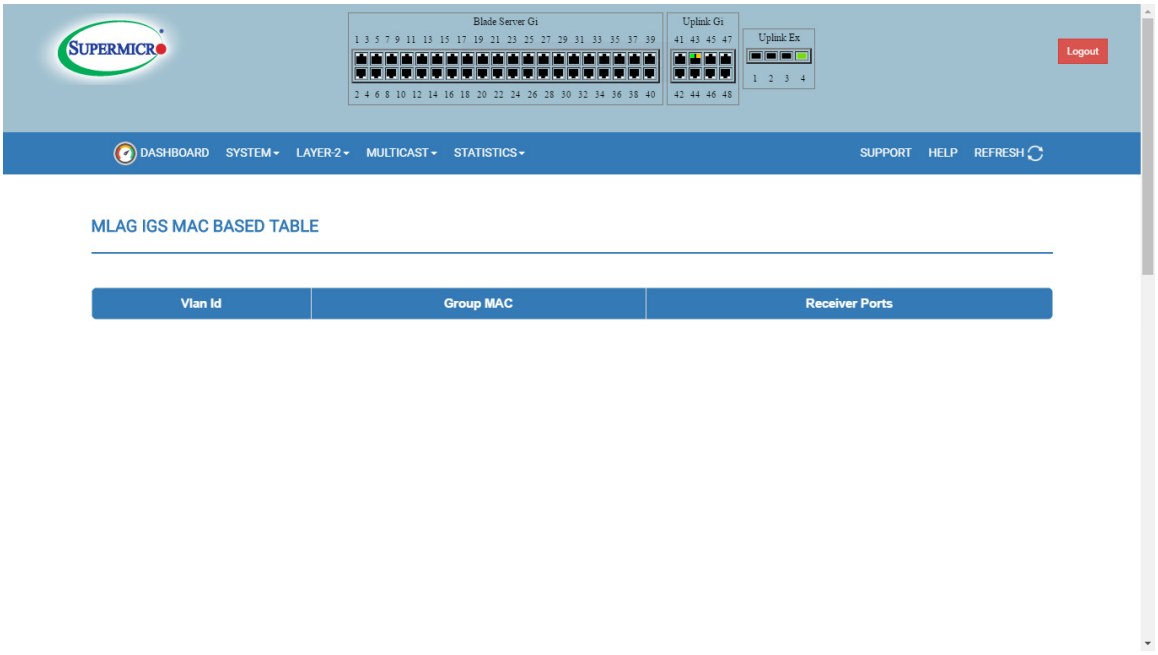


Fig: MLAG IGS Mac Table