



ADMINISTRATION GUIDE

Cisco Small Business

SFE/SGE Managed Switches



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

| | |
|--|-----------|
| Chapter 1: Getting Started | 1 |
| Starting the Application | 1 |
| Understanding the Interface | 3 |
| Using the Cisco Management Buttons | 5 |
| Using Screen and Table Options | 5 |
| Adding Device Information | 5 |
| Modifying Device Information | 6 |
| Deleting Device Information | 7 |
| Logging Off of the Device | 7 |
| The About Page | 7 |
| Chapter 2: Managing Device Information | 9 |
| Defining System Information | 9 |
| Managing Stacking | 11 |
| Understanding Switch Operating Modes | 11 |
| Configuring a Stack | 12 |
| Stack Membership | 14 |
| Defining Stacking Unit ID | 15 |
| Adding, Replacing and Removing Stacking Members — Examples | 21 |
| Managing Stacks | 23 |
| Viewing Device Health | 25 |
| Resetting the Device | 26 |
| Defining Bonjour | 27 |
| Disabling Bonjour | 29 |
| TCAM Utilization | 30 |
| Chapter 3: Configuring System Time | 33 |
| Defining System Time | 33 |
| Defining SNTP Settings | 36 |

| | |
|---|-----------|
| Defining SNMP Authentication | 39 |
| Chapter 4: Configuring Device Security | 41 |
| Passwords Management | 41 |
| Modifying the Local User Settings | 43 |
| Defining Authentication | 44 |
| Defining Profiles | 44 |
| Modifying an Authentication Profile | 47 |
| Mapping Authentication Profiles | 48 |
| Defining TACACS+ | 50 |
| Defining RADIUS | 55 |
| Defining Access Methods | 60 |
| Defining Access Profiles | 61 |
| Defining Profile Rules | 65 |
| Defining Traffic Control | 72 |
| Defining Storm Control | 73 |
| Defining Port Security | 76 |
| Defining 802.1X | 80 |
| Defining 802.1X Properties | 81 |
| Defining Port Authentication | 82 |
| Defining Authentication | 87 |
| Defining Authenticated Hosts | 91 |
| Defining Access Control | 92 |
| Defining MAC Based ACL | 92 |
| Defining IP Based ACL | 100 |
| Defining IPv6 Based ACLs | 112 |
| Defining ACL Binding | 121 |
| Defining DoS Prevention | 123 |
| DoS Global Settings | 123 |
| Defining Martian Addresses | 125 |
| Defining DHCP Snooping | 127 |

| | |
|---|-----|
| Defining DHCP Snooping Properties | 128 |
| Defining DHCP Snooping on VLANs | 129 |
| Defining Trusted Interfaces | 130 |
| Binding Addresses to the DHCP Snooping Database | 132 |
| Defining IP Source Guard | 135 |
| Defining Dynamic ARP Inspection | 141 |
| Defining ARP Inspection Properties | 142 |
| Defining ARP Inspection Trusted Interfaces | 144 |
| Defining ARP Inspection List | 146 |
| Assigning ARP Inspection VLAN Settings | 148 |

Chapter 5: Configuring Ports 151

| | |
|--|-----|
| Configuring Ports Settings for Layer 2 Enabled Devices | 151 |
| Configuring Ports Settings for Layer 3 Enabled Devices | 157 |

Chapter 6: Configuring VLANs 163

| | |
|------------------------------------|-----|
| Defining VLAN Properties | 164 |
| Modifying VLANs | 166 |
| Defining VLAN Membership | 167 |
| Modifying VLAN Membership | 169 |
| Assigning Ports to Multiple VLANs | 170 |
| Defining GVRP Settings | 173 |
| Modifying GVRP Settings | 174 |
| Defining VLAN Interface Settings | 176 |
| Modifying VLAN Interface Settings | 178 |
| Defining Customer VLANs Using QinQ | 180 |
| Defining Multicast TV VLAN | 181 |
| Defining CPE VLAN Mapping | 183 |
| Defining Protocol Groups | 184 |
| Defining a Protocol Port | 187 |

| | |
|--|------------|
| Chapter 7: Configuring IP Information | 190 |
| IP Addressing | 190 |
| Managing IPv6 | 190 |
| Viewing IPv6 Routes Table | 203 |
| Layer 2 IP Addressing | 204 |
| Layer 3 IP Addressing | 204 |
| Defining IPv4 Interface (Layer 2) | 205 |
| Defining IPv4 Interface (Layer 3) | 206 |
| Enabling ARP Proxy (Layer 3) | 209 |
| Defining UDP Relay (Layer 3) | 210 |
| Defining DHCP Relay (Layer 2) | 212 |
| Defining DHCP Relay Interfaces | 214 |
| Defining DHCP Relay (Layer 3) | 216 |
| ARP | 218 |
| Defining IP Routing | 221 |
| Domain Name System | 224 |
| Defining DNS Servers | 224 |
| Mapping DNS Hosts | 226 |
| Chapter 8: Defining Address Tables | 230 |
| Defining Static Addresses | 230 |
| Defining Dynamic Addresses | 233 |
| Chapter 9: Configuring Multicast Forwarding | 235 |
| IGMP Snooping | 235 |
| Modifying IGMP Snooping | 237 |
| Defining Multicast Group | 238 |
| Modifying a Multicast Group | 240 |
| Configuring IGMP Snooping Mapping | 242 |
| Defining Multicast TV Membership | 243 |
| Defining Multicast Forwarding | 244 |

| | |
|---|------------|
| Modifying Multicast Forwarding | 245 |
| Defining Unregistered Multicast Settings | 246 |
| Chapter 10: Configuring Spanning Tree | 249 |
| Defining Spanning Tree | 249 |
| Defining STP Properties | 249 |
| Defining Spanning Tree Interface Settings | 252 |
| Modifying Interface Settings | 256 |
| Defining Rapid Spanning Tree | 258 |
| Modifying RTSP | 261 |
| Defining Multiple Spanning Tree | 263 |
| Defining MSTP Properties | 263 |
| Defining MSTP Instance to VLAN | 265 |
| Defining MSTP Instance Settings | 266 |
| Defining MSTP Interface Settings | 267 |
| Chapter 11: Configuring Quality of Service | 273 |
| Defining General Settings | 274 |
| Defining CoS | 274 |
| Defining QoS Queue | 276 |
| Mapping CoS to Queue | 278 |
| Mapping DSCP to Queue | 279 |
| Configuring Bandwidth | 280 |
| Configuring VLAN Rate Limit | 282 |
| Defining Advanced QoS Mode | 285 |
| Configuring DSCP Mapping | 286 |
| Defining Class Mapping | 288 |
| Defining Aggregate Policer | 290 |
| Configuring Policy Table | 293 |
| Defining Policy Binding | 297 |
| Defining QoS Basic Mode | 299 |
| Rewriting DSCP Values | 300 |

| | |
|---|----------------|
| Chapter 12: Configuring SNMP | 302 |
| Configuring SNMP Security | 303 |
| Defining the SNMP Engine ID | 303 |
| Defining SNMP Views | 305 |
| Defining SNMP Users | 307 |
| Defining SNMP Groups | 310 |
| Defining SNMP Communities | 314 |
| Defining Trap Management | 319 |
| Defining Trap Settings | 319 |
| Configuring Station Management | 320 |
| Defining SNMP Filter Settings | 327 |
| Chapter 13: Managing System Files | 329 |
| Firmware Upgrade | 330 |
| Save Configuration | 331 |
| Copy Files | 333 |
| Active Image | 335 |
| Chapter 14: Managing Power-over-Ethernet Devices | 336 |
| Defining PoE Settings | 336 |
| Chapter 15: Managing Device Diagnostics | 340 |
| Viewing Integrated Cable Tests | 340 |
| Performing Optical Tests | 344 |
| Configuring Port Mirroring | 345 |
| Modifying Port Mirroring | 347 |
| Viewing CPU Utilization | 348 |
| Chapter 16: Managing System Logs | 350 |
| Enabling System Logs | 350 |
| Viewing the Device Memory Logs | 352 |

| | |
|----------------------------------|-----|
| Clearing Message Logs | 353 |
| Viewing the Flash Logs | 353 |
| Clearing Flash Logs | 354 |
| Viewing Remote Logs | 355 |
| Modifying Syslog Server Settings | 358 |

Chapter 17: Viewing Statistics 361

| | |
|---------------------------------------|-----|
| Viewing Ethernet Statistics | 361 |
| Defining Ethernet Interface | 361 |
| Viewing Etherlike Statistics | 363 |
| Viewing GVRP Statistics | 365 |
| Viewing EAP Statistics | 367 |
| Managing RMON Statistics | 369 |
| Viewing RMON Statistics | 370 |
| Resetting RMON Statistics Counters | 372 |
| Configuring RMON History | 372 |
| Defining RMON History Control | 372 |
| Viewing the RMON History Table | 375 |
| Defining RMON Events Control | 377 |
| Viewing the RMON Events Logs | 380 |
| Defining RMON Alarms | 381 |
| Managing QoS Statistics | 387 |
| Viewing Policer Statistics | 387 |
| Viewing Aggregated Policer Statistics | 389 |
| Viewing Queues Statistics | 389 |

Chapter 18: Aggregating Ports 393

| | |
|-------------------------|-----|
| Defining LAG Management | 394 |
| Defining LAG Settings | 396 |
| Configuring LACP | 400 |

Getting Started

This section provides an introduction to the user interface, and includes the following topics:

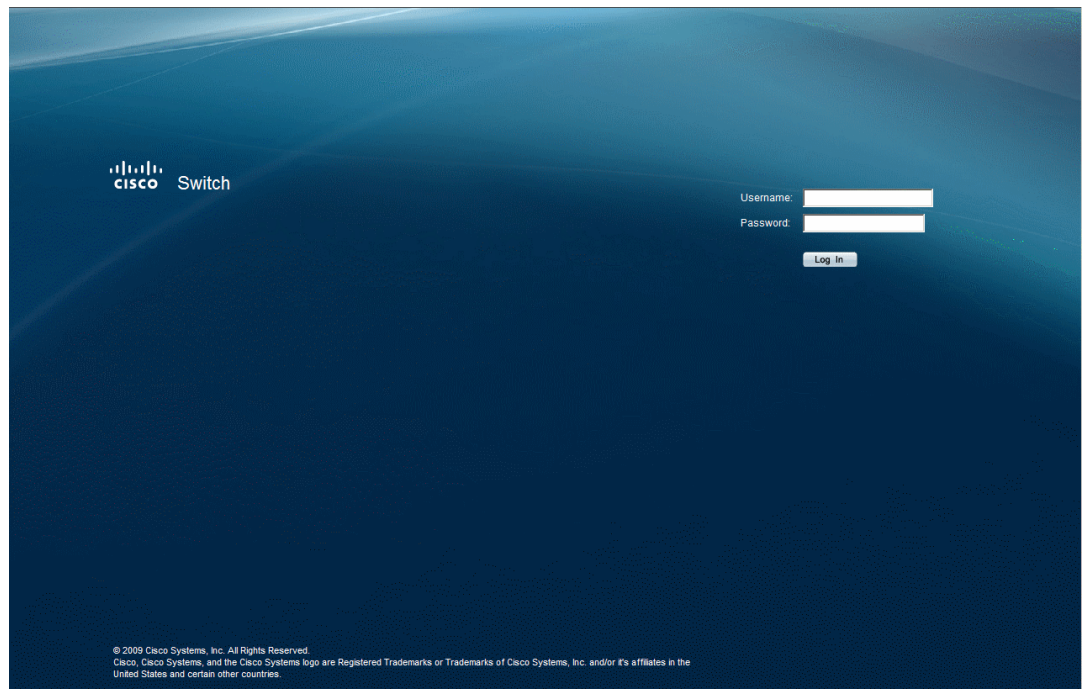
- Starting the Application
- Understanding the Interface
- Using the Cisco Management Buttons
- Using Screen and Table Options
- Logging Off of the Device
- The About Page

Starting the Application

To open the User Interface:

-
- STEP 1** Open a web browser.
- STEP 2** Enter the device's IP address in the address bar and press **Enter**. An *Enter Network Password Page* opens:

Enter Network Password Page



© 2009 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are Registered Trademarks or Trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

STEP 3 When the *Enter Network Password Page* initially loads, both fields are empty. Enter a Username and Password and click **Log In**. The default user name is *admin*. The default password is *admin*. Passwords are alpha-numeric and case-sensitive.

While the system is verifying the login attempt, the Login Progress Indicator appears. The indicator dots rotate clockwise to indicate that the system is still working.

If the login attempt is successful, the *System Information Page* opens.

System Information Page

Small Business
SGE2000P 48-port 10/100/1000 Ethernet Switch

System Information (SGE2010)

Model Name: 48-port 10/100/1000 Ethernet Switch

System Name:

System Location:

System Contact:

System Object ID: 1.3.6.1.4.1.9.6.1.72.2010.2

System Up Time: 3 days, 22 hours, 18 minutes, 32 seconds

Base MAC Address: 00:54:bd:12:a8:32

Switch Operation Mode After Reset: ☐ Standalone ☒ Stack

Jumbo Frame: ☐ Enable ☒ Disable

| Unit No. | Model Name | Hardware Version | Boot Version | Software Version |
|----------|------------|------------------|--------------|------------------|
| 1 | SGE2010 | 00.00.01 | 2.0.0.00 | 3.0.0.4 |
| 2 | SGE2000P | 00.00.10 | 1.0.0.05 | 3.0.0.4 |

Apply

© 2009 Cisco Systems, Inc. All rights reserved

If the login attempt fails because the user typed an incorrect username or password, the following message appears: “Invalid Username or Password. Please try again.”

If the login attempt fails due to another problem one of the following error messages appears:

“Login failed since too many users are logged in.”

“Login failed due to PC configuration problems.”

“There is no response from the server.”

Understanding the Interface

The *Interface Components Page* displays the interface components with their corresponding numbers.

Interface Components Page

System Information (SGE2010)

| Unit No. | Model Name | Hardware Version | Boot Version | Software Version |
|----------|------------|------------------|--------------|------------------|
| 1 | SGE2010 | 00.00.01 | 2.0.0.00 | 3.0.0.4 |
| 2 | SGE2000P | 00.00.10 | 1.0.0.05 | 3.0.0.4 |

© 2009 Cisco Systems, Inc. All rights reserved

The following table lists the interface components with their corresponding numbers:

Interface Components

Component

Description

1 Tree View

The Tree View provides easy navigation through the configurable device features. The main branches expand to provide the subfeatures.

2 Device View

The device view provides information about device ports, current configuration and status, table information, and feature components. The device view also displays other device information and dialog boxes for configuring parameters.

3 Device Information Area

The Device Information area displays some basic information regarding the device and the configuration.

Using the Cisco Management Buttons

Device Management buttons provide an easy method of configuring device information, and include the following:

Device Management Buttons

| Button Name | Description |
|----------------|-------------------------------|
| Apply | Applies changes to the device |
| Clear Counters | Clears statistic counters |
| Clear Logs | Clears log files |
| Add | Opens an Add page |
| Delete | Removes entries from tables |
| Test | Performs cable tests |

Using Screen and Table Options

The User Interface contains screens and tables for configuring devices. This section contains the following topics:

- Adding Device Information
- Modifying Device Information
- Deleting Device Information

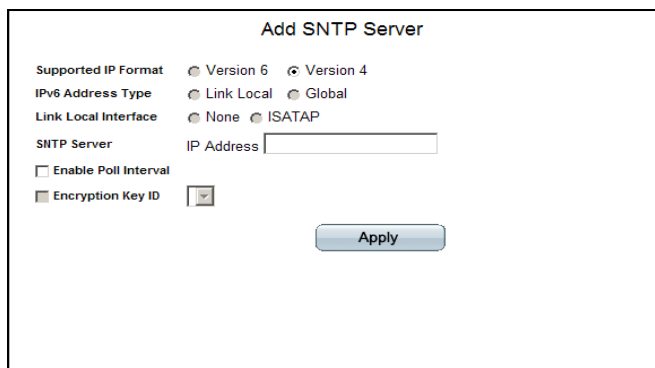
Adding Device Information

User defined information can be added to specific interface pages, by opening a new Add page. To add information to tables or interface pages:

STEP 1 Open an interface page.

STEP 2 Click the **Add** button. An add page opens, for example, the *Add SNMP Server Page*.

Add SNTP Server Page



The screenshot shows the 'Add SNTP Server' configuration page. It includes the following fields and options:

- Supported IP Format:** Radio buttons for Version 6 and Version 4 (selected).
- IPv6 Address Type:** Radio buttons for Link Local and Global.
- Link Local Interface:** Radio buttons for None and ISATAP.
- SNTP Server:** A text input field for the IP Address.
- Enable Poll Interval:** A checkbox.
- Encryption Key ID:** A dropdown menu.
- Apply:** A button at the bottom right.

STEP 3 Define the fields.

STEP 4 Click **Apply**. The configuration information is saved, and the device is updated.

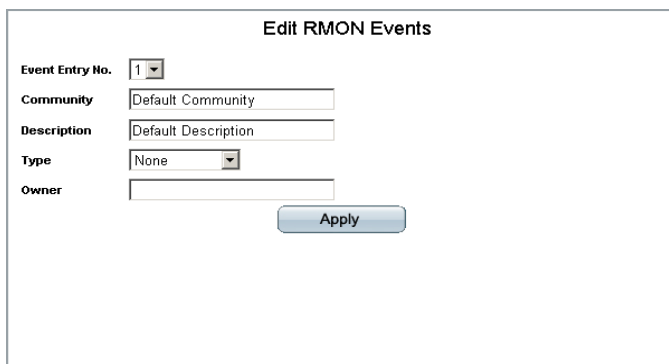
Modifying Device Information

STEP 1 Open the interface page.

STEP 2 Select a table entry.

STEP 3 Click the **Edit** Button. A Modify page opens, for example, the *Edit RMON Events Page* opens:

Edit RMON Events Page



The screenshot shows the 'Edit RMON Events' configuration page. It includes the following fields and options:

- Event Entry No.:** A dropdown menu with '1' selected.
- Community:** A text input field with 'Default Community'.
- Description:** A text input field with 'Default Description'.
- Type:** A dropdown menu with 'None' selected.
- Owner:** A text input field.
- Apply:** A button at the bottom right.

STEP 4 Define the fields.

STEP 5 Click **Apply**. The fields are modified, and the information is saved to the device.

Deleting Device Information

-
- STEP 1** Open the interface page.
 - STEP 2** Select a table row.
 - STEP 3** Check the Remove checkbox.
 - STEP 4** Click the Delete button. The information is deleted, and the device is updated.
-

Logging Off of the Device

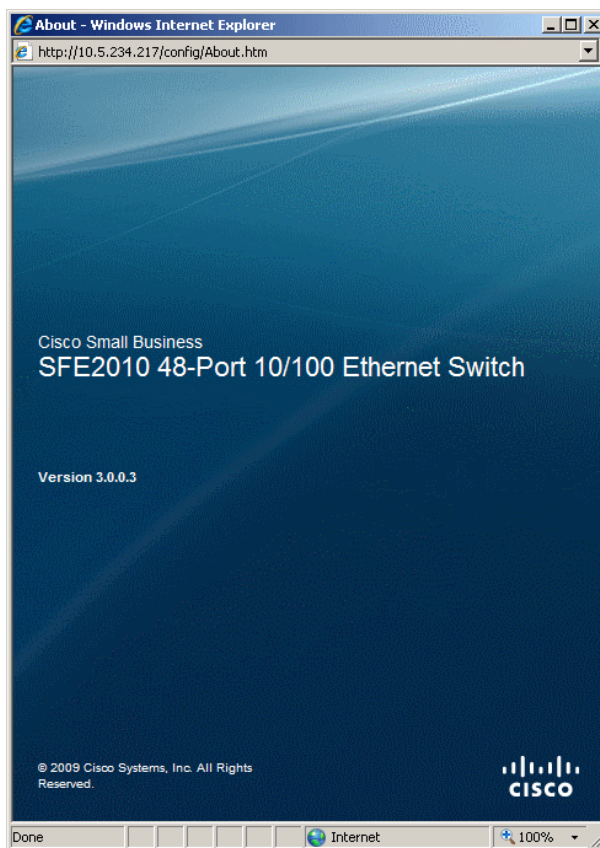
The application may automatically log out after ten minutes. When this occurs, the following message is displayed “You have been logged out as a result of being inactive for 10 minutes. Use the fields to login.” The *Enter Network Password Page* opens and, after login, the application returns to the *System Information Page*. In all logout instances, a message is displayed on the *Enter Network Password Page* to indicate the logged-out state.

To intentionally log out, click **Logout** in the top right corner of any screen. The system logs out and the following message appears: “You have logged out of the Cisco Unified Managed Switch

The About Page

Click **About** in the top right corner of any screen to display *The About Page*. This page displays the device name and version number.

The About Page



Managing Device Information

This section provides information for defining both basic and advanced system information. This section contains the following topics:

- Defining System Information
- Managing Stacks
- Viewing Device Health
- Resetting the Device
- Defining Bonjour
- TCAM Utilization

Defining System Information

The *System Information Page* contains parameters for configuring general device information.

To open the *System Information Page*:

- STEP 1** Click **System > System Management > System Information**. The *System Information Page* opens:

System Information Page

Small Business
SGE2000P 48-port 10/100/1000 Ethernet Switch

System Information (SGE2010)

Model Name: 48-port 10/100/1000 Ethernet Switch

System Name:

System Location:

System Contact:

System Object ID: 1.3.6.1.4.1.9.6.1.72.2010.2

System Up Time: 3 days, 22 hours, 18 minutes, 32 seconds

Base MAC Address: 00:54:bd:12:a8:32

Switch Operation Mode After Reset: ☐ Standalone ☒ Stack

Jumbo Frame: ☐ Enable ☒ Disable

| Unit No. | Model Name | Hardware Version | Boot Version | Software Version |
|----------|------------|------------------|--------------|------------------|
| 1 | SGE2010 | 00.00.01 | 2.0.0.00 | 3.0.0.4 |
| 2 | SGE2000P | 00.00.10 | 1.0.0.05 | 3.0.0.4 |

Apply

© 2009 Cisco Systems, Inc. All rights reserved

The *System Information Page* contains the following fields:

- **Model Name** — Displays the model name and number of ports supported by the system.
- **System Name** — Displays the user configured name of the system.
- **System Location** — Defines the location where the system is currently running. The field range is up to 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is up to 0-160 characters.
- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **System Up Time** — Displays the amount of time that has elapsed since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example: 41 days, 2 hours, 22 minutes and 15 seconds.
- **Base MAC Address** — Displays the device MAC address. If the system is in stack mode, the Base MAC Address of the master unit is displayed.

- **Hardware Version** — Displays the hardware version number.
- **Software Version** — Displays the software version number. If the system is in stack mode, the version of the master unit is displayed.
- **Boot Version** — Indicates the system boot version currently running on the device. If the system is in stack mode, the version of the master unit is displayed.
- **Switch Operation Mode After Reset** — Indicates the mode the device operates in after the system is reset. The possible field values are:
 - Standalone — Indicates the device operates as a stand-alone device after the system is reset.
 - Stack — Indicates the device operates as a Stacked unit after the system is reset.

Managing Stacking

This section contains information for understanding and configuring stacking.

- Configuring a Stack
- Stack Membership
- Defining Stacking Unit ID
- Adding, Replacing and Removing Stacking Members — Examples
- Managing Stacks

Understanding Switch Operating Modes

The device has the following operating modes:

- Stack
- Stand-alone.

Both the Stack and Stand-alone mode can be selected by the user during software boot or using the device GUI System Information page. The selected operating mode is enabled after the unit is reset. The factory default is Stack mode.

Stand-alone Mode

Devices operating in stand-alone mode run as a independent -single unit. All ports of a stand-alone switch operate as normal Ethernet links. A stand-alone switch does not participate in a stack even if the device is physically connected to a stack. However, a unit whose mode is changed from Stack to Stand-alone retains its stacking configuration information. That information is restored if the unit is returned to Stack mode.

Stack Mode

Devices operating in stack mode are not an independent unit, but are members of an organized group of switches known as a stack. A stack consists of a Master, a Backup Master switch, and up to six stacking member switches.

As a special case, a unit operating in Stacking mode, which is not connected to any other units, may operate as a **stack-of-one**.

The following device ports of each unit in a stack mode are reserved as stacking links, and cannot be used for regular network connections.

- SFE2000 - Default stacking ports: G1, G2. Configurable stacking port: G3/GBIC 1, G4/GBIC 2
- SGE2000 - Default stacking ports: 12/GBIC 3, 24/GBIC 4.
- SFE2010 - Default stacking ports: G1, G2. Configurable stacking port: GBIC 1, GBIC 2.
- SGE2010 - Default stacking ports: 24/GBIC 3, 48/GBIC 4

Configuring a Stack

A stack is initialized by the following sequence of operations:

- Physical connection of the switches in a stack topology. The system administrator connects the switches to be included in the stack in the desired order and topology (ring or chain).
- Powering on of the units. The system administrator powers on all the connected units. (A new stack consisting of factory default units may also be built by powering the units on one by one, as described in Recommended Procedures for Building a Stack).

- **Master Election.** Master Election takes place automatically to select the Master unit. If there are two or more units in the stack, then a Backup unit is also automatically selected.
- **Topology Discovery.** The stack Master unit carries out a process called topology discovery to learn which units are present in the stack, the order in which they are connected and the Unit ID that each unit reports itself as owning. The Master unit then examines the reported Unit IDs and notes any violations of the Unit ID Validity Rules. These include units reporting duplicate Unit IDs and units in factory default (Unit ID=0) mode. Topology discovery also takes place any time a change in the stack topology occurs, such as removing or adding a unit to the stack.
- **Unit ID Conflict Resolution.** The Master unit attempts to resolve conflicts among two or more units contending for the same Unit ID. After applying the rules for Unit ID Conflict Resolution, one unit retains its Unit ID. The other contending units are either shut down or reset to Unit ID=0 by the Master unit.
- **Automatic Unit ID Assignment.** The Master unit applies automatic numbering to units with Unit ID=0. These units include new factory units, units reset to factory default mode by the system administrator pressing the reset button on the switch or units automatically reset to Unit ID=0 by the Master unit during Unit ID Conflict Resolution.
- **Unit and Port Configuration.** At this point, the stack has a valid topology. The Master unit now configures all member units and their ports according to the configuration file stored in the Master unit. The Stack Initialization is complete and the stack enters normal operational mode. Configuration files are changed only through explicit user configuration. Configuration files are not automatically modified when:
 - Units are Added
 - Units are Removed
 - Units are reassigned Unit IDs
 - Units toggle between Stacking Mode and stand-alone Mode

Each time the system reboots, the Startup Configuration file in the Master unit is used to configure the stack. If a stack member is removed from the stack, and then replaced with a unit with the same Unit ID, the stack member is configured with the original device configuration. Only ports that are physically present are displayed in the web screens, and can be

configured through the web management system. By default, Unit IDs are assigned automatically. However, you can use the browser to assign a specific Unit ID; for example, the same unit ID as the unit which was recently removed.

Stack Membership

The system supports up to eight switching units per stack. A stack is comprised of three stacking member types:

- **Stacking Master** — Provides a single control, configuration and management point for stacking members through a single IP address interface. The Stacking Master maintains the stack management, device configuration. In addition, the Stacking Master detects and reconfigures the ports with minimal operational impact in the event of unit failure, inter-unit link failure, and unit insertion or removal. A stack must contain a single Stacking Master.

Each port in the stack has a specific Unit ID, port type, and port number, which is part of both the configuration commands and the configuration files. Configuration files are managed only from the Master unit. This includes:

- Saving to the FLASH
- Uploading Configuration files to an external TFTP Server
- Downloading Configuration files from an external TFTP Server
- The Backup Master is a stacking member that receives a copy of the Stacking Master Configuration file. A stack can contain a single Backup unit or none at all.

The Backup unit replaces the Master unit if one of the following events occur:

- The Master unit fails or is removed from the stack.
- Links from the Master unit to the stacking units fail.
- A soft switchover is performed via the web interface.

Switching between the Stacking Master and the Backup Master results in a limited service loss. The Stacking Master and the Backup Master maintain a *Warm Standby*, meaning that the Stacking Master and the Backup units are synchronized with the static configuration only. Any Dynamic Address Tables are relearned if a failure occurs. The Running Configuration file is synchronized between the Stacking Master and the Backup, and continues running on the Backup Master.

- The stacking members operate under the control of the Master unit. Device software is downloaded separately for each stack member. All stacking members must run the same software version. A stack may contain from zero to six stacking members (not including the Backup unit).

Defining Stacking Unit ID

Each member unit of a stack is assigned a Unit ID. The Unit ID assignment can be manually selected by the system administrator or automatically selected by the software. The value of the Unit ID also signifies the class of unit. For a stack comprised of factory default units only, the Unit IDs are assigned as follows:

- Unit ID 1 - Stacking Master
- Unit ID 2 - Backup Master
- Units ID 3 - 8 - Stacking members.

The Unit ID is displayed by a LED indicator on the front panel.

Units of a stack do not have to be connected in sequential order. For example, a stack may consist of the units connected in the following order:

Unit 3—Unit 5—Unit 1—Unit 4—Unit 2

It is recommended that a stack of new, factory default switches be initially configured in the automatic mode. This ensures that a group of factory delivered switches can be easily configured as a stack. After the initial setup of the stack, the Unit ID mode for a stack member may be changed.

Master-enabled Units and Force Master

Unit 1 and Unit 2 are called Master-Enabled units because they are the only units in an existing stack that are eligible to become the Master unit. One of these units becomes the Master unit and the other becomes the Backup unit. The Master unit selection can be made automatically by the system, or manually by the system administrator by setting one of the Master-enabled units as Force Master. The Backup unit may also be selected automatically by the system, or manually by setting the Unit ID. For example, the system administrator may set Unit 2 as Force Master and manually number another unit to be Unit 1. In this case Unit 2 becomes the Master unit and Unit 1 becomes the Backup unit.

Stacking Member Unit IDs

Units 3 through 8 are assigned to stacking members. Stacking members are managed by the Master unit.

Factory Default Units

A unit in factory default mode has the following attributes:

- **Unit ID** = 0. This setting indicates that the unit is in autonumbering mode.
- **Switch Operation Mode** = Stack.

The combination of these two settings directs the system to automatically configure the unit as a new stack member.

NOTE: A unit in stand-alone mode also displays Unit ID = 0.

Unit ID Validity Rules

Each member unit of a stack has a Unit ID that satisfies two conditions:

- A Unit ID is a number from 1 to 8.
- A Unit ID is unique within the stack.

Automatic Unit ID Assignment

Automatic Unit ID assignment is applied to Stack mode units with Unit ID of 0. This includes factory default units as well as units whose Unit IDs are reset to 0 as a result of Unit ID Conflict Resolution.

The Automatic Unit ID Assignment for units with Unit ID=0 proceeds as follows:

- A Unit ID is assigned from the available valid, unique Unit IDs, starting with the lowest available Unit ID.
- If two or more units are queued to receive Unit IDs, the units are assigned Unit IDs starting with the unit with the lowest MAC address.

Manual Unit ID Assignment

The system administrator can assign a specific, valid Unit ID to a stack member manually. A Unit ID that is manually assigned is not subject to automatic numbering.

Manual numbering for stacking members is beneficial for providing a fast and easy way of replacing stacking members. After a stack is initialized in factory default, automatic numbering mode, the Unit IDs can be manually set to the same Unit IDs assigned by automatic numbering. The system administrator can then configure the switch ports. The port configuration of the switch is automatically stored in the Stacking Master and Backup Master. If a stacking member must be replaced, an identical replacement stacking member can be hot swapped into the running stack. The hot swap can occur if the new stacking member is manually in the same

Unit ID as the switch being replaced. The newly inserted switch is identified by the Master unit by its Unit ID. Since the configuration of the original switch is also stored in the Master and Backup units by Unit ID, the new switch automatically receives the configuration of the old switch. This eliminates the need to configure the new switch and reduces the system downtime.

The advantage of manual vs. automatic unit numbering is illustrated in the following example:

A stack consists of Units 1,2,4,6,7. Unit 7 fails and an identical replacement unit is inserted. If the replacement unit is manually pre-set to be Unit 7, it can be inserted into the stack and inherit the configuration of the replaced (failing) Unit 7. However, if the replacement unit is not preset but is inserted in factory default mode (Unit 0), it is automatically renumbered to Unit 3 because that is the lowest available Unit ID in the stack. The new Unit 3 now inherits the previous unit 3 configuration. Otherwise, the system administrator must manually configure all the ports of the new Unit 3.

Unit ID Conflict Resolution

If two or more stacking members have the same valid Unit ID, the Master attempts to resolve the conflict by awarding the contested Unit ID to one of the units. For stacking members that are not granted the unit ID, the Stacking Master either:

- Automatically resets the Unit ID to 0. The Stacking members become eligible to be reassigned another Unit ID by *Automatic Unit ID Assignment*.
- The units are shut down. A unit that is automatically shut down remains powered on, but it is not operational, indicated by the solid red port Led. It is not a member of the stack and its connections are effectively disconnected from its immediate neighbors in the stack. If the stack is initially connected in a ring topology, the shutdown unit changes the topology into a chain. However, if the stack is initially configured in a chain topology, the shutdown unit breaks the chain. Depending on the particular configuration, may lead to other units being shut down. An automatically shut down unit remains shut down until the system administrator, manually renumbers the stacking member or removes the stacking member from the stack. A message is sent to the user that a unit failed to join the stack.

The Master unit attempts to resolve Unit ID conflicts by applying the following rules:

-
- STEP 1** When inserting a unit into a running stack, units that are members of the existing stack retain their Unit IDs. Therefore:
- If an automatically numbered unit was inserted into a running stack, the existing unit retains its Unit ID and the newer unit is reset to Unit ID=0.
 - If a manually numbered unit was inserted into a running stack, the existing unit retains its Unit ID and the manually numbered unit is shut down because its Unit ID cannot be changed automatically.
- STEP 2** When adding a unit to a stack at stack reset (boot), units with duplicate Unit IDs contend with each other for the same Unit ID according to the rules and restrictions imposed upon their unit class.
- Master-enabled units with duplicate Unit IDs compete with each other in the Master Election.
 - If two units are contending for the same Unit ID, the Master decides as follows:
 - If one unit is manually numbered and the other unit is automatically numbered, the manually numbered unit retains its Unit ID and the automatically numbered unit is reset to Unit ID=0.
 - If both units are automatically numbered, the unit with the lower MAC address retains its Unit ID and the other unit is reset to Unit ID=0.
 - If both units are manually numbered, the unit with the lower MAC address retains its Unit ID and the other unit is shut down.
- STEP 3** Two manually numbered units with the same Unit ID can never be added or inserted into a stack simultaneously. Both units are shut down.
- STEP 4** When inserting new units into a running stack, if the resulting total number of old and new units exceeds the maximum allowed (eight), all the new units are shut down.
- STEP 5** Connecting more than the maximum number (eight) of units in a new stack may produce unpredictable results due to race conditions among the units.
- STEP 6** Any units that have been reset to Unit ID 0 are then reassigned new Unit IDs, if possible, by Automatic Unit ID Assignment.
-

Master Election

The Master and Backup unit selection is known as Master Election. Master Election takes place if there are one or more eligible candidates contending to be the Master unit.

Master Election Candidate Eligibility

In general, not all stack member units are eligible to be candidates for Master Election. Eligibility for Master Election is determined in the following order.

-
- STEP 1** All Master-enabled switching units present in a stack are candidates for Master Election. All units that are not Master-enabled are not eligible for Master Election.
- STEP 2** If there are no Master-enabled units present in a stack, then all units in factory default mode (Unit ID=0, Switch Operation Mode=Stack) are candidates for Master Election. No other units are eligible for Master Election.

If neither Master-enabled nor factory default units are present, Master election does not take place and all units in the stack are effectively shut down. The stack remains in this inoperable state until either a new Master-enabled unit is connected to the stack or a current stack unit is manually reset to factory default mode (by pressing the reset switch on the front panel of the switch and holding it down for at least ten seconds).

Master Election Selection Rules

If there are two or more candidates for Master Election, the Stack Master is determined by comparing attributes of the contending units in a specific order. The order in which the attribute comparisons are made is:

- 1 - Unit assigned by the system administrator as Force Master
- 2 - Unit with the longest running time (measured in 10 minute increments)
- 3 - Unit having Unit ID=1
- 4 - Unit having the lowest MAC address

The Master Election proceeds by making the attribute comparisons in the above specified order. If there is a tie at any step, the election proceeds to the next step. However, units that fail to tie at any step are eliminated from the competition. Units that succeed in the tie in a given step, go on to compete in the next step. The election is decided at the first step for which there is a clear winner. The winner of that step is the winner of the Master Election and becomes the Master unit.

For example:

- If there are two or more Master-enabled units and only one of them has been assigned as Force Master, the Force Master unit is the winner of step 1 and therefore the winner of the Master Election.
- If there are two or more Master-enabled units that have been assigned as Force Master, then the Master Election proceeds to step 2, where the running times of the Force Master units are compared. If there is a winner at step 2, then the winner of that step also wins the Master Election and becomes the Master unit.
- If there is no winner of step 2, the election proceeds to step 3. Only contending units that have succeeded in tying in previous steps remain contenders. If there is a single unit with Unit ID=1, then that unit wins step 3 and the Master Election.
- If there are two or more units assigned to Unit ID=1, then the election proceeds to step 4. There is always a winner of step 4 because MAC addresses are unique.

Master Election Backup Unit Selection Rules

The candidate that wins the Master Election becomes the Master unit. If there is a single runner-up unit, that unit becomes the Backup unit. If there is a tie for the runner-up position, then the tie is resolved by applying the Unit ID Conflict Resolution rules.

Recommended Procedures for Building a Stack

To avoid possible Unit ID conflicts and device shutdowns, Cisco recommends that the following procedures be adopted when configuring and managing stacks:

- A stack should be initially configured by connecting all stack members in factory default mode.
- If there is a preference for assigning specific Unit IDs to specific devices, then the stack should be built by connecting and booting the devices, in factory default mode, one by one in the desired Unit ID order that they will be assigned in the stack. That is, the device that will be the Master unit should be powered on first. After it boots and is automatically numbered (as Unit 1) it becomes the Master unit. The unit that will become the Backup unit is then connected to the Master unit and powered on. It is assigned to be Unit 2 by the Master unit and becomes the Backup unit. The next unit is then connected to either the Master (Unit 1) or Backup (Unit 2) unit and then powered on. It is assigned to be Unit 3 by the Master unit. Subsequent units are joined to the stack by connecting

each one to any existing stack member unit and then powering the new unit on. Each new unit is assigned the next available Unit ID.

- After the stack is initialized and configured, the system administrator may reset the Unit IDs manually to the same values assigned by automatic numbering.

Adding, Replacing and Removing Stacking Members — Examples

The following examples illustrate stacking behavior when adding, replacing or removing stack members:

- A stack is initially configured with Units 1,2,3,4,5,6,7,8. Master Unit 1 is then removed while the stack is running and is replaced with another switch that is in factory default mode. What happens?

When Master Unit 1 is removed, Backup Unit 2 automatically becomes the Master unit. The newly inserted Unit 0 enters the stack and is automatically numbered as Unit 1, but remains a stacking member (Since it did not enter the stack as a Master-enabled unit and the stack already had a Master unit, its entry did not trigger a Master Election.). However, after being assigned to be Unit 1, it becomes a Master-enabled unit and will be a candidate in the next Master Election. For instance, if the stack is reset, it will win the Master Election and become the Master unit, while the present Master unit, Unit 2, will become the Backup unit.

Removing or replacing stack members incorrectly may result in an inoperable unit or stack, as illustrated in the following examples:

- A stack is initially configured with Units 1,2,4,6,7. Units 1 and 2 are then removed, leaving Units 4, 6, 7. The stack is permanently disabled because there is no Master unit, and the remaining units 4, 6, 7 are shut down. There are no Master-enabled units, so Master Election cannot take place. In this example, it makes no difference whether or not Units 4, 6, 7 were automatically numbered or manually numbered. Rebooting the units does not change the situation, even for automatically numbered units. Since there are no Unit ID conflicts, all the units retain their Unit IDs and therefore Automatic Unit ID Assignment does not occur. Then, after rebooting, all units are again shut down. Only by selecting one of the remaining units to be Force Master or by manually resetting at least one of them to factory default (Unit 0) mode can these units be configured as an active stack.

- A stack is initially configured in chain topology and the units are connected as follows:

Unit 2—Unit 5—Unit 1—Unit 4—Unit 6—Unit 8

The system administrator resets Unit 4 but does not realize that the **Switch Operation Mode After Reset** field on the *System Information* page was mistakenly checked as *stand-alone*. No physical connections are changed. Unit 4 reboots in stand-alone mode, effectively cutting off Units 6 and 8 from the stack. Units 6 and 8 are shut down. The stack continues to operate, but with Units 1, 2 and 5 being the only active units.

- In the previous example, suppose that the system administrator realizes the error after rebooting Unit 4 as a stand-alone device. The system administrator should reboot Unit 4 in Stack mode. If the stack has not been reset, the Master unit retains the original stack configuration file. Also, Unit 4 retains its stacking configuration information when its mode is changed from Stack to stand-alone, and restores that information when returning to Stack mode.
- A stack is initially configured and all units are manually numbered. The units are connected in a chain topology as follows:

Unit 2—Unit 5—Unit 1—Unit 3—Unit 4—Unit 6—Unit 7—Unit 8

Unit 3 fails. Since Units 4, 6, 7 and 8 are cut off from the Master unit, they are automatically shut down. This leaves only Units 1, 2 and 5 running in the stack.

The system administrator prepares a replacement unit by manually renumbering a unit from another stack. However, the replacement unit is mistakenly renumbered as Unit 4 instead of Unit 3. What happens if the replacement unit is inserted into the running stack (in the same position as Unit 3)? When the new Unit 4 is inserted into the running stack, the Master unit executes Topology Discovery and discovers the new Unit 4. But now the presence of the old Unit 4 is also discovered because of the revived

connection to the stack via the new Unit 4. The old Unit 4 and the new Unit 4 appear to the Master unit as two new, manually numbered units trying to simultaneously join the stack. Therefore, both units are shut down, and thus Units 6, 7 and 8 remain shut down.

What happens if the replacement unit is inserted into the stack (in the same position as Unit 3) after first powering off all units and then simultaneously powering on all units?

If all units in the stack are reset, the Master unit performs Topology Discovery during the software boot, revealing that there are two duplicate Unit IDs (old and new Unit 4). Since both units are manually numbered, both units are shut down by the Master unit. This, in turn, again leaves Units 6, 7 and 8 disconnected from the Master unit, thus shutting them down also.

- A stack is initially configured in a chain topology as follows:

Unit 8—Unit 5—Unit 1—Unit 3—Unit 4—Unit 6—Unit 7—Unit 2

Unit 1 is the Master and Unit 2 is the Backup. Unit 3 fails. What happens?

The failure of Unit 3 disconnects Units 4, 6, 7 and 2 from the Master unit. Backup Unit 2 senses the loss of the Master and automatically becomes the Master of a stack comprised of Units 2, 4, 6 and 7. Unit 1 remains the Master of the now reduced stack, consisting of Units 1, 5 and 8. Thus the failure of Unit 3 has split the original stack into two smaller stacks. However, while the two stacks continue in operation, this situation may create problems on the network because Unit 2 and Unit 1 have the same Master configuration files. The significance of this is that both stacks share the same IP address, making network communication with either stack ambiguous.

Managing Stacks

The *Stack Management Page* allows network managers to configure stacking members on the device and determine to either reset the entire stack or a specific device. Device configuration changes that are not saved before the device is reset are not saved. If the Master unit is reset, the entire stack is reset.

To open the *Stack Management Page*:

- STEP 1** Click **System > System Management > Stack Management**. The *Stack Management Page* opens:

Stack Management Page

Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch

Stack Management

Master Election

☒ Automatically ☐ Force Master

| Unit No. | Model Name | Unit No. After Reset | Uplink | Downlink |
|----------|------------|----------------------|-----------|-----------|
| 1 | SGE2010 | Auto | 2 | link down |
| 2 | SGE2000P | 2 | link down | 1 |

Apply

© 2009 Cisco Systems, Inc. All rights reserved

The *Stack Management Page* contains the following fields:

- **Master Election** — Indicates the method of electing the master device. The possible values are:
 - *Automatically* — The master is selected automatically by software.
 - *Force Master* — The unit is forced to be master of the stack. Note that only Unit 1 or Unit 2 can be the stack master.
- **Unit No.** — Displays the stacking member unit number for which the stacking parameters are displayed.
- **Model Name** — Displays the model name of ports supported by the system.
- **Unit No. After Reset** — Indicates the new unit number of the stacking member after the device is reset.
- **Uplink** — Indicates the next higher stacking unit in the uplink path.
- **Downlink** — Indicates the next lower stacking unit in the downlink path.

- STEP 2** Define the relevant fields.

STEP 3 Click Apply. Stack management is defined, and the device is updated.

Viewing Device Health

The *Health Page* displays physical device information, including information about the device's power and ventilation sources.

STEP 1 Click **System** > **System Management** > **Health**. The *Health Page* opens:

Health Page

The screenshot shows the Cisco Health Page for a Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE. The left sidebar contains a navigation menu with the following items: System, System Management (expanded), System Information (SGE2000P), Stack Management, Health (highlighted), Reset, TCAM Utilization, Time, IP Addressing, Domain Name System, SNMP, Admin, Statistics, Bridging, Security Suite, and Quality of Service. The main content area displays the Health page with a table showing the status of the power supply and fans.

| Unit No. | Power Supply Status | | Fan Status | | | | |
|----------|---------------------|-------------|------------|------|------|------|------|
| | PS | RPS | Fan1 | Fan2 | Fan3 | Fan4 | Fan5 |
| 2 | OK | Not Present | OK | OK | OK | OK | OK |

The *Health Page* contains the following fields:

- **Unit No.** — Indicates the number of stack member for which the device information is displayed.
- **Power Supply Status** — Displays the power supply status. The internal power supply is displayed as PS in the interface, while the redundant power supply is displayed as RPS. If the status is displayed as *Not Present*, this indicates that a redundant power supply is not connected (for RPS only).
- **Fan Status** — Displays the fan status. The device has up to five fans. Each fan is denoted as fan plus the fan number. The possible field values are:

- *OK* — Indicates the fan is operating normally.
- *Fail* — Indicates the fan is not operating normally.

NOTE: The GE device has up to five fans (the FE device has one fan).

Resetting the Device

The *Reset Page* enables the device to be reset from a remote location. Save all changes to the Start up Configuration file before resetting the device. This prevents the current device configuration from being lost.

If a Master unit and/or a backup Master unit is removed from the stack and the user wishes to configure one of the member units (Units 3-8) to be a backup Master, the user must reset the unit and configure a new unit number to stack (using the Unit number selection process).

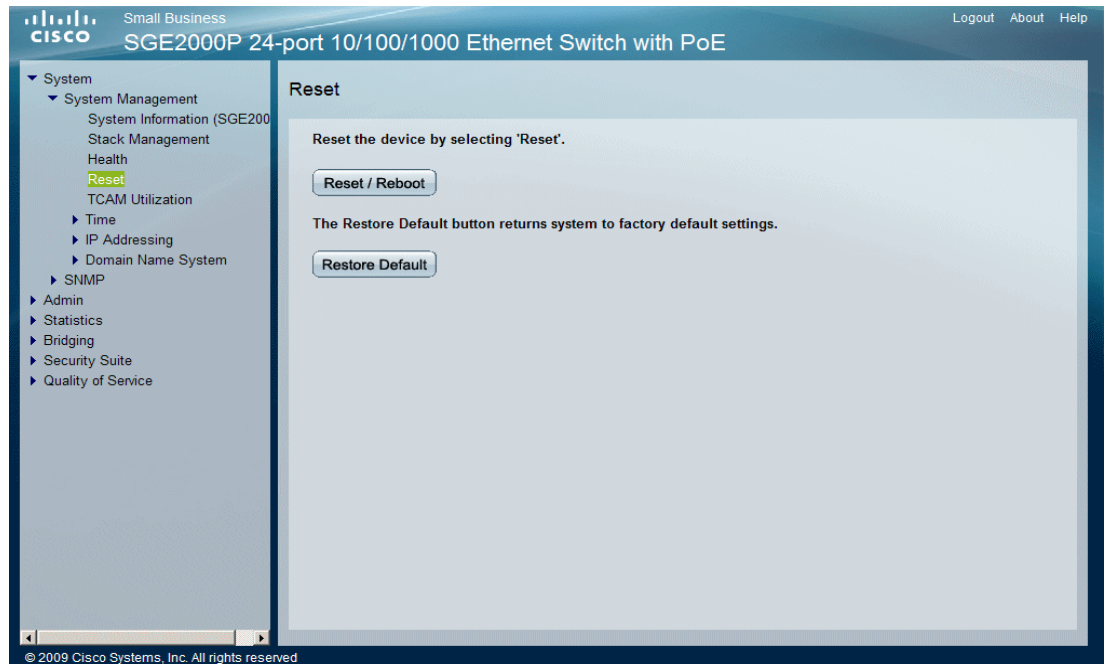
The following resets the device:

- **Restart / Reboot** — Resets the device. Ensure the device configuration has been saved.
- **Restore Default** — The device is restored to the factory default configuration. In Stacking mode, unit no. 1 becomes the Master, and the stacking members are reset.

To open the *Reset Page*.

STEP 1 Click **System > System Management > Reset**. The *Reset Page* opens:

Reset Page



STEP 2 Click one of the available Reset commands. The device resets.

STEP 3 Enter the user name and password to reconnect to the Web Interface.

Defining Bonjour

Bonjour is a service discovery protocol that enables automatic discovery of computers, devices and services on IP networks. Bonjour's *multicast Domain Name System* (mDNS) service allows the device to publish device services by sending and receiving UDP packets only to the following multicast address 224.0.0.251 and to port number 5353.

The *Bonjour Page* contains information for enabling/disabling Bonjour on the device, specifying a Service Type and the related port used for publishing devices over the network. A Service Type is the type of service registration performed as part of the device system start up. It is intended to assure the uniqueness of the published service and proclaims the related information. The device information published via DNS includes the following details:

- Model Number
- Device Type
- Firmware Version
- MAC Address
- Serial Number
- Hostname

The Service Types that are provided for Bonjour are: **_csbdp**, (a Cisco specific Service Type) , **HTTP**, **HTTPS** and **Other**. **Other** allows for additional Service Types to be added manually.

To define Bonjour:

STEP 1 Click **System > Admin > Bonjour**. The *Bonjour Page* opens:

Bonjour Page

The *Bonjour Page* contains the following fields:

- **Bonjour State** — Enables Bonjour thereby allowing the Switch to publish device services via Bonjour using the mDNS service. The possible field values are:
 - *Enable* — Enables Bonjour on the device. This is the default value.

- *Disable* — Disables Bonjour on the device.
- **Service Type Selection** — Defines the *DNS Service Discovery* (DNS-SD) Service Type used to publish devices on the network. The possible field values are:
 - *_csbdp (default)* — Specifies the Service Type selected is *_csbdp*. This is a Cisco generic Service Type. The port number is chosen randomly from the port range of 4000-5000 at the initialization stage and is used afterwards. This is the default value.
 - *HTTP* — Specifies the Service Type selected is HTTP which is published using the default http TCP port 80. HTTP is used mainly for human-readable HTML content served over HTTP.
 - *HTTPS* — Specifies the Service Type selected is secured HTTP which is published using the default http TCP port 443.
 - *Other* — Indicates a user-defined Service Type to be added.
- **Service Type** — Displays the selected Service Type defined in the Service Type field.
- **Port** — Defines the selected port used for the relevant Service Type. The port number for *_csbdp*, HTTP and HTTPS Service Types are predefined and therefore are displayed as read-only values.

STEP 2 Select a Service Type from the Service Type Selection drop-down field.

STEP 3 Define a Port number, only if Other is the selected Service Type.

STEP 4 Click **Apply**. The Service Type is defined, and the device is updated.

Disabling Bonjour

STEP 1 Click **System > Admin > Bonjour**. The *Bonjour Page* opens:

STEP 2 Select Disable from the **Bonjour State** field drop-down menu.

STEP 3 Click **APPLY**. The Bonjour protocol is disabled, and the device is updated.

TCAM Utilization

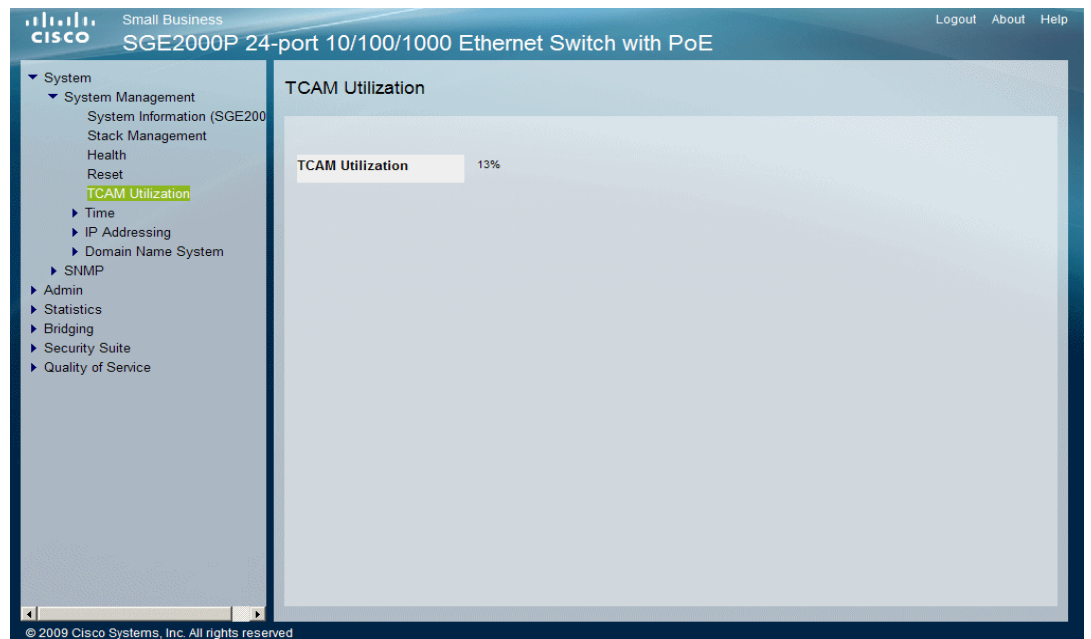
The maximum number of rules that may be allocated by all applications on the device is 1024. Some applications allocate rules upon their initiation. Additionally, applications that initialize during system boot use some of their rules during the startup process.

The following table lists all applications that can allocate TCAM rules. Each allocation has its specific allocation policy.

TCAM Allocation

| Application | Per Port/ Per Device | Allocation on Activation | Application Upper Limit | TCAM rules per User ACL | Comments |
|-------------------------|-------------------------|--------------------------|-------------------------|--|--|
| QoS Advanced Mode rules | Port | 6/device | No limit | 1 or 2 TCAM entries per each rule. | Feature is activated by default. |
| Access Control Rules | Port | 6/device | No limit | 1 or 2 TCAM entries per each rule. | Feature is activated by default. |
| PVE | Port | 2/port or LAG | --- | --- | Feature is activated by default. Allocation done only during initialization. |
| IP Subnet VLAN | Port | 0 | 255 | 2 or 4 | Rules are duplicated for both IP and MAC based VLANs. |
| Protocol Based VLAN | Port | 0 | No limit | 1 or 2 | Rules are duplicated for both IP and MAC based VLANs. |
| MAC Based VLAN | Port | 0 | 432 | 1 or 2 | Rules are duplicated for both IP and MAC based VLANs. |
| DHCP Snooping | Device | 2/device | No limit | 8 TCAM entries/1 DHCP Snooping rule | |
| IP Source Guard | Port | 0 | No limit | 1 TCAM entry/1 IP Source Guard entry | |
| ARP Inspection | Device | 2/device | 128 | 4 TCAM entries/1 ARP Inspection rule | |
| VLAN Rate Limiting | Both | 0 | 255 | 1 global rule/1 VLAN Rate Limit. Additional rule is created for each "permit" rule on the interface. | |

TCAM Utilization Page



The *TCAM Utilization Page* contains the following fields:

- **TCAM Utilization** — Indicates the percentage of the available TCAM resources which are used. For example, if more ACLs and policy maps are defined, the system uses more TCAM resources.

Configuring System Time

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems.

This section provides information for configuring the system time, and includes the following topics:

- Defining System Time
- Defining SNTP Settings
- Defining SNTP Authentication

Defining System Time

The *System Time Page* contains fields for defining system time parameters for both the local hardware clock, and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

To define system time:

STEP 1 Click **System > System Management > Time > System Time**. The *System Time Page* opens:

System Time Page

The screenshot shows the Cisco System Time configuration page. The left sidebar contains a navigation tree with 'System' > 'System Management' > 'Time' > 'System Time' highlighted. The main content area is titled 'System Time' and contains the following fields:

- Clock Source:** Two radio buttons, 'Use Local Settings' (selected) and 'Use SNTP Server'.
- Local Settings:**
 - Date:** A text field with '01/Oct/08' and a format '(DD/MMM/YY)'.
 - Local Time:** A text field with '06:12:53' and a format '(HH:MM:SS)'.
 - Time Zone Offset:** A dropdown menu showing 'GMT'.
 - Daylight Saving:** A checkbox labeled 'Daylight Saving' with three radio buttons: 'USA' (selected), 'European', and 'Other'.
 - Time Set Offset:** A text field with '0' and a unit '(Min)'.
 - From:** Two text fields for date and time, with formats '(DD/MMM/YY)' and '(HH:MM)'.
 - To:** Two text fields for date and time, with formats '(DD/MMM/YY)' and '(HH:MM)'.
 - Recurring:** A checkbox labeled 'Recurring' with two sets of fields for 'From' and 'To' dates and times, each with formats '(DD/MMM/YY)' and '(HH:MM)'.
- Apply:** A button at the bottom.

The *System Time Page* contains the following fields:

- **Clock Source** — Indicates the source used to set the system clock. The possible field values:
 - *Use Local Settings* — The system time is set on the local device. This is the default value.
 - *Use SNTP Server* — Sets the system time via an SNTP server.
- **Date** — Indicates the system date. The field format is , for example, .
- **Local Time** — Indicates the system time. The field format is HH:MM:SS, for example, 21:15:03.
- **Time Zone Offset** — Indicates the difference between *Greenwich Mean Time* (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GMT –5. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area.
- **Daylight Savings** — Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:
 - *USA* —

- *European* — The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.
- *Other* — The DST definitions are user-defined based on the device locality. If Other is selected, the *From* and *To* fields must be defined.
- **Time Set Offset** — Indicates the difference in minutes between DST and the local standard time. The default time is 60 minutes.

The following fields are active for non-USA and European countries.

- **From** — Indicates the time that DST ends in countries other than USA or Europe in the format in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25Oct07 and 5:00.
- **To** — Indicates the time that DST ends in countries other than USA or Europe in the format in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23Mar08 and 12:00.
- **Recurring** — Select if the DST period in countries other than USA or European is constant from year to year. The possible field values are:
- **From** — Indicates the day and time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:
 - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday- Saturday.
 - *Week* — The week within the month from which DST begins every year. The possible field range is 1-5.
 - *Month* — The month of the year in which DST begins every year. The possible field range is Jan.-Dec.
 - *Time* — The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.
- **To** — Indicates the day and time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:
 - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.

- *Week* — The week within the month at which DST ends every year. The possible field range is 1-5.
- *Month* — The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
- *Time* — The time at which DST ends every year. The field format is Hour:Minute, for example, 05:30.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The Time Settings are defined, and the device is updated.

Defining SNTP Settings

The *SNTP Settings Page* contains information for enabling SNTP servers, as well as adding new SNTP servers. In addition, the *SNTP Settings Page* enables the device to request and accept SNTP traffic from a server.

To define SNTP global settings:

- STEP 1** Click **System > System Management > Time > SNTP Settings**. The *SNTP Settings Page* opens:

SNTP Settings Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE management interface. The left sidebar contains a tree view with the following structure:

- System
 - System Management
 - System Information (SGE2000P)
 - Stack Management
 - Health
 - Reset
 - TCAM Utilization
 - Time
 - System Time
 - SNTP Settings** (highlighted)
 - SNTP Authentication
 - IP Addressing
 - Domain Name System
 - SNMP
 - Admin
 - Statistics
 - Bridging
 - Security Suite
 - Quality of Service

The main content area is titled 'SNTP Settings'. It features a checkbox labeled 'Enable SNTP Broadcast Reception' which is currently unchecked. Below this is a section titled 'Unicast SNTP Servers' containing a table with the following columns: SNTP Server, Poll Interval, Encryption Key ID, Preference, Status, Last Response, Offset, and Delay. There are 'Delete' and 'Add' buttons to the right of the table, and an 'Apply' button at the bottom of the section.

The *SNTP Settings Page* contains the following fields:

- **Enable SNTP Broadcast** — Enables polling the selected SNTP Server for system time information.
- **SNTP Server** — Indicates the SNTP server IP address. Up to eight SNTP servers can be defined.
- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for system time information. By default, the poll interval is 1024 seconds.
- **Encryption Key ID** — Indicates the Key Identification used to communicate between the SNTP server and device. The range is 1 - 4294967295.
- **Preference** — The SNTP server providing SNTP system time information. The possible field values are:
 - *Primary* — The primary server provides SNTP information.
 - *Secondary* — The backup server provides SNTP information.
 - *In progress* — The SNTP server is currently sending or receiving SNTP information.

- *Unknown* — The progress of the SNTP information currently being sent is unknown. For example, the device is currently trying to locate an interface.
- **Status** — The operating SNTP server status. The possible field values are:
 - *Up* — The SNTP server is currently operating normally.
 - *Down* — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
 - *Unknown* — Indicates that the device (sntp client) is currently looking for sntp server.
- **Last Response** — Indicates the last time a response was received from the SNTP server.
- **Offset** — Indicates the difference in minutes between DST and the local standard time. The default time is 60 minutes.
- **Delay** — Indicates the amount of time it takes to reach the SNTP server.

STEP 2 Click the **Add** button. The *Add SNTP Server Page* opens:

Add SNTP Server Page

The *Add SNTP Server Page* contains the following fields:

- **Supported IP Format** — Provides the supported IP format: Version 6 or Version 4.
 - **IPv6 Address Type** — Indicates the type of IP Address: Link Local or Global.
- **SNTP Server** — The SNTP server's IP address.
- **Enable Poll Interval** — Select whether or not the device polls the selected SNTP server for system time information.

- **Encryption Key ID** — Select if Key Identification is used to communicate between the SNTP server and device. The range is 1 - 4294967295.

STEP 3 Define the relevant fields.

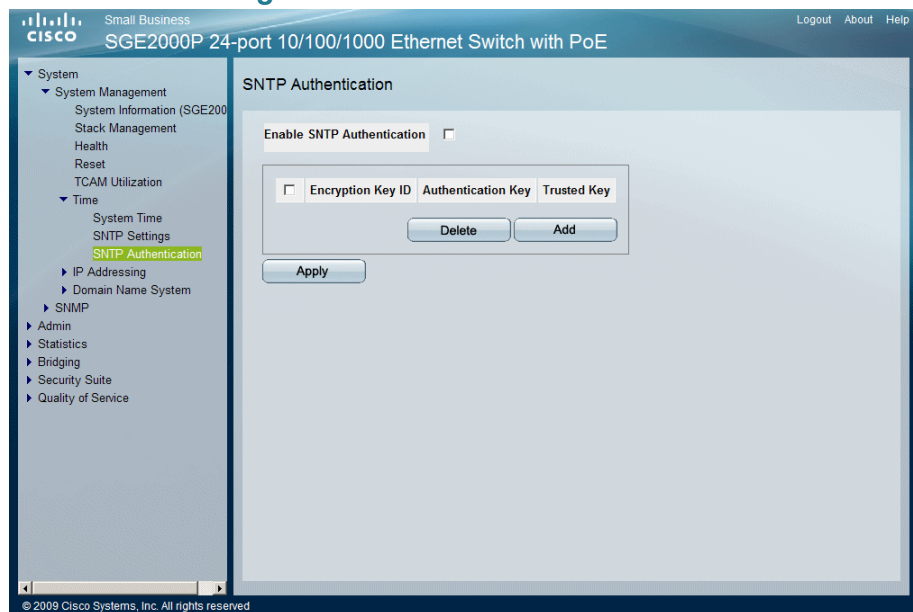
STEP 4 Click **Add**. The SNTP Server is added, and the device is updated.

Defining SNTP Authentication

The *SNTP Authentication Page* provides parameters for performing authentication of the SNTP server.

STEP 1 Click **System > System Management > Time > SNTP Authentication**. The *SNTP Authentication Page* opens:

SNTP Authentication Page



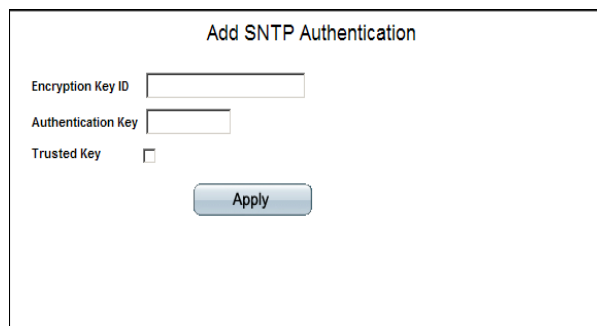
The *SNTP Authentication Page* contains the following fields:

- **Enable SNTP Authentication** — Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:

- *Checked* — Authenticates SNTP sessions between the device and SNTP server.
- *Unchecked* — Disables authenticating SNTP sessions between the device and SNTP server.
- **Encryption Key ID** — Indicates the Key Identification used to authenticate the SNTP server and device. The field value is up to 4294967295 characters.
- **Authentication Key** — Displays the key used for authentication.
- **Trusted Key** — Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.

STEP 2 Click the **Add** button. The *Add SNTP Authentication Page* opens:

Add SNTP Authentication Page



The screenshot shows a web form titled "Add SNTP Authentication". It contains three input fields: "Encryption Key ID" (a text box), "Authentication Key" (a text box), and "Trusted Key" (a checkbox). Below these fields is a blue "Apply" button.

The *Add SNTP Authentication Page* contains the following fields:

- **Encryption Key ID** — Defines the Key Identification used to authenticate the SNTP server and device. The field value is up to 4294967295 characters.
- **Authentication Key** — Defines the key used for authentication.
- **Trusted Key** — Indicates if an encryption key is used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The SNTP Authentication is defined, and the device is updated.

Configuring Device Security

The Security Suite contains the following topics:

- Passwords Management
- Defining Authentication
- Defining Access Methods
- Defining Traffic Control
- Defining 802.1X
- Defining Access Control
- Defining DoS Prevention
- Defining DHCP Snooping
- Defining Dynamic ARP Inspection

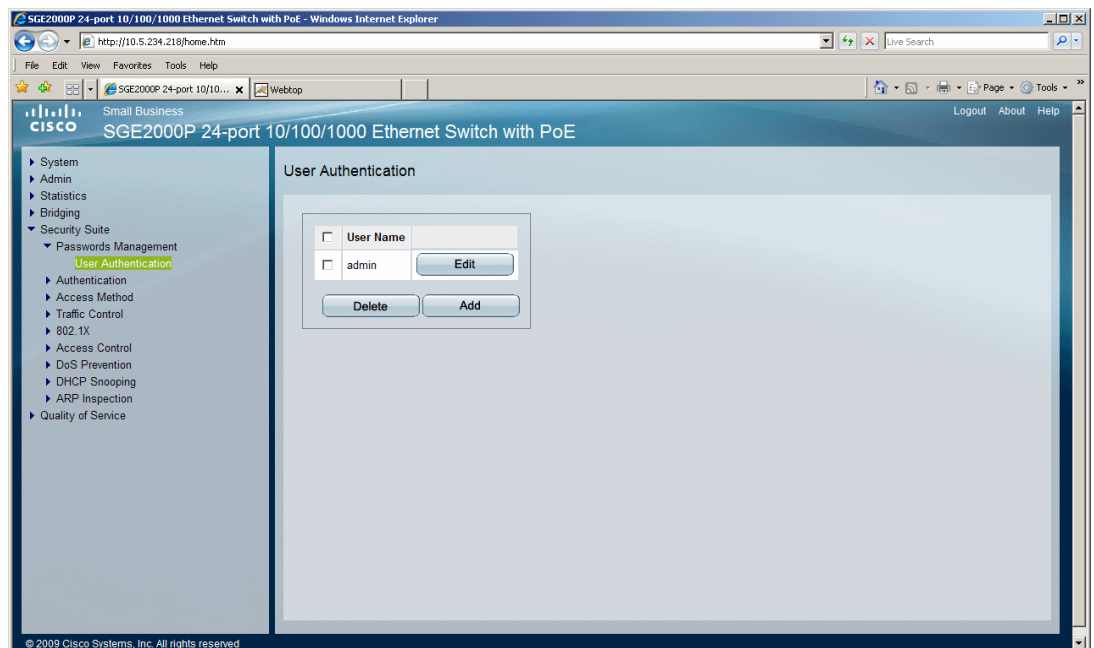
Passwords Management

This section contains information for defining passwords. Passwords are used to authenticate users accessing the device. By default, a single user name is defined, *admin*, with the password *admin*. An additional user name/ password can also be configured.

To define Passwords:

- STEP 1** Click **Security Suite > Passwords Management > User Authentication**. The *User Authentication Page* opens:

User Authentication Page



The *User Authentication Page* contains the following fields:

- **User Name** — Displays the user name.

- STEP 2** Click the **Add** button. The *Add Local User Page* opens:

Add Local User Page

Add Local User

| | |
|-------------------------|--|
| User Name | <input style="width: 90%;" type="text"/> |
| Password | <input style="width: 90%;" type="password"/> |
| Confirm Password | <input style="width: 90%;" type="password"/> |

The *Add Local User Page* contains the following fields:

- **User Name** — Displays the user name.

- **Password** — Specifies the new password. The is not displayed. As it entered an * corresponding to each character is displayed in the field. (Range: 1-159 characters)
- **Confirm Password** — Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.

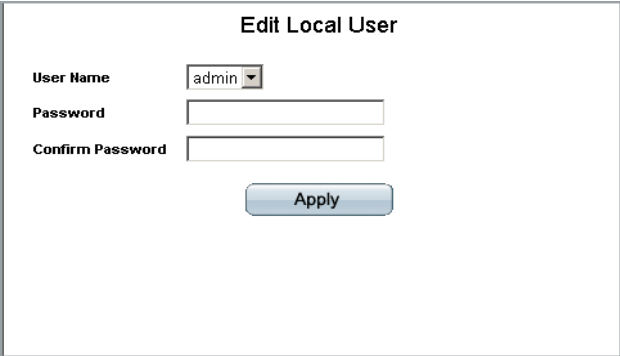
STEP 3 Click the **Delete** button to cancel the selected Profile Name.

Modifying the Local User Settings

STEP 1 Click **Security Suite > Passwords Management > User Authentication**. The *User Authentication Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Local User Page* opens:

Edit Local User Page



The screenshot shows a web form titled "Edit Local User". It contains three input fields: "User Name" with a dropdown menu showing "admin", "Password" with a text box, and "Confirm Password" with a text box. Below the fields is an "Apply" button.

The *Edit Local User Page* contains the following fields:

- **User Name** — Displays the user name.
- **Password** — Specifies the new password. The password is not displayed. As it entered an * corresponding to each character is displayed in the field. (Range: 1-159 characters)
- **Confirm Password** — Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.

STEP 3 Define the relevant fields.

Click **Apply**. The local user settings are modified, and the device is updated.

Defining Authentication

The Authentication section contains the following pages:

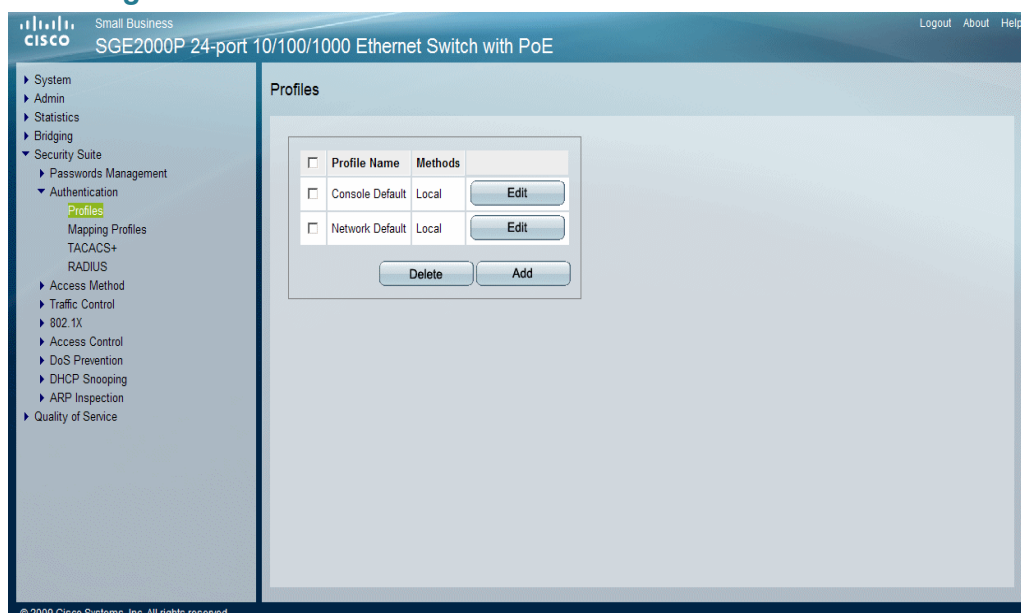
- Defining Profiles
- Mapping Authentication Profiles
- Defining TACACS+
- Defining RADIUS

Defining Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

STEP 1 Click **Security Suite > Authentication > Profiles**. The *Profiles Page* opens:

Profiles Page



The *Profiles Page* contains the following fields:

- **Profile Name** — Displays the Profile name defined for the Login Table.
- **Methods** — Defines the user authentication methods. The order of the authentication methods defines the order in which authentication is attempted. For example, if the authentication method order is RADIUS, Local, the system first attempts to authenticate the user on a RADIUS server. If there is no available RADIUS server, then authentication is attempted on the local data base. Note that if the RADIUS server is available, but authentication fails, then the user is denied access. The possible field values are:
 - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
 - *RADIUS* — Authenticates the user at the RADIUS server.
 - *TACACS+* — Authenticates the user at the TACACS+ server.
 - *None* — Indicates that no authentication method is used to authenticate the user.

STEP 2 Click the **Add** button. The *Add Authentication Profile Page* opens:

Add Authentication Profile Page

The screenshot shows a web interface for adding an authentication profile. It includes a text field for the profile name, a list of optional authentication methods (Local, RADIUS, TACACS+, None), and a list of selected methods. Navigation arrows are provided between the two lists, and an 'Apply' button is at the bottom.

The *Add Authentication Profile Page* contains the following fields:

- **Profile Name** — Displays the Authentication profile name.
- **Authentication Method** — Defines the user authentication methods. The order of the authentication methods defines the order in which authentication is attempted. For example, if the authentication method order is RADIUS, Local, the system first attempts to authenticate the user on a RADIUS server. If there is no available RADIUS server, then authentication is attempted on the local data base. Note that if the RADIUS server is available, but authentication fails, then the user is denied access. The possible field values are:
 - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No option can be inserted below *Local*.
 - *RADIUS* — Authenticates the user at the RADIUS server.
 - *TACACS+* — Authenticates the user at the TACACS+ server.
 - *None* — Indicates that no authentication method is used to authenticate the user. No option can be inserted below *None*.

STEP 3 Click the **Delete** button to delete the *Authentication Profile*.

Modifying an Authentication Profile

STEP 1 Click **Security Suite > Authentication > Profiles**. The *Profiles Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Authentication Profile Page* opens:

Edit Authentication Profile Page

The screenshot shows a web interface titled "Add Authentication Profile". It contains a text input field for "Profile Name". Below this is a section for "Authentication Method". This section is divided into two columns: "Optional Methods" and "Selected Methods". The "Optional Methods" column contains a list box with the items "Local", "RADIUS", "TACACS+", and "None". Between the two columns are two small buttons with right-pointing arrows. The "Selected Methods" column contains an empty list box. At the bottom of the form is a blue "Apply" button.

The *Edit Authentication Profile Page* contains the following fields:

- **Profile Name** — Displays the Authentication profile name.
- **Authentication Methods** — Defines the user authentication methods. The possible field values are:
 - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
 - *RADIUS* — Authenticates the user at the RADIUS server.
 - *TACACS+* — Authenticates the user at the TACACS+ server.
 - *None* — Indicates that no authentication method is used to authenticate the device.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The authentication profile is defined, the device is updated.

Mapping Authentication Profiles

After authentication profiles are defined, authentication profiles can be applied to management access methods. For example, console users can be authenticated by one authentication profile, while Telnet users are authenticated by another authentication profile.

Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

The *Mapping Profiles Page* contains parameters for mapping authentication methods. To map authentication profiles:

- STEP 1** Click **Security Suite > Authentication > Mapping Profiles**. The *Mapping Profiles Page* opens:

Mapping Profiles Page

The screenshot shows the 'Mapping Profiles' configuration page for a Cisco Small Business SGE2000P switch. The left sidebar contains a navigation tree with 'Mapping Profiles' highlighted. The main content area has three sections: 'Console', 'Telnet', and 'Secure Telnet (SSH)'. Each section has a dropdown menu for selecting a profile. Below these are sections for 'Secure HTTP' and 'HTTP', each with 'Optional Methods' and 'Selected Methods' lists. The 'Optional Methods' list includes 'RADIUS', 'TACACS+', and 'None'. The 'Selected Methods' list currently contains 'Local'. An 'Apply' button is at the bottom.

The *Mapping Profiles Page* contains the following fields:

- **Console** — Indicates that Authentication profiles are used to authenticate console users.
- **Telnet** — Indicates that Authentication profiles are used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Indicates that Authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

- **Secure HTTP** — Configures the device Secure HTTP settings.

Optional Methods — Lists available authentication methods.

- *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No authentication method can be added under *Local*.
- *RADIUS* — *Remote Authorization Dial-In User Service* (RADIUS) servers provide additional security for networks.
- *TACACS+* — *Terminal Access Controller Access Control System* (TACACS+) provides centralized security user access validation.
- *None* — Indicates that no authentication method is used to authenticate the device. No authentication method can be added under *None*.

Selected Methods — Selects authentication methods from the methods offered in the Optional methods area.

- **HTTP** — Configures the device HTTP settings.

Optional Methods — Lists available authentication methods.

- *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No authentication method can be added under *Local*.
- *RADIUS* — *Remote Authorization Dial-In User Service* (RADIUS) servers provide additional security for networks.
- *TACACS+* — *Terminal Access Controller Access Control System* (TACACS+) provides centralized security user access validation.
- *None* — Indicates that no authentication method is used to authenticate the device. No authentication method can be added under *None*.

Selected Methods — Selects authentication methods from the methods offered in the Optional methods area.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The authentication profile is defined, the device is updated.

Defining TACACS+

The devices provide *Terminal Access Controller Access Control System* (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers. The *TACACS+ Page* contains fields for assigning the Default Parameters for the TACACS+ servers. TACACS+ is supported on IPv4 and not on IPv6.

To define TACACS+:

STEP 1 Click **Security Suite > Authentication > TACACS+**. The *TACACS+ Page* opens:

TACACS+ Page

The screenshot shows the TACACS+ configuration page. On the left is a navigation menu with options like System, Admin, Statistics, Bridging, Security Suite, Passwords Management, Authentication, Profiles, Mapping Profiles, TACACS+, RADIUS, Access Method, Traffic Control, 802.1X, Access Control, DoS Prevention, DHCP Snooping, ARP Inspection, and Quality of Service. The main area is titled 'TACACS+' and contains the following fields:

- Default Parameters**
 - Supported IP Format**: Version 4
 - Source IPv4 Address**: 0.0.0.0
 - Key String**: (empty field)
 - Timeout for Reply**: 5 (Sec)
- Table** (for multiple servers):

| Host IP Address | Priority | Source IP Address | Authentication Port | Timeout for Reply | Single Connection | Status |
|--------------------------|----------|-------------------|---------------------|-------------------|-------------------|--------|
| <input type="checkbox"/> | | | | | | |

Buttons at the bottom include 'Apply', 'Delete', and 'Add'.

The *TACACS+ Page* contains the following fields:

- **Supported IP Format** — TACACS+ is supported only on IPv4.
- **Source IPv4 Address** — Displays the device source IPv4 address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- **Timeout for Reply** — Displays the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.

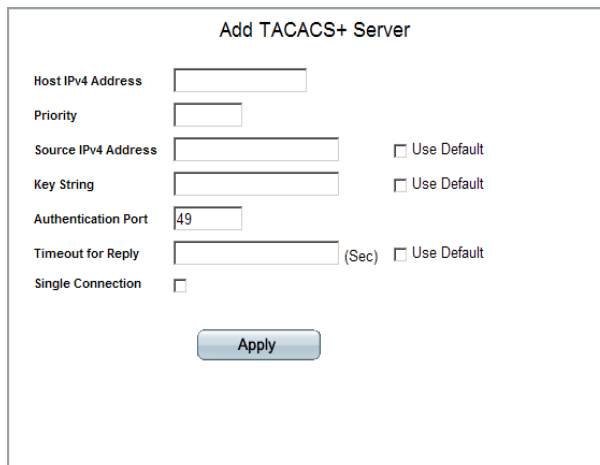
The following parameters are configured for each TACACS+ server:

- **Host IP Address** — Displays the TACACS+ Server IP address.
- **Priority** — Displays the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port** — Displays the port number through which the TACACS+ session occurs. The default is port 49.

- **Timeout for Reply** — Displays the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server when selected.
- **Status** — Displays the connection status between the device and the TACACS+ server. The possible field values are:
 - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
 - *Not Connected* — Indicates there is no current connection between the device and the TACACS+ server.

STEP 2 Click the **Add** button. The *Add TACACS+ Server Page* opens:

Add TACACS+ Server Page



The screenshot shows the 'Add TACACS+ Server' configuration page. It contains the following fields and options:

- Host IPv4 Address**: A text input field.
- Priority**: A text input field.
- Source IPv4 Address**: A text input field with a checkbox labeled 'Use Default' to its right.
- Key String**: A text input field with a checkbox labeled 'Use Default' to its right.
- Authentication Port**: A text input field containing the value '49'.
- Timeout for Reply**: A text input field with '(Sec)' to its right and a checkbox labeled 'Use Default' to its right.
- Single Connection**: A checkbox.
- Apply**: A button at the bottom center.

The *Add TACACS+ Server Page* contains the following fields:

- **Host IPv4 Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The default is 0.
- **Source IPv4 Address** — Defines the device source IPv4 address used for the TACACS+ session between the device and the TACACS+ server. The possible values are:
 - **User Defined** — Allows the user to define the source IPv4 Address.

- **Use Default** — Uses the default value for the parameter. If *Use Default* check box is selected, the global value of 0.0.0.0. is used and interpreted as a request to use the IP address of the outgoing IP interface.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server. The possible values are:
 - **User Defined** — Allows the user to define the Key String value.
 - **Use Default** — Uses the default value for the parameter. If *Use Default* check box is selected, the global value is used which is an empty string.
- **Authentication Port** — Defines the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** — Defines the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
 - **User Defined** — Allows the user to define the *Timeout for Reply* value.
 - **Use Default** — Uses the default value for the parameter. If *Use Default* check box is selected, the default is 5 seconds.
- **Single Connection** — Enables a single open connection between the device and the TACACS+ server when selected.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The TACACS+ server is added, and the device is updated.

Modifying TACACS+ Settings

STEP 1 Click **Security Suite > Authentication > TACACS+**. The *TACACS+ Page* opens:

STEP 2 Click the **Edit** Button. The *Edit TACACS+ Server Page* opens:

Edit TACACS+ Server Page

The screenshot shows the 'Edit TACACS+ Server' configuration window. It includes the following fields and options:

- Host IP Address:** A dropdown menu showing '10.10.10.10'.
- Priority:** A text input field containing '1'.
- Source IP Address:** A text input field containing '10.10.10.10' with a '(X.X.X.X)' hint and a 'Use Default' checkbox.
- Key String:** A text input field with a 'Use Default' checkbox.
- Authentication Port:** A text input field containing '49'.
- Timeout for Reply:** A text input field containing '30' with a '(Sec)' hint and a 'Use Default' checkbox.
- Status:** A label showing 'Not Connected'.
- Single Connection:** A checkbox that is currently unchecked.
- Apply:** A button at the bottom center.

The *Edit TACACS+ Server Page* contains the following fields:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Defines the device source IPv4 address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- **Authentication Port** — Defines the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** — Defines the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- **Status** — Displays the connection status between the device and the TACACS+ server. The possible field values are:
 - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
 - *Not Connected* — Indicates there is no current connection between the device and the TACACS+ server.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server when selected
- **Use Default** — Indicates that the factory default value is used.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The authentication profile is defined, the device is updated.

Defining RADIUS

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access. The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To define RADIUS:

STEP 1 Click **Security Suite > Authentication > RADIUS**. The *RADIUS Page* opens:

RADIUS Page

The *RADIUS Page* contains the following fields:

- **Radius Accounting** — Defines the authentication method used for RADIUS session accounting. Possible field values are:
 - *802.1X* — 802.1X authentication is used to initiate accounting.
 - *Login* — Login authentication is used to initiate accounting.

- *Both* — Both 802.1X and login authentication are used to initiate accounting.
 - *None* — No authentication is used to initiate accounting.
- **Supported IP Format** — Indicates whether Ipv4 or Ipv6 are supported.
- **Default Retries** — Provides the default retries.
- **Default Timeout for Reply** — Provides the device default Timeout for Reply.
- **Default Dead Time** — Provides the device default Dead Time.
- **Default Key String** — Provides the device default Default Key String.
- **Source IPv4 Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Source IPv6 Address** — Defines the source IP address that is used for communication with RADIUS servers.

The following parameters are configured for each RADIUS server:

- **IP Address** — Displays the Authentication Server IP addresses.
- **Priority** — Indicates the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Displays the Authentication port's IP address.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server.
- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.

- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
 - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
 - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
 - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.

STEP 2 Click the **Add** button. The *Add RADIUS Server Page* opens:

Add RADIUS Server Page

The *Add RADIUS Server Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - *Version6* — Indicates the device supports IPv6.
 - *Version4* — Indicates the device supports IPv4.
- **IPv6 Address type** — Displays the IPv6 Type. The possible field value is:

- *Global* — Indicates the IPv6 address is a global Unicast IPV6 type which is visible and reachable from different subnets.
- **Host IP Address** — Displays the *RADIUS* Server IP address.
- **Priority** — Displays the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server.
- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
 - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
 - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
 - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.

- **Use Default** — Uses the default value for the parameter.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The RADIUS Server is added, and the device is updated.

Modifying RADIUS Server Settings

STEP 1 Click **Security Suite > Authentication > RADIUS**. The *RADIUS Page* opens:

STEP 2 Click the **Edit** button. The *Edit RADIUS Server Page* opens:

Edit RADIUS Server Page

| Field | Value | Use Default |
|---------------------|------------------------|-------------------------------------|
| IP Address | 10.10.10.10 | <input type="checkbox"/> |
| Priority | 0 | <input type="checkbox"/> |
| Source IP Address | Default | <input checked="" type="checkbox"/> |
| Authentication Port | 1812 | <input type="checkbox"/> |
| Accounting Port | 1813 | <input type="checkbox"/> |
| Number of Retries | Default | <input checked="" type="checkbox"/> |
| Timeout for Reply | Default (Sec) | <input checked="" type="checkbox"/> |
| Dead Time | Default (Min) | <input checked="" type="checkbox"/> |
| Key String | Default (Alphanumeric) | <input checked="" type="checkbox"/> |
| Usage Type | All | <input type="checkbox"/> |

Apply

The *Edit RADIUS Server Page* contains the following fields:

- **IP Address** — Defines the RADIUS Server IP address.
- **Priority** — Displays the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Authentication Port** — Displays the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server.

- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
 - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
 - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
 - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.
- **Use Default** — Uses the default value for the parameter.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The RADIUS Server is modified, and the device is updated.

Defining Access Methods

The access method section contains the following pages:

- Defining Access Profiles
- Defining Profile Rules

Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The Access Profile Page contains the currently configured access profiles and their activity status. Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

To define access profiles:

- STEP 1** Click **Security Suite > Access Method > Access Profiles**. The *Access Profiles Page* opens:

Access Profiles Page

| Access Profile Name | Current Active Access Profile |
|---------------------|----------------------------------|
| None | <input checked="" type="radio"/> |
| Console Only | <input type="radio"/> |

Delete Add

The *Access Profiles Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Current Active Access Profile** — Defines the access profile currently active.

- STEP 2** Click the **Add** button. The *Add Access Profile Page* opens:

Add Access Profile Page

The *Add Access Profile Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - *Version 6* — Indicates the device supports IPv6.
 - *Version 4* — Indicates the device supports IPv4.
- **IPv6 Address Type** — Displays the IPv6 Type. The possible field values are:
 - *Link Local* — Indicates the IPv6 address is link-local, that uniquely identifies hosts on a single network link. A Link-local address has a prefix of 'FE80'. The link-local addresses are not routable and can be used for communication on the same network only.
 - *Global Unicast* — Indicates the IPv6 address is a global Unicast IPV6 type which is visible and reachable from different subnets.
- **Link Local Interface** — Displays the VLAN ID on which IPv6 is configured.
- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:

- *All* — Assigns all management methods to the rule.
- *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
- *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
 - *Port* — Specifies the port on which the access profile is defined.
 - *LAG* — Specifies the LAG on which the access profile is defined.
 - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
 - *Permit* — Permits access to the device.
 - *Deny* — Denies access to the device. This is the default.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The access profile is added, and the device is updated.

Defining Profile Rules

Access profiles can contain up to 128 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- IP Address
- Prefix Length
- Forwarding Action

To define profile rules:

- STEP 1** Click **Security Suite > Access Method > Profile Rules**. The *Profile Rules Page* opens:

Profile Rules Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Security Suite
 Passwords Management
 Authentication
 Access Method
 Access Profiles
 Profile Rules
 Traffic Control
 802.1X
 Access Control
 DoS Prevention
 DHCP Snooping
 ARP Inspection
 Quality of Service

Profile Rules

Access Profile Name: Console Only

| <input type="checkbox"/> | Priority | Interface | Management Method | Source IP Address | Prefix Length | Action | |
|-------------------------------------|----------|-----------|-------------------|-------------------|---------------|--------|------|
| <input checked="" type="checkbox"/> | 1 | | All | 0.0.0.0 | /32 | Deny | Edit |

Delete Add

© 2009 Cisco Systems, Inc. All rights reserved

The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
 - *Port* — Attaches the rule to the selected port.
 - *LAG* — Attaches the rule to the selected LAG.
 - *VLAN* — Attaches the rule to the selected VLAN.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
 - *All* — Assigns all management methods to the rule.

- *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
- *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
- *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
 - *Permit* — Permits access to the device.
 - *Deny* — Denies access to the device. This is the default.

Adding Profile Rules

STEP 2 Click the **Add** button. The *Add Profile Rule Page* opens:

Add Profile Rule Page

The *Add Profile Rule Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - *Version 6* — Indicates the device supports IPv6.
 - *Version 4* — Indicates the device supports IPv4.
- **IPv6 Address type** — Displays the IPv6 Type. The possible field values are:
 - *Link Local* — Indicates the IPv6 address is link-local, that uniquely identifies hosts on a single network link. A Link-local address has a prefix of 'FE80'. The link-local addresses are not routable and can be used for communication on the same network only.
 - *Global Unicast* — Indicates the IPv6 address is a global Unicast IPV6 type which is visible and reachable from different subnets.
- **Link Local Interface** — Displays the VLAN ID on which IPv6 is configured.
- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.

- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
 - *All* — Assigns all management methods to the rule.
 - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
 - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
 - *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
 - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
 - *Port* — Specifies the port on which the access profile is defined.
 - *LAG* — Specifies the LAG on which the access profile is defined.
 - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.

- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
 - *Permit* — Permits access to the device.
 - *Deny* — Denies access to the device. This is the default.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The profile rule is added, and the device is updated.

Modifying Profile Rules

STEP 1 Click **Security Suite > Access Method > Profile Rules**. The *Profile Rules Page* opens:

STEP 2 Click the **Edit** button. The *Edit Profile Rule Page* opens:

Edit Profile Rule Page

The *Edit Profile Rule Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:

- *Version 6* — Indicates the device supports IPv6.
- *Version 4* — Indicates the device supports IPv4.
- **IPv6 Address type** — Displays the IPv6 Type. The possible field values are:
 - *Link Local* — Indicates the IPv6 address is link-local, that uniquely identifies hosts on a single network link. A Link-local address has a prefix of 'FE80'. The link-local addresses are not routable and can be used for communication on the same network only.
 - *Global* — Indicates the IPv6 address is a global Unicast IPV6 type which is visible and reachable from different subnets.
- **Link Local Interface** — Displays the VLANID on which IPv6 is configured.
- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
 - *All* — Assigns all management methods to the rule.
 - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
 - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
 - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
 - *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.

- *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
 - *Port* — Specifies the port on which the access profile is defined.
 - *LAG* — Specifies the LAG on which the access profile is defined.
 - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
 - *Permit* — Permits access to the device.
 - *Deny* — Denies access to the device. This is the default.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The profile rule is modified, and the device is updated.

Defining Traffic Control

The Traffic Control section contains the following topics:

- Defining Storm Control
- Defining Port Security

Defining Storm Control

Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports.

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Storm Control is enabled per port by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port and discards the frames when the rate exceeds a user-defined rate.

The *Storm Control Page* provides fields for configuring Broadcast Storm Control.

To define storm control:

- STEP 1** Click **Security Suite** > **Traffic Control** > **Storm Control**. The *Storm Control Page* opens:

Storm Control Page

Small Business
Cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Security Suite
 Passwords Management
 Authentication
 Access Method
 Traffic Control
 Storm Control
 Port Security
 802.1X
 Access Control
 DoS Prevention
 DHCP Snooping
 ARP Inspection
 Quality of Service

Storm Control

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

| # | Port | Enable Broadcast Control | Broadcast Rate Threshold | Broadcast Mode | |
|----|-------|--------------------------|--------------------------|----------------|------|
| 1 | 2/g1 | Disabled | 3500 | Broadcast Only | Edit |
| 2 | 2/g2 | Disabled | 3500 | Broadcast Only | Edit |
| 3 | 2/g3 | Disabled | 3500 | Broadcast Only | Edit |
| 4 | 2/g4 | Disabled | 3500 | Broadcast Only | Edit |
| 5 | 2/g5 | Disabled | 3500 | Broadcast Only | Edit |
| 6 | 2/g6 | Disabled | 3500 | Broadcast Only | Edit |
| 7 | 2/g7 | Disabled | 3500 | Broadcast Only | Edit |
| 8 | 2/g8 | Disabled | 3500 | Broadcast Only | Edit |
| 9 | 2/g9 | Disabled | 3500 | Broadcast Only | Edit |
| 10 | 2/g10 | Disabled | 3500 | Broadcast Only | Edit |
| 11 | 2/g11 | Disabled | 3500 | Broadcast Only | Edit |
| 12 | 2/g12 | Disabled | 3500 | Broadcast Only | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *Storm Control Page* contains the following fields:

- **Copy From Entry Number** — Copies the storm control configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied storm control configuration to the specified table entry.
- **Unit Number** — Displays the stacking member for which the storm control parameters are displayed.
- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — The possible field values are:
 - *Enable* — Enables Storm Control
 - *Disable* — Disables Storm Control. This is the default value.
- **Broadcast Rate Threshold** — Indicates the maximum rate (kilobits per second) at which unknown packets are forwarded.
 - For FE ports, the rate is 70 - 100,000 Kbps.
 - For GE ports, the rate is 35,000 - 100,000 Kbps.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:
 - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
 - *Broadcast Only* — Counts only Broadcast traffic.
 - *Unknown Unicast, Multicast & Broadcast* — Counts Unknown Unicast, Broadcast and Multicast traffic together. This option is available on GE ports only. On FE devices, this option can only be set globally for the device from the *Storm Control Page*.

STEP 2 Define the relevant fields.

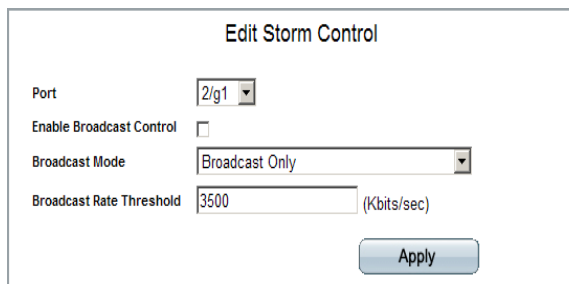
STEP 3 Click **Apply**. Storm control of the device is updated.

Modifying Storm Control

STEP 1 Click **Security Suite > Traffic Control > Storm Control**. The *Storm Control Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Storm Control Page* opens:

Edit Storm Control Page



The screenshot shows a web-based configuration interface titled "Edit Storm Control". It contains the following fields:

- Port:** A dropdown menu with "2/g1" selected.
- Enable Broadcast Control:** An unchecked checkbox.
- Broadcast Mode:** A dropdown menu with "Broadcast Only" selected.
- Broadcast Rate Threshold:** A text input field containing "3500" with "(Kbits/sec)" as a unit label.
- Apply:** A button at the bottom right.

The *Edit Storm Control Page* contains the following fields:

- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — The possible field values are:
 - *Checked* — Enables Storm Control.
 - *Unchecked* — Disables Storm Control.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the interface. The possible field values are:
 - *Unknown Unicast, Multicast & Broadcast* — Counts Unknown Unicast, Broadcast and Multicast traffic together. This option is available on GE ports only. On FE devices, this option can only be set globally for the device from the *Storm Control Page*.
 - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
 - *Broadcast Only* — Counts only Broadcast traffic.
- **Broadcast Rate Threshold** — Displays the maximum rate (packets per second) at which unknown packets are forwarded.
 - For FE ports, the rate is 70 - 100,000 Kbps.
 - For GE ports, the rate is 35,000 - 100,000 Kbps.

STEP 3 Modify the relevant fields.

STEP 4 Click **Apply**. Storm control is modified, and the device is updated.

Defining Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- Cause the port to be shut down.

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset. Disabled ports are activated from the *Port Security Page*.

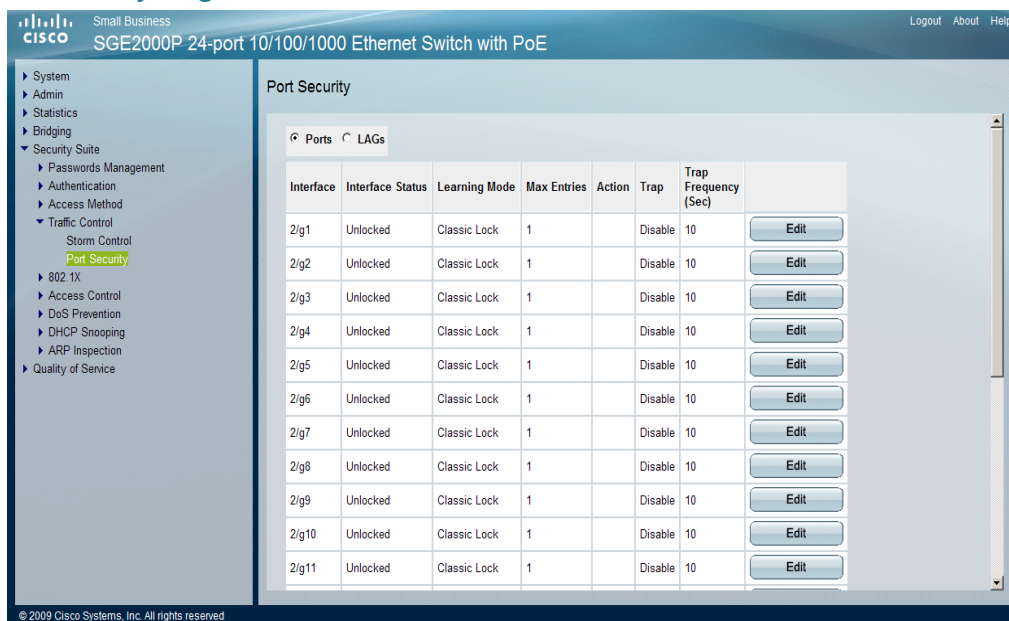


NOTE To configure port lock, 802.1x multiple host mode must be enabled.

To define port security:

STEP 1 Click **Security Suite > Traffic Control > Port Security**. The *Port Security Page* opens:

Port Security Page



The *Port Security Page* contains the following fields:

- **Ports of Unit** — Indicates the port number and stacking member on which port security is configured.
- **LAGs** — Indicates the LAG number on which port security is configured.
- **Interface** — Displays the port or LAG name.
- **Interface Status** — Indicates the port security status. The possible field values are:
 - *Unlocked* — Indicates the port is currently unlocked. This is the default value.
 - *Locked* — Indicates the port is currently locked.
- **Learning Mode** — Defines the locked port type. The *Learning Mode* field is enabled only if *Locked* is selected in the *Interface Status* field. In order to change the *Learning Mode*, the *Lock Interface* must be set to *Unlocked*. Once the mode is changed, the *Lock Interface* can be reinstated. The possible field values are:

- *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
- *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.
- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The possible range is 1-128. The default is 1.
- **Action** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
 - *Discard* — Discards packets from any unlearned source. This is the default value.
 - *Forward* — Forwards packets from an unknown source without learning the MAC address.
 - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
 - *Enable* — Enables traps.
 - *Disable* — Disables traps.
- **Trap Frequency (Sec)** — Displays the amount of time (in seconds) between traps. The default value is 10 seconds.

STEP 2 Define the relevant fields.

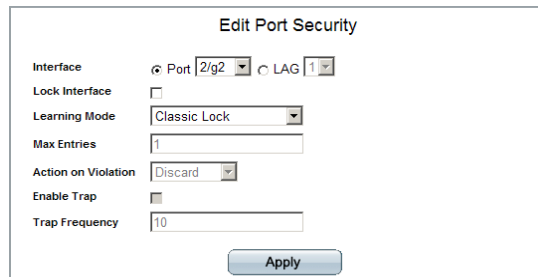
STEP 3 Click **Apply**. Port security is defined, and the device is updated.

Modifying Port Security

STEP 1 Click **Security Suite > Traffic Control > Port Security**. The *Port Security Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Port Security Page* opens:

Edit Port Security Page



The screenshot shows the 'Edit Port Security' configuration window. It contains the following fields and controls:

- Interface:** A dropdown menu with radio buttons for 'Port' (selected) and 'LAG'. The selected value is '2/g2' for Port and '1' for LAG.
- Lock Interface:** A checkbox that is currently unchecked.
- Learning Mode:** A dropdown menu with 'Classic Lock' selected.
- Max Entries:** A text input field containing the value '1'.
- Action on Violation:** A dropdown menu with 'Discard' selected.
- Enable Trap:** A checkbox that is currently unchecked.
- Trap Frequency:** A text input field containing the value '10'.
- Apply:** A button at the bottom right of the form.

The *Edit Port Security Page* contains the following fields:

- **Interface** — Select the port or LAG name.
- **Lock Interface** — Indicates the port security status. The possible field values are:
 - *Unchecked* — Indicates the port is currently unlocked. This is the default value.
 - *Checked* — Indicates the port is currently locked.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated. The possible field values are:
 - *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
 - *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.
- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the

Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The possible range is 1-128. The default is 1.

- **Action on Violation** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
 - *Discard* — Discards packets from any unlearned source. This is the default value.
 - *Forward* — Forwards packets from an unknown source without learning the MAC address.
 - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Enable Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
 - *Checked* — Enables traps.
 - *Unchecked* — Disables traps.
- **Trap Frequency** — Displays the amount of time (in seconds) between traps. The default value is 10 seconds.

STEP 3 Modify the relevant fields.

STEP 4 Click **Apply**. Port security is modified, and the device is updated.

Defining 802.1X

802.1x Port Base Network Access Control allows access to a switch port by authenticated and authorized device(s) attached to the port, and prevents access to the port in cases the authentication and authorization fail. Port Authentication includes:

- **Authenticators** — A port that enforces authentication of the remote device (suplicants) before permitting port access.
- **Suplicants** — A remote device attaching to a port seeking port access.

- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

The 802.1X section contains the following topics:

- Defining 802.1X Properties
- Defining Port Authentication
- Defining Authentication
- Defining Authenticated Hosts

Defining 802.1X Properties

The *802.1X Properties Page* provides parameters for enabling port authentication, and selecting the authentication method. To define port based authentication:

STEP 1 Click **Security Suite > 802.1X > Properties**. The *802.1X Properties Page* opens:

802.1X Properties Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE configuration interface. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging, Security Suite, Passwords Management, Authentication, Access Method, Traffic Control, 802.1X, Properties (highlighted), Port Authentication, Authentication, Authenticated Hosts, Access Control, DoS Prevention, DHCP Snooping, ARP Inspection, and Quality of Service. The main content area is titled 'Properties' and contains the following fields: Port Based Authentication State (set to 'Disable'), Authentication Method (set to 'None'), Guest VLAN (checkbox), and Guest VLAN ID (dropdown). An 'Apply' button is located below the fields. The footer of the interface reads '© 2009 Cisco Systems, Inc. All rights reserved'.

The *802.1X Properties Page* contains the following fields:

- **Port Based Authentication State** — Enables Port-based Authentication on the device. The possible field values are:

- *Enable* — Enables port-based authentication on the device.
 - *Disable* — Disables port-based authentication on the device.
- **Authentication Method** — Defines the user authentication methods. The possible field values are:
 - *RADIUS, None* — Indicates port authentication is performed first via the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then the *None* option is used, and the session is permitted.
 - *RADIUS* — Authenticates the user at the RADIUS server.
 - *None* — No authentication method is used to authenticate the port.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
 - *Checked* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
 - *Unchecked* — Disables use of a Guest VLAN for unauthorized ports. This is the default.
- **Guest VLAN ID** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

STEP 2 Modify the relevant fields.

STEP 3 Click **Apply**. The 802.1X properties are modified, and the device is updated.

Defining Port Authentication

The *802.1X Port Authentication Page* provides parameters for defining 802.1X on ports.

STEP 1 Click **Security Suite > 802.1X > Port Authentication**. The *802.1X Port Authentication Page* opens:

802.1X Port Authentication Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Port Authentication

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

| # | Port | User Name | Current Port Control | Guest VLAN | Authentication Method | Periodic Reauthentication | Reauthentication Period | Authenticator State | Quiet Period | Resending EAP |
|----|-------|------------|----------------------|-------------|-----------------------|---------------------------|-------------------------|---------------------|--------------|---------------|
| 1 | 2/g1 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 2 | 2/g2 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 3 | 2/g3 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 4 | 2/g4 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 5 | 2/g5 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 6 | 2/g6 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 7 | 2/g7 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 8 | 2/g8 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 9 | 2/g9 | * | Disable | 802.1x Only | Disable | 3600 | Initialize | 60 | 30 | 2 |
| 10 | 2/g10 | Authorized | Disable | 802.1x Only | Disable | 3600 | Force Authorized | 60 | 30 | 2 |

© 2009 Cisco Systems, Inc. All rights reserved

The *802.1X Port Authentication Page* contains the following fields:

- **Copy from Entry Number** — Copies the port authentication configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied port authentication configuration to the specified table entry.
- **Unit Number** — Displays the stacking member for which the port authentication parameters are displayed.
- **Port** — Displays the list of interfaces.
- **User Name** — Displays the user name.
- **Current Port Control** — Displays the current port authorization state.
- **Guest VLAN** — Displays the Guest VLAN.
- **Authentication Method** — Displays the authentication method in use.
- **Periodic Reauthentication** — Enables port reauthentication. The default value is disabled.

- **Reauthentication Period** — Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Authenticator State** — Specifies the port authorization state. The possible field values are as follows:
 - *ForceAuthorized* — Indicates the controlled port state is set to Force-Authorized (forward traffic).
 - *ForceUnauthorized* — Indicates the controlled port state is set to Force-Unauthorized (discard traffic).
 - *Initialize* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
- **Quiet Period** — Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange (Range: 0-65535).
- **Resending EAP** — Specifies the number of seconds that the switch waits for a response to an EAP - request/identity frame, from the supplicant (client), before resending the request.
- **Max EAP Requests** — Indicates the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the number of seconds that lapses before EAP requests are resent to the supplicant (Range: 1-65535). The field default is 30 seconds.
- **Server Timeout** — Specifies the number of seconds that lapses before the switch resends a request to the authentication server (Range: 1-65535). The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The 802.1X port authentication settings are defined, and the device is updated.

Modifying 802.1X Security

STEP 1 Click **Security Suite > 802.1X > Port Authentication**. The *802.1X Properties Page* opens:

STEP 2 Click the **Edit** button. The *Port Authentication Settings Page* opens:

Port Authentication Settings Page

| | |
|----------------------------------|--------------------------|
| Port | 2/g1 |
| User Name | |
| Current Port Control | Authorized |
| Admin Port Control | forceAuthorized |
| Enable Guest VLAN | <input type="checkbox"/> |
| Authentication Method | 802.1x Only |
| Enable Periodic Reauthentication | <input type="checkbox"/> |
| Reauthentication Period | 3600 |
| Reauthenticate Now | <input type="checkbox"/> |
| Authenticator State | Initialize |
| Quiet Period | 60 (Sec) |
| Resending EAP | 30 (Sec) |
| Max EAP Requests | 2 |
| Supplicant Timeout | 30 (Sec) |
| Server Timeout | 30 (Sec) |
| Termination Cause | Port re-initialize |

Apply

The *Port Authentication Settings Page* contains the following fields:

- **Port** — Indicates the port on which port-based authentication is enabled.
- **User Name** — Displays the user name.
- **Current Port Control** — Displays the current port authorization state.
- **Admin Port Control** — Defines the admin port authorization state. The possible field values are:
 - *Auto* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
 - *ForceAuthorized* — Indicates the interface is in an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.

- *ForceUnauthorized* — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Enable Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
 - *Checked* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
 - *Unchecked* — Disables port-based authentication on the device. This is the default.
- **Authentication Method** — Defines the user authentication method. The possible field values are:
 - *802.1x Only* — Enables only 802.1x authentication on the device.
 - *MAC Only* — If enabled, causes the port to transition to the authorized or unauthorized state based on the supplicant's MAC address.
 - *802.1x & MAC* — Enables 802.1x + MAC Authentication on the device. In the case of 802.1x + MAC, 802.1x takes precedence.
- **Enable Periodic Reauthentication** — Permits port reauthentication during the specified Reauthentication Period (see below). The possible field values are:
 - *Checked* — Enables immediate port reauthentication. This is the default value.
 - *Unchecked* — Disables port reauthentication.
- **Reauthentication Period** — Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Reauthenticate Now** — Specifies that authentication is applied on the device when the **Apply** button is pressed.
 - *Checked* — Enables immediate port reauthentication.
 - *Unchecked* — Port authentication according to the Reauthentication settings above.
- **Authenticator State** — Specifies the port authorization state. The possible field values are as follows:

- *Force-Authorized* — Indicates the controlled port state is set to Force-Authorized (forward traffic).
 - *Force-Unauthorized* — Indicates the controlled port state is set to Force-Unauthorized (discard traffic).
- **Quiet Period** — Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange (Range: 0-65535).
- **Resending EAP** — Specifies the number of seconds that the switch waits for a response to an EAP - request/identity frame, from the supplicant (client), before resending the request.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the number of seconds that lapses before EAP requests are resent to the supplicant (Range: 1-65535). The field default is 30 seconds.
- **Server Timeout** — Specifies the number of seconds that lapses before the switch resends a request to the authentication server (Range: 1-65535). The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated, if applicable.

STEP 3 Modify the relevant fields.

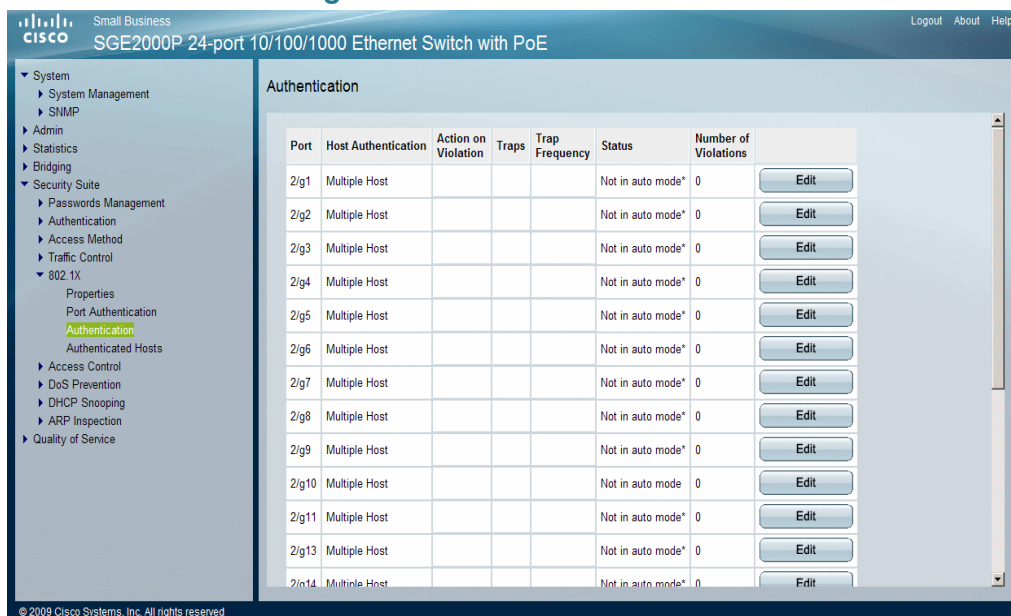
STEP 4 Click **Apply**. The port authentication settings are defined, and the device is updated.

Defining Authentication

The *802.1X Authentication Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs.

STEP 1 Click **Security Suite > 802.1X > Authentication**. The *802.1X Authentication Page* opens:

802.1X Authentication Page



The *802.1X Authentication Page* contains the following fields:

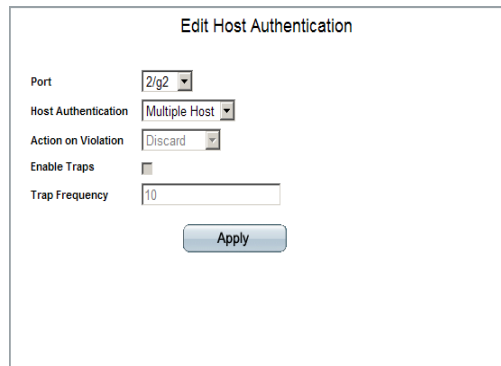
- **Unit Number** — Displays the stacking member for which the Multiple Hosts configuration is displayed.
- **Port** — Displays the port number for which the Multiple Hosts configuration is displayed.
- **Host Authentication**— Defines the Host Authentication mode. The possible field values are:
 - *Single* — Only the authorized host can access the port.
 - *Multiple Host* — Multiple hosts can be attached to a single 802.1x-enabled port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
 - *Multi Session* — Enables number of specific authorized hosts to get access to the port. Filtering is based on the source MAC address.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:

- *Forward* — Forwards the packet.
 - *Discard* — Discards the packets. This is the default value.
 - *Shutdown* — Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
 - *Enable* — Indicates that traps are enabled for Multiple hosts.
 - *Disable* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- **Status** — Indicates the host status. If there is an asterisk *, the port is either not linked or is down. The possible field values are:
 - *Unauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
 - *Force-Authorized* — Indicates that the port control is Forced Authorized, and clients have full port access.
 - *Single-host Lock* — Indicates that the port control is Auto and only a single client has been authenticated via the port.
 - *Multiple Hosts* — Indicates that the port control is Auto and Multiple Hosts mode is enabled. One client has been authenticated.
 - *Multiple Sessions* — Indicates that the port control is Auto and Multiple Sessions mode is enabled. At least one client has been authenticated.
 - *Number of Violations* — Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

Modifying Authentication Settings

STEP 2 Click the **Edit** button. The *Edit Authentication Page* opens:

Edit Authentication Page



The screenshot shows a web-based configuration interface titled "Edit Host Authentication". It contains several fields: "Port" with a dropdown menu showing "2/g2"; "Host Authentication" with a dropdown menu showing "Multiple Host"; "Action on Violation" with a dropdown menu showing "Discard"; "Enable Traps" with an unchecked checkbox; and "Trap Frequency" with a text input field containing "10". An "Apply" button is located at the bottom right of the form.

The *Edit Authentication Page* contains the following fields:

- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Host Authentication**— Defines the Host Authentication mode. The possible field values are:
 - *Single* — Only the authorized host can access the port.
 - *Multiple Host* — Multiple hosts can be attached to a single 802.1x-enabled port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
 - *Multi Session* — Enables number of specific authorized hosts to get access to the port. Filtering is based on the source MAC address.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
 - *Discard* — Discards the packets. This is the default value.
 - *Forward* — Forwards the packet.
 - *Shutdown* — Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- **Enable Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
 - *Checked* — Indicates that traps are enabled for Multiple hosts.
 - *Unchecked* — Indicates that traps are disabled for Multiple hosts.

- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.

STEP 3 Modify the relevant fields.

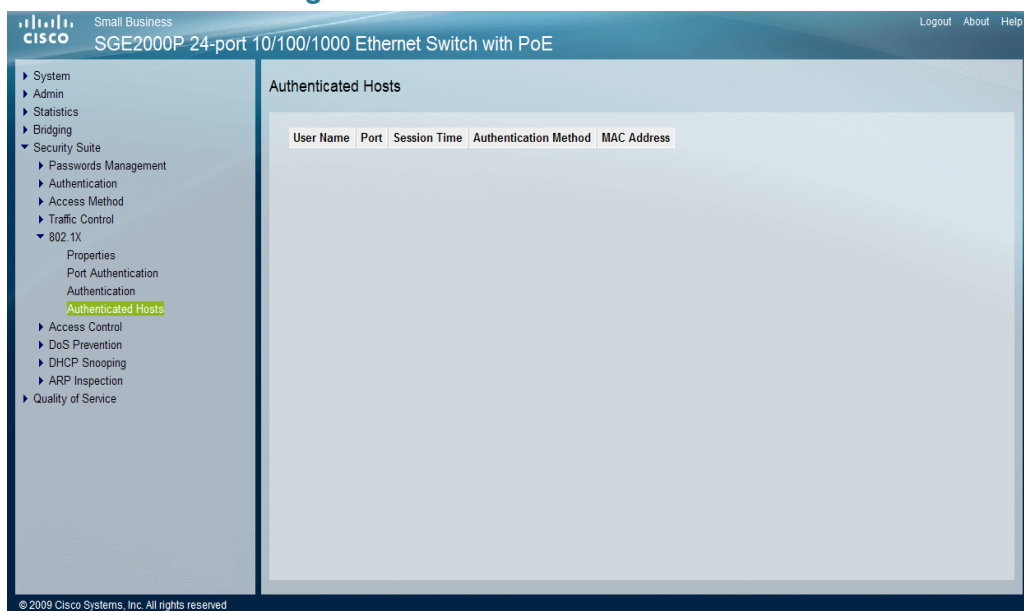
STEP 4 Click **Apply**. The settings are defined, and the device is updated.

Defining Authenticated Hosts

The *Authenticated Hosts Page* contains a list of authenticated users.

STEP 1 Click **Security Suite > 802.1X > Authenticated Hosts**. The *Authenticated Hosts Page* opens:

Authenticated Hosts Page



The *Authenticated Hosts Page* contains the following fields:

- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- **Session time** — Displays the amount of time (in seconds) the supplicant was logged on the port.

- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
 - *Remote* — Indicates the 802.1x authentication is not used on this port (port is forced-authorized).
 - *None* — Indicates the supplicant was not authenticated.
 - *RADIUS* — Indicates the supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

STEP 2 Modify the relevant fields.

STEP 3 Click **Apply**. The settings are defined, and the device is updated.

Defining Access Control

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 256 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. If they are denied entry, the user can disable the port. ACLs are composed of *Access Control Entries (ACEs)* that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 256.

The Access Control section contains the following topics:

- Defining MAC Based ACL
- Defining IP Based ACL
- Defining IPv6 Based ACLs
- Defining ACL Binding

Defining MAC Based ACL

The *MAC Based ACL Page* allows a MAC-based *Access Control List (ACL)* to be defined. The table lists *Access Control Elements (ACE)* rules, which can be added only if the ACL is not bound to an interface.

To define the MAC Based ACL:

- STEP 1** Click **Security Suite > Access Control > MAC Based ACL**. The *MAC Based ACL Page* opens:

MAC Based ACL Page

Small Business
Cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

MAC Based ACL

ACL Name

| <input type="checkbox"/> | Priority | Source | Destination | VLAN ID | Inner VLAN | 802.1p | 802.1p Mask | Ether Type | Action |
|--------------------------|----------|------------------|------------------|---------|------------|--------|-------------|------------|--------|
| | | MAC Address Mask | MAC Address Mask | | | | | | |
| | | | | | | | | | |

Delete Rule Add Rule

Delete ACL Add ACL

© 2009 Cisco Systems, Inc. All rights reserved

The *MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Defines the source MAC address to match the ACE.
- **Source MAC Mask** — Defines the source MAC mask to match the ACE.
- **Destination MAC Address** — Defines the destination MAC address to match the ACE.
- **Destination MAC Mask** — Defines the destination MAC mask to the which packets are matched.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4093.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.

- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **EtherType** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. For example, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. Possible field values are:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the Edit Interface Settings Page.

STEP 2 To remove an ACL, click the **Delete ACL** button.

STEP 3 To remove an ACE rule, click the rule's checkbox and click the **Delete Rule** button.

STEP 4 Click the **Add ACL** button. The *Add MAC Based ACL Page* opens:

Add MAC Based ACL Page

The *Add MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.

- **New Rule Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address:**
 - *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
 - *Wildcard Mask* — Indicates the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **Dest. MAC Address:**
 - *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
 - *Wildcard Mask* — Indicates the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcards bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:

- *Permit* — Forwards packets which meet the ACL criteria.
- *Deny* — Drops packets which meet the ACL criteria.
- *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

STEP 5 Define the relevant fields.

STEP 6 Click **Apply**. The MAC Based ACL is defined, and the device is updated.

Adding Rule to MAC Based ACL

STEP 1 Select an existing ACL.

STEP 2 Click the **Add Rule** button. The *Add MAC Based Rule Page* opens:

Add MAC Based Rule Page

The screenshot shows the 'Add MAC Based Rule' configuration page. The fields are as follows:

- ACL Name:** a
- New Rule Priority:** (empty text box)
- Source MAC Address:** (radio button icon) (empty text box)
- Wildcard Mask:** (empty text box) ☐ Any
- Dest. MAC Address:** (radio button icon) (empty text box)
- Wildcard Mask:** (empty text box) ☐ Any
- VLAN ID:** (empty text box)
- Inner VLAN:** (empty text box)
- 802.1p:** (empty text box)
- 802.1p Mask:** (empty text box)
- Ethertype:** (empty text box)
- Action:** Permit (dropdown menu)
- Apply:** (button)

The *Add MAC Based Rule Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **New Rule Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address**

- **MAC Address** — Matches the source MAC address from which packets are addressed to the ACE.
- **Wildcard Mask** — Indicates the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **Destination MAC Address**
 - **MAC Address** — Matches the destination MAC address to which packets are addressed to the ACE.
 - **Wildcard Mask** — Indicates the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:
 - **Permit** — Forwards packets which meet the ACL criteria.
 - **Deny** — Drops packets which meet the ACL criteria.
 - **Shutdown** — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The ACL Rule is defined, and the device is updated.

Modifying MAC Based ACL

STEP 1 Click **Security Suite > Access Control > MAC Based ACL**. The *MAC Based ACL Page* opens.

STEP 2 Click the **Edit** button. The *Rule Settings Page* opens:

Rule Settings Page

Rule Settings

| | | | |
|--------------------|--|---------------|--|
| ACL Name | acl1 | | |
| New Rule Priority | 1 | | |
| Source MAC Address | <input type="text" value="aa:bb:cc:aa:bb:cc"/> | Wildcard Mask | <input type="text" value="11:cc:dd:11:ee:21"/> C Any |
| Dest. MAC Address | <input type="text" value="11:cc:dd:11:ee:ee"/> | Wildcard Mask | <input type="text" value="11:cc:dd:11:ee:19"/> C Any |
| VLAN ID | 1 | | |
| Inner VLAN | <input type="text"/> | | |
| 802.1p | <input type="text"/> | | |
| 802.1p Mask | <input type="text"/> | | |
| Ethertype | <input type="text"/> | | |
| Action | Permit <input type="button" value="v"/> | | |

The *Rule Settings Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Source MAC Address:**
 - *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
 - *Wildcard Mask* — Indicates the source MAC Address wildcard mask. Wildcards are used to mask all or part of a source MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets

are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.

- **Destination MAC Address:**

- *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
- *Wildcard Mask* — Indicates the destination MAC Address wildcard mask. Wildcards are used to mask all or part of a destination MAC Address. Wildcard masks specify which octets are used and which octets are ignored. A wildcard mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.

- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The Rule settings are modified, and the device is updated.

Defining IP Based ACL

The *IP Based ACL Page* contains information for defining IP Based ACLs, including defining the ACEs defined for IP Based ACLs.

To define an IP based ACL:

- STEP 1** Click **Security Suite > Access Control > IP Based ACL**. The *IP Based ACL Page* opens:

IP Based ACL Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Security Suite
 Passwords Management
 Authentication
 Access Method
 Traffic Control
 802.1X
 Access Control
 MAC Based ACL
 IP Based ACL
 IPv6 Based ACL
 ACL Binding
 DoS Prevention
 DHCP Snooping
 ARP Inspection
 Quality of Service

IP Based ACL

ACL Name

* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

| <input type="checkbox"/> | Rule Priority | Protocol | Source Port | Dest. Port | Flag Set | ICMP Type | ICMP Code | IGMP Type | Source | Destination | DSCP | IP.Prec. |
|--------------------------|---------------|----------|-------------|------------|----------|-----------|-----------|-----------|-----------------|-----------------|------|----------|
| | | | | | | | | | IP Address Mask | IP Address Mask | | |
| | | | | | | | | | | | | |

Delete Rule

Delete ACL

© 2009 Cisco Systems, Inc. All rights reserved

The *IP Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. The possible field values are:
 - *ICMP* — *Internet Control Message Protocol* (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
 - *IGMP* — *Internet Group Management Protocol* (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

- *IP* — *Internet Protocol* (IP). Specifies the format of packets and their addressing method. IP addresses packets and forwards the packets to the correct port.
- *TCP* — *Transmission Control Protocol* (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order they are sent.
- *EGP* — *Exterior Gateway Protocol* (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
- *IGP* — *Interior Gateway Protocol* (IGP). Allows for routing information exchange between gateways in an autonomous network.
- *UDP* — *User Datagram Protocol* (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
- *HMP* — *Host Mapping Protocol* (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
- *RDP* — *Remote Desktop Protocol* (RDP). Allows a clients to communicate with the Terminal Server over the network.
- *IDPR* — Matches the packet to the *Inter-Domain Policy Routing* (IDPR) protocol.
- *IPv6* — *Internet Routing Protocol version 6* (IPv6). Provides a newer version of the Internet Protocol, and follows *IP version 4* (IPv4). IPv6 increases the IP address size from 32 bits to 128 bits. In addition, IPv6 support more levels of addressing hierarchy, more addressable nodes, and supports simpler auto-configuration of addresses.
- *IPv6:ROUTE* — Matches packets to the *IPv6 Route through a Gateway* (IPv6:ROUTE).
- *IPv6:FRAG* — Matches packets to the *IPv6 Fragment Header* (IPv6:FRAG).
- *IDRP* — Matches the packet to the *Inter-Domain Routing Protocol* (IDRP).
- *RSVP* — Matches the packet to the *ReSerVation Protocol* (RSVP).
- *AH* — *Authentication Header* (AH). Provides source host authentication and data integrity.

- *IPv6:ICMP* — Matches packets to the Matches packets to the IPv6 and *Internet Control Message Protocol*.
 - *EIGRP* — *Enhanced Interior Gateway Routing Protocol* (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
 - *OSPF* — The *Open Shortest Path First* (OSPF) protocol is a link-state, hierarchical *Interior Gateway Protocol* (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate *Virtual Private Networks* (VPNs).
 - *IPIP* — *IP over IP* (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensure that IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
 - *PIM* — Matches the packet to *Protocol Independent Multicast* (PIM).
 - *L2TP* — Matches the packet to *Layer 2 Internet Protocol* (L2IP).
 - *ISIS* — *Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks.
 - *ANY* — Matches the protocol to any protocol.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
 - **Dest. Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
 - **Flag Set** — Sets the indicated TCP flag that can be triggered.
 - **ICMP Type** — Filters packets by ICMP message type. The field values is 0-255.
 - **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
 - **IGMP Type** — Filters packets by IGMP message or message types.
 - **Source**

- **IP Address** — Displays the source port IP address to which packets are addressed to the ACE.
- **Wildcard Mask** — Displays the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination**
 - **IP Address** — Displays the destination port IP address to which packets are addressed to the ACE.
 - **Wildcard Mask** — Displays the destination IP address wildcard mask.
- **DCSP** — Matches the packets DSCP value.
- **IP Prec** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Delete ACL button** — To remove an ACL, click the **Delete ACL** button.
- **Delete Rule button** — To remove an ACE rule, click the rule's checkbox and click the **Delete Rule** button.

STEP 2 Click the **Add ACL** button. The *Add IP Based ACL Page* opens:

Add IP Based ACL Page

The screenshot shows the 'Add IP Based ACL' configuration page. It contains the following fields and controls:

- ACL Name:** A text input field.
- New Rule Priority:** A checkbox and a text input field.
- Protocol:** A dropdown menu with 'ICMP' selected.
- Protocol ID to Match:** A text input field.
- Source Port:** A text input field with a 'Any' link.
- Destination Port:** A text input field with a 'Any' link.
- TCP Flags:** A checkbox and a row of dropdowns for Urg, Ack, Psh, Rst, Syn, and Fin.
- ICMP:** A checkbox, a dropdown for 'Echo-Reply', and a dropdown for 'ICMP Type'.
- ICMP Code:** A text input field with a 'Any' link.
- IGMP:** A checkbox, a dropdown for 'DVMRP', and a dropdown for 'IGMP Type'.
- Source IP Address:** A text input field with a 'Wild Card Mask' field and a 'Any' link.
- Destination IP Address:** A text input field with a 'Wild Card Mask' field and a 'Any' link.
- Traffic Class:** A checkbox and a dropdown for 'Match DSCP'.
- Action:** A dropdown menu with 'Permit' selected.
- Match IP Precedence:** A text input field.
- Apply:** A button at the bottom right.

The *Add IP Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IP Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
 - **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
 - **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
 - **IGMP** — Filters packets by IGMP message or message types.

- **ICMP** — Filters packets by ICMP message type. The field values is 0-255.
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP Type** — Filters packets by IGMP message or message types.
- **Source IP Address** — Matches the source port IP address from which packets are addressed to the ACE.
 - *Wildcard Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
 - *Wildcard Mask* — Defines the destination IP address of the wildcard mask.
- **Traffic Class** — Indicates the traffic class to which the packets are matched. Select either **Match DSCP** or **Match IP Precedence**.
 - *Match DSCP* — Matches the packet to the DSCP tag value. The possible field range is 0-63.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 3 Define the relevant fields,

STEP 4 Click **Apply**. The IP Based ACL is defined, and the device is updated.

Modifying IP Based ACL

STEP 1 Click **Security Suite > Access Control > IP Based ACL**. The *IP Based ACL Page* opens.

STEP 2 Click the **Edit** button. The *Edit IP Based ACL Page* opens:

Edit IP Based ACL Page

Edit IP Based ACL

ACL Name: 22

New Rule Priority: 2

Protocol: Select from List: ICMP Protocol ID to Match: Any

Source Port: Any

Destination Port: Any

TCP Flags: Urg Set Ack Set Psh Set Rst Set Syn Set Fin Set

ICMP: Select from List: Echo-Reply ICMP Type: 0 Any

ICMP Code: Any

IGMP: Select from List: DVMRP IGMP Type: 19 Any

Source IP Address: Any Wild Card Mask: Any

Destination IP Address: Any Wild Card Mask: Any

Traffic Class: Match DSCP Match IP Precedence

Action: Permit

Apply

The *Edit IP Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IPv6 based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IPv6 Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.

- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP** — Filters packets by IGMP message or message types.
- **Source**
 - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
 - *Wildcard Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination**
 - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
 - *Wildcard Mask* — Defines the destination IP address of the wildcard mask.
- **Traffic Class** — Indicates the traffic class to which the packet is matched. Select either **Match DSCP** or **Match IP Precedence**.
 - *Match DSCP* — Matches the packet to the DSCP tag value.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.

- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 3 Define the relevant fields,

STEP 4 Click **Apply**. The IP Based ACL is modified, and the device is updated.

Defining Rules Associated with IP-ACL

STEP 1 Click **Security Suite >Access Control > IP Based ACL**. The *IP Based ACL Page* opens:

STEP 2 Click the **Add Rule** button. The *Rules Associated with IP-ACL Page* opens:

Rules Associated with IP-ACL Page

Add IP Based Rule

ACL Name: 22

New Rule Priority:

Protocol: ☐ Select from List: ICMP ☐ Protocol ID to Match: ☐ Any

Source Port: ☐ Any

Destination Port: ☐ Any

TCP Flags: ☐ Urg: Set ☐ Ack: Set ☐ Psh: Set ☐ Rst: Set ☐ Syn: Set ☐ Fin: Set

ICMP: ☐ Select from List: Echo-Reply ☐ ICMP Type: 0 ☐ Any

ICMP Code: ☐ Any

IGMP: ☐ Select from List: DVMRP ☐ IGMP Type: 19 ☐ Any

Source IP Address: Wild Card Mask: ☐ Any

Destination IP Address: Wild Card Mask: ☐ Any

Traffic Class: ☐ ☐ Match DSCP: ☐ Match IP Precedence:

Action: Permit

The *Rules Associated with IP-ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
 - **ICMP** — Indicates if ICMP packets are permitted on the network.
 - **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
 - **IGMP** — Filters packets by IGMP message or message types.

- **Source IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
- **Dest. IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
- **Traffic Class** — Indicates the traffic class to which the packet is matched. Select either **Match DSCP** or **Match IP Precedence**.
 - *Match DSCP* — Matches the packet to the DSCP tag value.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 3 Select an ACL from the ACL Name drop-down list.

STEP 4 Click the **Add Rule** button. The *Add IP Based Rule Page* opens:

Add IP Based Rule Page

Add IP Based Rule

ACL Name: 22

New Rule Priority:

Protocol: ☐ Select from List: ICMP ☐ Protocol ID to Match: ☐ Any

Source Port: ☐ ☐ Any

Destination Port: ☐ ☐ Any

TCP Flags: ☐ Urg: Set ☐ Ack: Set ☐ Psh: Set ☐ Rst: Set ☐ Syn: Set ☐ Fin: Set

ICMP: ☐ Select from List: Echo-Reply ☐ ICMP Type: 0 ☐ Any

ICMP Code: ☐ ☐ Any

IGMP: ☐ Select from List: DVMRP ☐ IGMP Type: 19 ☐ Any

Source IP Address: ☐ Wild Card Mask: ☐ Any

Destination IP Address: ☐ Wild Card Mask: ☐ Any

Traffic Class: ☐ Match DSCP: ☐ Match IP Precedence:

Action: Permit

The *Add IP Based Rule Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IP Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.

- **IGMP** — Filters packets by IGMP message or message types.
- **Source IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
- **Dest. IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
- **Traffic Class** — Indicates the traffic class to which the packet is matched. Select either **Match DSCP** or **Match IP**:
 - *Match DSCP* — Matches the packet to the DSCP tag value.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management Page*.

STEP 5 Define the relevant fields,

STEP 6 Click **Apply**. The IP Based rules are modified, and the device is updated.

Defining IPv6 Based ACLs

The *IPv6 Based ACL Page* contains information for defining IPv6 Based ACLs, including defining the ACEs defined for IPv6 Based ACLs.

STEP 1 Click **Security Suite >Access Control > IPv6 Based ACL**. The *IPv6 Based ACL Page* opens:

IPv6 Based ACL Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Security Suite
 Passwords Management
 Authentication
 Access Method
 Traffic Control
 802.1X
 Access Control
 MAC Based ACL
 IP Based ACL
 IPv6 Based ACL
 ACL Binding
 DoS Prevention
 DHCP Snooping
 ARP Inspection
 Quality of Service

IPv6 Based ACL

ACL Name

* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

| <input type="checkbox"/> | Rule Priority | Protocol | Source Port | Dest. Port | Flag Set | ICMP Type | ICMP Code | Source | | Destination | | DSCP | IP-Prec |
|--------------------------|---------------|----------|-------------|------------|----------|-----------|-----------|------------|---------------|-------------|---------------|------|---------|
| | | | | | | | | IP Address | Prefix Length | IP Address | Prefix Length | | |
| | | | | | | | | | | | | | |

Delete Rule Add Rule

Delete ACL Add ACL

© 2009 Cisco Systems, Inc. All rights reserved.

The *IPv6 Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol.
 - *ICMP* — *Internet Control Message Protocol* (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
 - *IGMP* — *Internet Group Management Protocol* (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.
 - *IP* — *Internet Protocol* (IP). Specifies the format of packets and their addressing method. IP addresses packets and forwards the packets to the correct port.

- *TCP — Transmission Control Protocol* (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order the are sent.
- *EGP — Exterior Gateway Protocol* (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
- *IGP — Interior Gateway Protocol* (IGP). Allows for routing information exchange between gateways in an autonomous network.
- *UDP — User Datagram Protocol* (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
- *HMP — Host Mapping Protocol* (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
- *RDP — Remote Desktop Protocol* (RDP). Allows a clients to communicate with the Terminal Server over the network.
- *IDPR — Matches the packet to the Inter-Domain Policy Routing* (IDPR) protocol.
- *IPV6 — Internet Routing Protocol version 6* (IPv6). Provides a newer version of the Internet Protocol, and follows *IP version 4* (IPv4). IPv6 increases the IP address size from 32 bits to 128 bits. In addition, IPv6 support more levels of addressing hierarchy, more addressable nodes, and supports simpler auto-configuration of addresses.
- *IPV6:ROUTE — Matches packets to the IPv6 Route through a Gateway* (IPV6:ROUTE).
- *IPV6:FRAG — Matches packets to the IPv6 Fragment Header* (IPV6:FRAG).
- *IDRP — Matches the packet to the Inter-Domain Routing Protocol* (IDRP).
- *RSVP — Matches the packet to the ReSerVation Protocol* (RSVP).
- *AH — Authentication Header* (AH). Provides source host authentication and data integrity.
- *IPV6:ICMP — Matches packets to the Matches packets to the IPv6 and Internet Control Message Protocol*.

- *EIGRP* — *Enhanced Interior Gateway Routing Protocol* (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
 - *OSPF* — The *Open Shortest Path First* (OSPF) protocol is a link-state, hierarchical *Interior Gateway Protocol* (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate *Virtual Private Networks* (VPNs).
 - *IPIP* — *IP over IP* (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensure that IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
 - *PIM* — Matches the packet to *Protocol Independent Multicast* (PIM).
 - *L2TP* — Matches the packet to *Layer 2 Internet Protocol* (L2IP).
 - *ISIS* — *Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks.
 - *ANY* — Matches the protocol to any protocol.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
 - **Dest. Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
 - **Flag Set** — Sets the indicated TCP flag that can be triggered.
 - **ICMP Type** — Filters packets by ICMP message type. The field values is 0-255.
 - **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
 - **Source**
 - **IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
 - **Prefix Length** — Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.

- **Destination**
 - **IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
 - **Prefix Length** — Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.
- **DCSP** — Matches the packets DSCP value.
- **IP-Prec.** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 2 Click the **Add ACL** button. The *Add IPv6 Based ACL Page* opens:

Add IPv6 Based ACL Page

The screenshot shows the 'Add IPv6 Based ACL' configuration page. The fields are as follows:

- ACL Name:** A text input field.
- New Rule Priority:** A checkbox labeled 'New Rule Priority' followed by a text input field.
- Protocol:** Radio buttons for 'Select from List' (with a dropdown menu showing 'TCP') and 'Protocol ID to Match' (with a text input field). A radio button labeled 'Any' is also present.
- Source Port:** Radio buttons for a text input field and 'Any'.
- Destination Port:** Radio buttons for a text input field and 'Any'.
- TCP Flags:** A checkbox labeled 'TCP Flags' followed by dropdown menus for Urg, Ack, Psh, Rst, Syn, and Fin, each with 'Dont Care' as a default option.
- ICMP:** Radio buttons for 'Select from List' (with a dropdown menu showing 'Destination Unreachable (1)') and 'ICMP Type' (with a text input field). A radio button labeled 'Any' is also present.
- ICMP Code:** Radio buttons for a text input field and 'Any'.
- Source IP Address:** Radio buttons for a text input field and 'Prefix Length' (with a text input field). A radio button labeled 'Any' is also present.
- Destination IP Address:** Radio buttons for a text input field and 'Prefix Length' (with a text input field). A radio button labeled 'Any' is also present.
- Traffic Class:** A checkbox labeled 'Traffic Class' followed by radio buttons for 'Match DSCP' (with a text input field) and 'Match IP Precedence' (with a text input field).
- Action:** A dropdown menu showing 'Permit'.
- Apply:** A button at the bottom right.

The *Add IPv6 Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IP Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
 - *ICMP* — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:.

- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **Source**
 - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
 - *Prefix Length* — Matches the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.
- **Destination**
 - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
 - *Prefix Length* — Matches the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.
- **Traffic Class** — Indicates the traffic class to which the packet is matched. Select either **Match DSCP** or **Match IP Precedence**.
 - *Match DSCP* — Matches the packet to the DSCP tag value.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 3 Define the relevant fields,

STEP 4 Click **Apply**. The IP Based ACL is defined, and the device is updated.

Modifying IPv6 Based ACL

STEP 1 Click **Security Suite >Access Control > IPv6 Based ACL**. The *Edit IPv6 Based ACL Page* opens.

STEP 2 Click the **Edit** button. The *Edit IP Based ACL Page* opens:

Edit IPv6 Based ACL Page

The screenshot shows the 'Edit IP Based ACL' configuration page. The fields are as follows:

- ACL Name:** 22
- New Rule Priority:** 2
- Protocol:** Select from List: ICMP
- Source Port:** Any
- Destination Port:** Any
- TCP Flags:** Urg (Set), Ack (Set), Psh (Set), Rst (Set), Syn (Set), Fin (Set)
- ICMP:** Select from List: Echo-Reply
- ICMP Code:** Any
- IGMP:** Select from List: DVMRP
- IGMP Type:** 19
- Source IP Address:** Any
- Destination IP Address:** Any
- Traffic Class:** Match DSCP, Match IP Precedence
- Action:** Permit

An **Apply** button is located at the bottom right of the form.

The *Edit IPv6 Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IPv6 based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IPv6 Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu. The possible field range is 0 - 65535.

- **TCP Flags** — Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **Source**
 - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
 - *Prefix Length* — Matches the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.
- **Destination**
 - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
 - *Prefix Length* — Matches the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash /.
- **Traffic Class** — Indicates the traffic class to which the packet is matched. Select either **Match DSCP** or **Match IP Precedence**.
 - *Match DSCP* — Matches the packet to the DSCP tag value.
 - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

STEP 3 Define the relevant fields,

STEP 4 Click **Apply**. The IP Based ACL is modified, and the device is updated.

Defining ACL Binding

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on a port or a LAG flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets. To bind ACLs to an interface:

STEP 1 Click **Security Suite > Access Control > ACL Binding**. The *ACL Binding Page* opens:

ACL Binding Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Binding
Security Suite
 Passwords Management
 Authentication
 Access Method
 Traffic Control
 802.1X
 Access Control
 MAC Based ACL
 IP Based ACL
 IPv6 Based ACL
 ACL Binding
 DoS Prevention
 DHCP Snooping
 ARP Inspection
 Quality of Service

ACL Binding

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

☒ Ports ☐ LAGs

| <input type="checkbox"/> | # | Interface | ACL Name | Type | |
|--------------------------|----|-----------|----------|------|------|
| <input type="checkbox"/> | 1 | 2/g1 | | | Edit |
| <input type="checkbox"/> | 2 | 2/g2 | | | Edit |
| <input type="checkbox"/> | 3 | 2/g3 | | | Edit |
| <input type="checkbox"/> | 4 | 2/g4 | | | Edit |
| <input type="checkbox"/> | 5 | 2/g5 | | | Edit |
| <input type="checkbox"/> | 6 | 2/g6 | | | Edit |
| <input type="checkbox"/> | 7 | 2/g7 | | | Edit |
| <input type="checkbox"/> | 8 | 2/g8 | | | Edit |
| <input type="checkbox"/> | 9 | 2/g9 | | | Edit |
| <input type="checkbox"/> | 10 | 2/g10 | | | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *ACL Binding Page* contains the following fields:

- **Copy From Entry Number** — Copies the ACL binding configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied ACL binding configuration to the specified table entry.
- **Ports /LAGs** — Indicates the interface to which the ACL is bound.

For each entry, an interface has a bound ACL.

- **Interface** — Indicates the interface to which the associated ACL is bound.
- **ACL Name** — Indicates the ACL which is bound to the associated interface.
- **Type** — Indicates the ACL type to which is bound to the interface.

STEP 2 Modify the relevant fields.

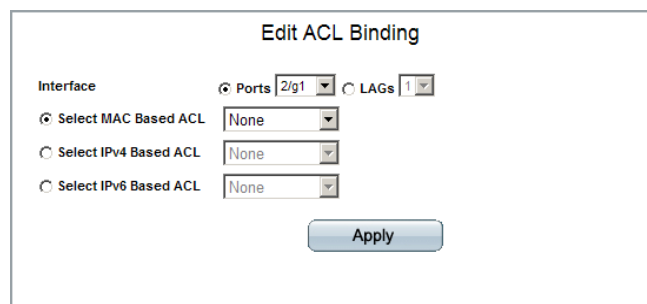
STEP 3 Click **Apply**. The settings are defined, and the device is updated.

Modifying ACL Binding

STEP 1 Click **Security Suite > Access Control > ACL Binding**. The *ACL Binding Page* opens:

STEP 2 Click the **Edit** button. The *Edit ACL Binding Page* opens:

Edit ACL Binding Page



The *Edit ACL Binding Page* contains the following fields:

- **Interface** — Indicates the interface to which the ACL is bound.
- **Select MAC Based ACL** — Indicates the MAC based ACL which is bound to the interface.
- **Select IPv4 Based ACL** — Indicates the IPv4 based ACL which is bound to the interface.
- **Select IPv6 Based ACL** — Indicates the IPv6 based ACL which is bound to the interface.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The ACL binding is defined, and the device is updated.

Defining DoS Prevention

Denial of Service (DOS) increases network security by preventing packets with invalid IP addresses from entering the network. DoS eliminates packets from malicious networks which can compromise a network's stability.

The device provides a Security Suite that allows administrators to match, discard, and redirect packets based on packet header values. Packets which are redirected are analyzed for viruses and Trojans.

DoS enables network managers to:

- Deny packets that contain reserved IP addresses
- Prevent TCP connections from a specific interface
- Discard echo requests from a specific interface
- Discard IP fragmented packets from a specific interface

The DoS Prevention section contains the following topics:

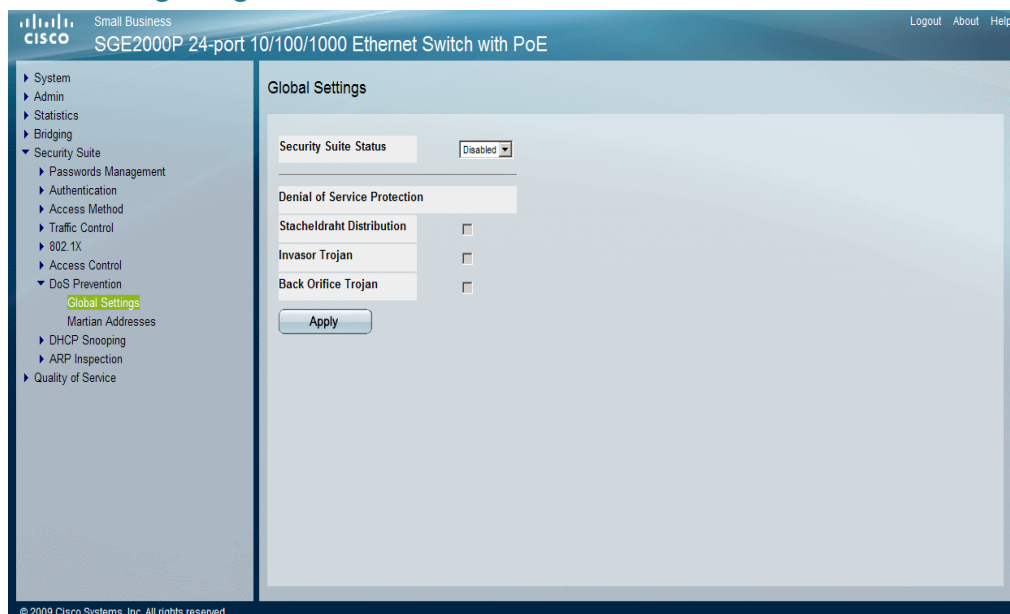
- DoS Global Settings
- Defining Martian Addresses

DoS Global Settings

The *Global Settings Page* allows network managers to enable and define global DoS attack prevention parameters on the device. To open the *Global Settings Page*:

- STEP 1** Click **Security Suite > DoS Prevention > Global Settings**. The *Global Settings Page* opens:

Global Settings Page



The *Global Settings Page* contains the following fields:

- **Security Suite Status** — Indicates if DoS security is enabled on the device. The possible field values are:
 - *Enabled* — Enables DoS security.
 - *Disabled* — Disables DoS security on the device. This is the default value.
- **Denial of Service Protection** — Indicates if any of the services listed below are enabled. If the service protection is disabled, the *Stacheldraht Distribution*, *Invasor Trojan*, and *Back Orifice Trojan* fields are disabled.
- **Stacheldraht Distribution** — Discards TCP packets with source TCP port equal to 16660
- **Invasor Trojan** — Discards TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- **Back Orifice Trojan** — Discards UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

- STEP 2** Define the relevant fields.

-
- STEP 3** Click **Apply**. The DoS prevention global settings are defined, and the device is updated.
-

Defining Martian Addresses

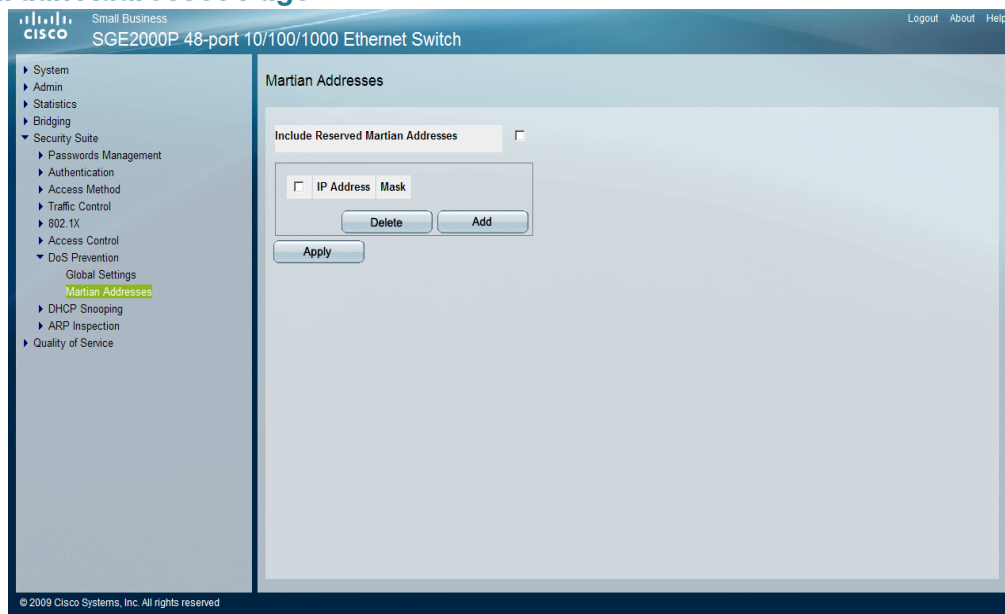
Martian Address Filtering enables discarding IP packets from invalid IP addresses. Martian addresses include packets from a source IP addresses outside or not used within the configured network. Martian addresses include any address within the following ranges:

- **0.0.0.0/8 (Except 0.0.0.0/32 as a Source Address)** — Addresses in this block refer to source hosts on this network.
- **127.0.0.0/8** — Used as the Internet host loopback address.
- **192.0.2.0/24** — Used as the TEST-NET in documentation and example codes.
- **224.0.0.0/4 (As a Source IP Address)** — Used in IPv4 Multicast address assignments, and This formerly known as Class D Address Space.
- **240.0.0.0/4 (Except 255.255.255.255/32 as a Destination Address)** — Reserved address range, and is formerly known as Class E Address Space.

To define Martian Addresses:

STEP 1 Click **Security Suite > DoS Prevention > Martian Addresses**. The *Martian Addresses Page* opens:

Martian Addresses Page



The *Martian Addresses Page* contains the following fields:

- **Include Reserved Martian Addresses** — Indicates that packets arriving from Martian addresses are dropped. Enabled is the default value. When enabled, the following IP addresses are included:
 - 0.0.0.0/8 (except 0.0.0.0/32), 127.0.0.0/8
 - 192.0.2.0/24 , 224.0.0.0/4
 - - 240.0.0.0/4 (except 255.255.255.255/32)
- **IP Address** — Displays the IP addresses for which DoS attack is enabled.
- **Mask** — Displays the Mask for which DoS attack is enabled.

STEP 2 To remove a Martian address, click the entry's checkbox and click the **Delete** button.

STEP 3 Click the **Add** button. The *Add Martian Addresses Page* opens:

Add Martian Addresses Page

Supported IP Format Version 4

IP Address ☐ 10.0.0.0/8 ☒ New IP Address

☒ Mask

☐ Prefix Length

Apply

The *Add Martian Addresses Page* contains the following fields:

- **Supported IP Format** — Indicates only Ipv4 is supported.
- **IP Address** — Enter the Martian IP addresses for which DoS attack is enabled. The possible values are:
 - One of the addresses in the Martian IP address list.
 - New IP Address — Enter an IP Address that is not on the list.
- **Mask** — Enter the Mask for which DoS attack is enabled.
- **Prefix Length** — Defines the IP route prefix for the destination IP.

STEP 4 Define the relevant fields,

STEP 5 Click **Apply**. The Martian Addresses are defined, and the device is updated.

Defining DHCP Snooping

DHCP Snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The *DHCP Snooping Table* contains the untrusted interfaces MAC address, IP address, Lease Time, VLAN ID, and interface information.

The DHCP Snooping section contains the following topics:

- Defining DHCP Snooping Properties
- Defining DHCP Snooping on VLANs
- Defining Trusted Interfaces
- Binding Addresses to the DHCP Snooping Database
- Defining IP Source Guard

Defining DHCP Snooping Properties

The *DHCP Snooping Properties Page* contains parameters for enabling DHCP Snooping on the device.

To define the DHCP Snooping general properties:

- STEP 1** Click **Security Suite > DHCP Snooping > Properties**. The *DHCP Snooping Properties Page* opens:

DHCP Snooping Properties Page

The screenshot shows the Cisco Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch configuration interface. The sidebar on the left contains a tree view with the following items: System, Admin, Statistics, Bridging, Security Suite (expanded), Passwords Management, Authentication, Access Method, Traffic Control, 802.1X, Access Control, DoS Prevention, DHCP Snooping (expanded), Properties (highlighted), VLAN Settings, Trusted Interfaces, Binding Database, IP Source Guard, ARP Inspection, and Quality of Service. The main content area is titled 'Properties' and contains the following configuration fields:

| | |
|--------------------------|---|
| Enable DHCP Snooping | <input type="checkbox"/> |
| Option 82 Passthrough | <input type="checkbox"/> |
| Verify MAC Address | <input checked="" type="checkbox"/> |
| Backup Database | <input type="checkbox"/> |
| Database Update Interval | <input type="text" value="1200"/> (Sec) |

Below the fields is an 'Apply' button. The footer of the page reads '© 2009 Cisco Systems, Inc. All rights reserved'.

The *DHCP Snooping Properties Page* contains the following fields:

- **Enable DHCP Snooping** — Indicates if DHCP Snooping is enabled on the device. The possible field values are:
 - *Checked* — Enables DHCP Snooping on the device.

- *Unchecked* — Disables DHCP Snooping on the device. This is the default value.
- **Option 82 Passthrough** — Indicates if the device forwards or rejects packets that include Option 82 information, while DHCP Snooping is enabled.
 - *Checked* — Device forwards packets containing Option 82 information.
 - *Unchecked* — Device rejects packets containing Option 82 information.
- **Verify MAC Address** — Indicates if the MAC address is verified. The possible field values are:
 - *Checked* — Verifies (on an untrusted port) that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload).
 - *Unchecked* — Disables verifying that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header. This is the default value.
- **Backup Database** — Indicates if the DHCP Snooping Database learning and update is enabled. All changes to the binding storage file are implemented only if the device's system clock is synchronized with the SNTP Server. The possible field values are:
 - *Checked* — Enables backing up of the allotted IP address in the DHCP Snooping Database.
 - *Unchecked* — Disables backing up to the allotted IP address in the DHCP Snooping Database. This is the default value.
- **Database Update Interval** — Indicates how often the DHCP Snooping Database is backed up. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.

STEP 2 Modify the relevant fields.

STEP 3 Click **Apply**. The settings are defined, and the device is updated.

Defining DHCP Snooping on VLANs

The *DHCP Snooping VLAN Settings Page* allows network managers to enable DHCP snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure DHCP Snooping is enabled on the device.

To define DHCP Snooping on VLANs:

- STEP 1** Click **Security Suite > DHCP Snooping > VLAN Settings**. The *DHCP Snooping VLAN Settings Page* opens:

DHCP Snooping VLAN Settings Page

The screenshot shows the Cisco Small Business SGE2000P web interface. The top navigation bar includes 'Logout', 'About', and 'Help'. The left sidebar lists various configuration categories, with 'Security Suite' expanded to show 'DHCP Snooping' and 'VLAN Settings' highlighted. The main content area is titled 'VLAN Settings' and contains two input fields: 'VLAN ID' and 'Enabled VLANs'. Below the 'VLAN ID' field are 'Add' and 'Delete' buttons. The 'Enabled VLANs' field is currently empty. The footer of the interface states '© 2009 Cisco Systems, Inc. All rights reserved'.

The *DHCP Snooping VLAN Settings Page* contains the following fields:

- **VLAN ID** — Indicates the VLAN to be added to the Enabled VLAN list.
- **Enabled VLANs** — Contains a list of VLANs for which DHCP Snooping is enabled.

- STEP 2** Modify the relevant fields.

- STEP 3** Click **Apply**. The settings are defined, and the device is updated.

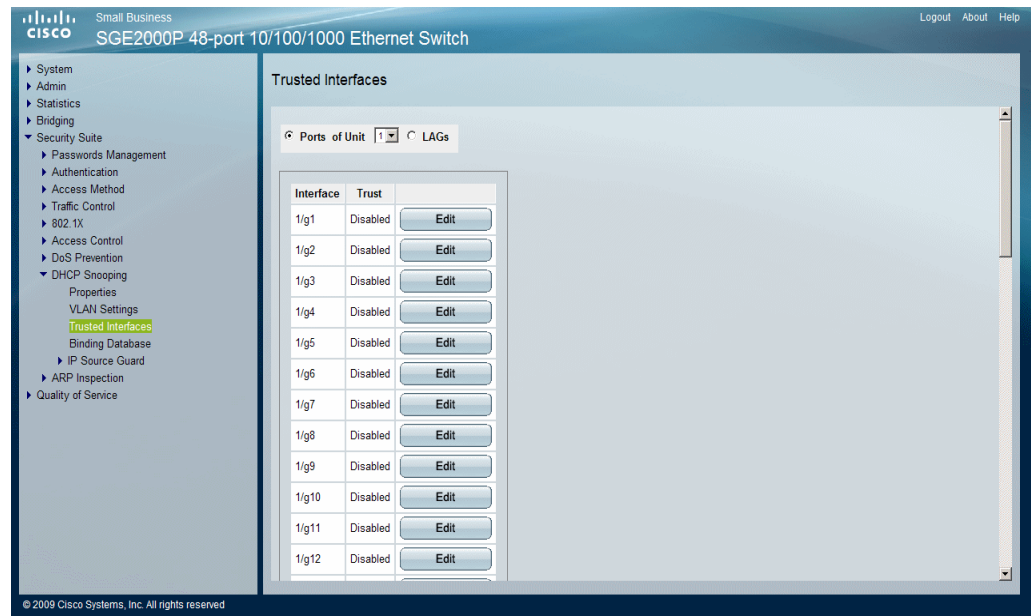
Defining Trusted Interfaces

The *Trusted Interfaces Page* allows network managers to define Trusted interfaces. The device transfers all DHCP requests to trusted interfaces.

To define trusted interfaces:

STEP 1 Click **Security Suite > DHCP Snooping > Trusted Interfaces**. The *Trusted Interfaces Page* opens:

Trusted Interfaces Page



The *Trusted Interfaces Page* contains the following fields:

- **Ports of Unit** — Displays the ports which can be defined as trusted.
- **LAGs** — Displays the LAGs which can be defined as trusted.

Trusted Interface Table

- **Interface** — Contains a list of existing interfaces.
- **Trust** — Indicates whether the interface is a Trusted interface.

STEP 2 Select either Ports or LAGs.

STEP 3 In the table, select an interface and click **Edit**. The *Edit Trusted Interface Page* opens.

Edit Trusted Interface Page

Interface ☒ Port 1/g1 ☐ LAG LAG 1

Trust Status Disable

Apply

In addition to the *Trusted Interfaces Page*, the *Edit Trusted Interface Page* contains the following field:

- **Interface** — Contains a list of existing interfaces.
- **Trust Status** — Indicates whether the interface is a Trusted Interface.
 - *Enable* — Interface is in trusted mode.
 - *Disable* — Interface is in untrusted mode.

STEP 4 Define the fields.

STEP 5 Click **Apply**. The Trusted Interfaces configuration is defined and the device is updated.

Binding Addresses to the DHCP Snooping Database

The *Binding Database Page* contains parameters for querying and adding IP addresses to the DHCP Snooping Database.

To bind addresses to the DHCP Snooping database:

- STEP 1** Click **Security Suite > DHCP Snooping > Binding Database**. The *Binding Database Page* opens:

Binding Database Page

The *Binding Database Page* contains the following fields:

- **Supported IP Format** — Indicates only Ipv4 is supported.

- STEP 2** Define any of the following fields as a query filter:

Query By

- **MAC Address** — Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
- **IP Address** — Indicates the IP addresses recorded in the DHCP Database. The Database can be queried by IP address.
- **VLAN** — Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
- **Interface** — Contains a list of interface by which the DHCP Database can be queried. The possible field values are:
 - *Unit No.* and *Port* — Queries the VLAN database by a specific stacking member and port number.

- *LAG* — Queries the VLAN database by LAG number.

STEP 3 Click **Query**. The results appear in the *Query Results* table.

Query Results

The Query Results table contains the following fields:

- **MAC Address** — Indicates the MAC address found during the query.
- **VLAN ID** — Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **IP Address** — Indicates the IP address found during the query.
- **Interface** — Indicates the specific interface connected to the address found during the query.
- **Type** — Displays the IP address binding type. The possible field values are:
 - *Static* — Indicates the IP address is static.
 - *Dynamic* — Indicates the IP address is defined as a dynamic address in the DHCP database.
 - *Learned* — Indicates the IP address is dynamically defined by the DHCP server. (This field appears as a read-only field in the table).
- **Lease Time** — Displays the lease time. The Lease Time defines the amount of time the DHCP Snooping entry is active. Addresses whose lease times are expired are deleted from the database. The possible values are 10 – 4294967295 seconds. In the *Add DHCP Snooping Page*, select **Infinite** if the DHCP Snooping entry never expires.

STEP 4 Define the fields.

STEP 5 Click **Apply**. The bound address is added to the database and the device is updated.

STEP 6 Click **Delete** to delete the data from the *Query Results* Table.

STEP 7 To remove dynamic addresses from the *Query Results* table, click **Clear Dynamic**.

Defining IP Source Guard

IP Source Guard is a security feature that restricts the client IP traffic to those source IP addresses configured in the DHCP Snooping Binding Database and in manually configured IP source bindings. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

- DHCP snooping must be enabled on the device's untrusted interfaces and on the relevant VLAN, in order to activate the IP source guard feature.
- IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.
- IP Source Guard uses *Ternary Content Addressable Memory* (TCAM) resources, requiring use of 1 TCAM rule per 1 IP Source Guard address entry. If the number of IP Source Guard entries exceeds the number of available TCAM rules, new IP source guard addresses remain inactive.
- IP Source Guard cannot be configured on routed ports.
- If IP Source Guard and MAC address filtering is enabled on a port, Port Security cannot be activated on the same port.
- If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is not active in that condition.
- If a port's status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

The IP Source Guard section contains the following topics:

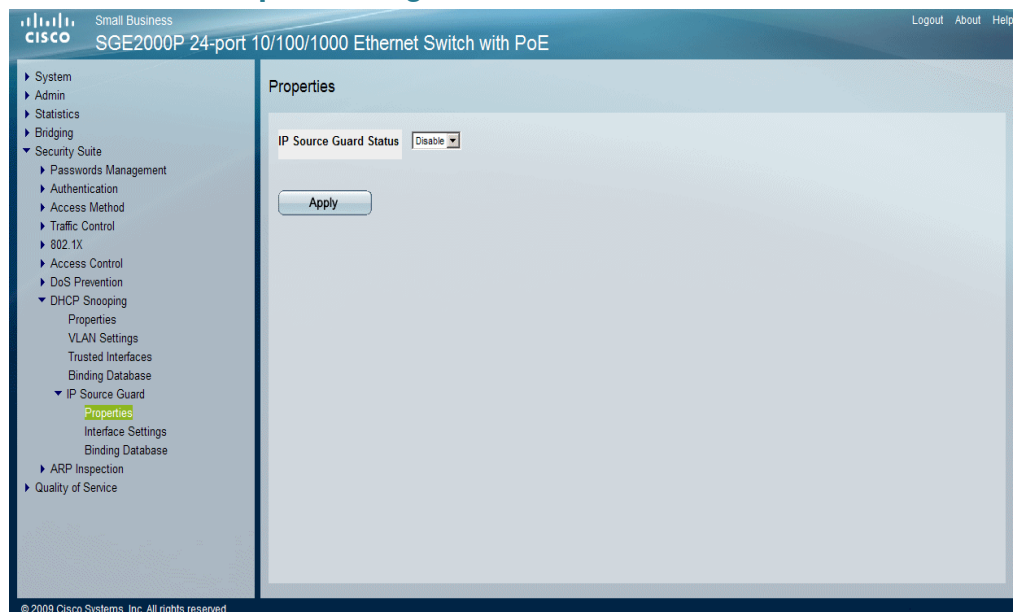
- Configuring IP Source Guard Properties
- Defining IP Source Guard Interface Settings
- Querying the IP Source Binding Database

Configuring IP Source Guard Properties

The *IP Source Guard Properties Page* allows network managers to enable the use of IP Source Guard on the device. IP Source Guard must be enabled for the device before it can be enabled on individual ports or LAGs. To enable IP Source Guard:

- STEP 1** Click **Security Suite > DHCP Snooping > IP Source Guard > Properties**. The *IP Source Guard Properties Page* opens:

IP Source Guard Properties Page



The *IP Source Guard Properties Page* contains the following fields:

- **IP Source Guard Status** — Enables the use of IP Source Guard status on the device.
 - *Enable* — Indicates that IP Source Guard is enabled for the device.
 - *Disable* — Indicates that IP Source Guard is disabled for the device.

- STEP 2** Enable or Disable use of IP Source Guard on the device.

- STEP 3** Click **Apply**. The IP Source Guard configuration is modified, and the device is updated.

Defining IP Source Guard Interface Settings

In the *IP Source Guard Interface Settings Page*, IP Source Guard can be enabled on DHCP Snooping untrusted interfaces, permitting the transmission of DHCP packets allowed by DHCP Snooping. If source IP address filtering is enabled, packet transmission is permitted as follows:

- **IPv4 traffic** — Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
- **Non IPv4 traffic** — All non-IPv4 traffic is permitted.

NOTE: IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.

If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is not active in that condition.

If a port's status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

STEP 1 Click **Security Suite > DHCP Snooping > IP Source Guard > Interface Settings**. The *IP Source Guard Interface Settings Page* opens:

IP Source Guard Interface Settings Page



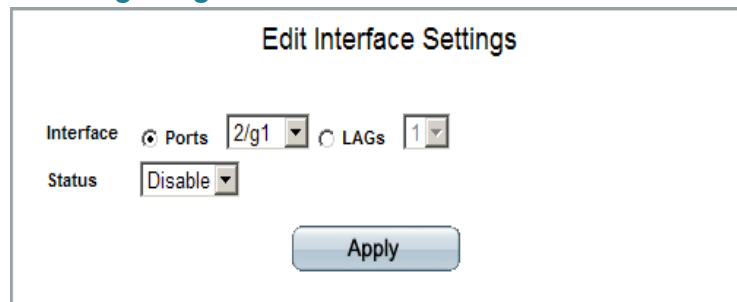
The *IP Source Guard Interface Settings Page* contains the following fields:

- **Ports of Unit** — Displays the stacking unit's port number on which the IP source guard is enabled.
- **LAGs** — Displays the stacking unit's LAG number on which the IP source guard is enabled.
- **Interface** — Indicates the port's or LAG's number.

- **Status** — Indicates if IP Source Guard is enabled or disabled.
 - *Enabled* — Indicates that IP Source Guard is enabled on the interface.
 - *Disabled* — Indicates that IP Source Guard is disabled on the interface. This is the default value.

STEP 2 Click **Edit**. The *Edit Interface Settings Page* opens:

Edit Interface Settings Page



STEP 3 Modify the fields.

STEP 4 Click **Apply**. The new IP Source Guard Interface configuration is added, and the device is updated.

Querying the IP Source Binding Database

The *IP Source Guard Binding Database Page* enables network managers to query and view information about inactive addresses recorded in the DHCP Database. To query the IP Source Guard Database:

- STEP 1** Click **Security Suite > DHCP Snooping > IP Source Guard > Binding Database**. The *IP Source Guard Binding Database Page* opens:

IP Source Guard Binding Database Page

The screenshot shows the 'Binding Database' configuration page. On the left is a navigation tree with 'Binding Database' highlighted. The main area contains the following sections:

- Supported IP Format:** Version 4
- TCAM Resources:** Includes a 'Retry Frequency' field set to 60 (Sec) and an 'Insert Inactive' section with radio buttons for 'Never' and 'Retry Now'.
- Query by:** A section with checkboxes for 'MAC Address', 'IP Address', 'VLAN', and 'Interface'. The 'Interface' option is selected, with sub-selects for 'Ports' (20) and 'LAGs' (1).
- Query:** A button to execute the query.
- Table:** A table with columns: Interface, Status, IP Address, VLAN, MAC Address, Type, Reason.
- Buttons:** 'Back', 'Next', and 'Apply' buttons are located at the bottom.

The *IP Source Guard Binding Database Page* contains the following fields:

TCAM Resources

- **Supported IP Format** — Indicates the IP Address format. The possible values are Version 6 or Version 4.
- **Insert Inactive** — Indicates the IP Source Guard Database uses the TCAM resources for managing the database. The device can try to activate inactive addresses in various time intervals:
 - *Retry Frequency* — Try to activate inactive addresses at a specified interval. The possible values are 10 - 600 seconds.
 - *Never* — Never try to activate inactive addresses.
 - *Retry Now* — Try to activate inactive addresses immediately

Query By

- STEP 2** In the Query By section, select and define the preferred filter for searching the IP Source Guard Database:

- **MAC Address** — Queries the database by MAC address.
- **IP Address** — Queries the database by IP address.
- **VLAN** — Queries the database by VLAN ID.
- **Interface** — Queries the database by interface number. The possible field values are:
 - *Unit No.* and *Port* — Queries the database by a specific stacking member and port number.
 - *LAG* — Queries the VLAN database by LAG number.

STEP 3 Click **Query**. The results appear in the Query Results table.

Query Results

The Query Results table contains the following fields:

- **Interface** — Displays the interface number.
- **Status** — Displays the current interface status. The possible field values are:
 - *Active* — Indicates the interface is currently active.
 - *Inactive* — Indicates the interface is currently inactive.
- **IP Address** — Indicates IP address of the interface.
- **VLAN** — Indicates if the address is associated with a VLAN.
- **MAC Address** — Displays the MAC address of the interface.
- **Type** — Displays the IP address type. The possible field values are:
 - *Dynamic* — Indicates the IP address is dynamically created.
 - *Static* — Indicates the IP address is a static IP address.
 - *Learned* — Indicates the IP address is dynamically defined by the DHCP server. (This field appears as a read-only field in the table).
- **Reason** — Displays the reason an IP source address is inactive. The possible field options are:
 - *No Problem* — Indicates the IP address is active.
 - *VLAN* — Indicates that DHCP Snooping is not enabled on the VLAN.
 - *Trusted Port* — Indicates the port is a trusted port.

- Resource Problem — Indicates that the TCAM is full.

STEP 4 Click **Apply**. The device is updated.

Defining Dynamic ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses. Classic ARP does the following:

- Permits two hosts on the same network to communicate and send packets.
- Permits two hosts on different networks to communicate via a gateway.
- Permits routers to send packets via a host to a different router on the same network.
- Permits routers to send packets to a destination host via a local host.

ARP Inspection intercepts, discards, and logs ARP packets that contain invalid IP-to-MAC address bindings. This eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. Packets are classified as:

- **Trusted** — Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspection List. Trusted packets are forwarded without ARP Inspection.
- **Untrusted** — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
 - *Source MAC* — Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
 - *Destination MAC* — Compares the packet's destination MAC address in the Ethernet header against the destination interface's MAC address. This check is performed for ARP responses.
 - *IP Addresses* — Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

If the packet's IP address was not found in the ARP Inspection List, and DHCP snooping is enabled for a VLAN, a search of the DHCP Snooping Database is performed. If the IP address is found, the packet is valid and is forwarded.



NOTE ARP inspection is performed only on untrusted interfaces.

The ARP Inspection section contains the following topics:

- Defining ARP Inspection Properties
- Defining ARP Inspection Trusted Interfaces
- Defining ARP Inspection List
- Assigning ARP Inspection VLAN Settings

Defining ARP Inspection Properties

The *ARP Inspection Properties Page* provides parameters for enabling and setting global Dynamic ARP Inspection parameters, as well as defining ARP Inspection Log parameters.

To define ARP Inspection properties:

- STEP 1** Click **Security Suite > ARP Inspection > Properties**. The *ARP Inspection Properties Page* opens:

ARP Inspection Properties Page

The screenshot shows the Cisco Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch web interface. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging, Security Suite (expanded), Passwords Management, Authentication, Access Method, Traffic Control, 802.1X, Access Control, DoS Prevention, DHCP Snooping, ARP Inspection (expanded), Properties (highlighted), Trusted Interfaces, ARP Inspection List, VLAN Settings, and Quality of Service. The main content area is titled 'Properties' and contains the following fields: 'Enable ARP Inspection' with an unchecked checkbox, 'ARP Inspection Validate' with an unchecked checkbox, and 'Log Buffer Interval' with a radio button selected for 'Retry Frequency' (set to 5 seconds) and an unchecked radio button for 'Never'. An 'Apply' button is located below these fields. The footer of the page reads '© 2009 Cisco Systems, Inc. All rights reserved'.

The *ARP Inspection Properties Page* contains the following fields:

- **Enable ARP Inspection** — Enables ARP Inspection on the device. The possible field values are:
 - *Checked* — Enables ARP Inspection on the device.
 - *Unchecked* — Disables ARP Inspection on the device. This is the default value.
- **ARP Inspection Validate** — Enables ARP Inspection Validation on the device. The possible field values are:
 - *Checked* — Enables ARP Inspection Validation on the device. Source MAC, Destination MAC, and IP addresses are checked in ARP requests and responses.

- *Unchecked* — Disable ARP Inspection Validation on the device. This is the default value.
- **Log Buffer Interval** — Defines the minimal interval between successive Syslog messages. The possible field values are:
 - *Retry Frequency* — Frequency at which the log is updated. The possible range is 0-86400 seconds. 0 seconds specifies immediate transmissions of Syslog messages. The default value is 5 seconds.
 - *Never* — Log is never updated.

STEP 2 Define the relevant fields,

STEP 3 Click **Apply**. The ARP Inspection Properties are defined, and the device is updated.

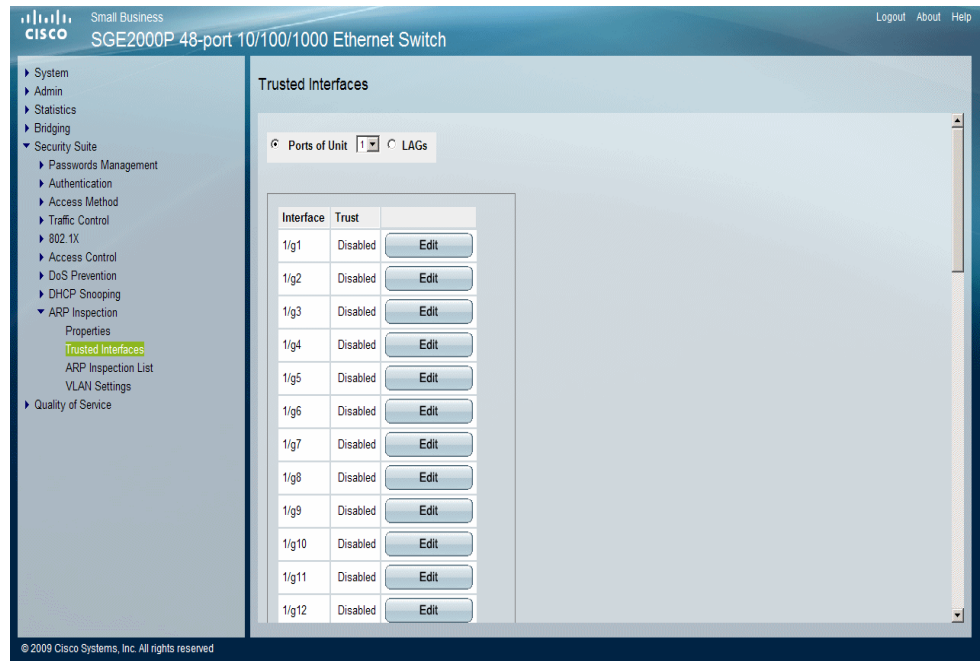
Defining ARP Inspection Trusted Interfaces

The *ARP Inspection Trusted Interfaces Page* allows network managers to define trusted and untrusted interfaces. These settings are independent of the trusted interface settings defined for DHCP snooping. ARP Inspection is enabled only on untrusted interfaces.

To define trusted interfaces:

STEP 1 Click **Security Suite > ARP Inspection > Trusted Interfaces**. The *ARP Inspection Trusted Interfaces Page* opens:

ARP Inspection Trusted Interfaces Page

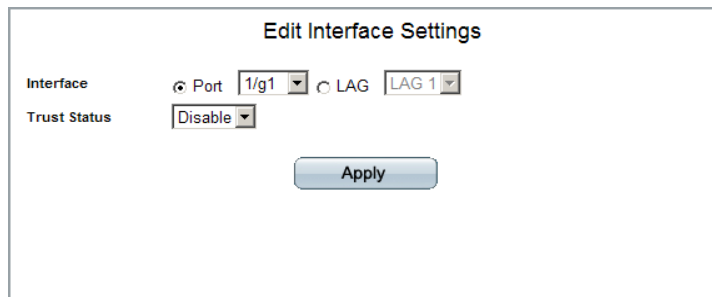


The *ARP Inspection Trusted Interfaces Page* contains the following fields:

- **Ports of Unit** — Specifies the port and stacking member for which the Trusted Interface settings are displayed.
- **LAGs** — Specifies the LAG for which the Trusted Interface settings are displayed.
- **Interface** — Displays the name or number of the interface on which ARP Inspection Trust mode can be enabled.
- **Trust** — Enables or disables ARP Inspection Trust mode on the interface. The possible field values are:
 - *Enabled* — Indicates the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests/replies sent to/from the interface.
 - *Disabled* — Indicates the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests/replies sent to/from the interface. This is the default value.

STEP 2 Click **Edit**. The *Edit Interface Settings Page* opens:

Edit Interface Settings Page



Edit Interface Settings

Interface ☒ Port 1/g1 ☐ LAG LAG 1

Trust Status Disable

Apply

STEP 3 Define the fields.

STEP 4 Click **Apply**. The Trusted Interface's configuration is modified, and the device is updated.

Defining ARP Inspection List

The *ARP Inspection List Page* provides information for creating static ARP Binding Lists. ARP Binding Lists contain the List Name, IP address and MAC address which are validated against ARP requests and replies.

To add an ARP Inspection List entry:

- STEP 1** Click **Security Suite > ARP Inspection > ARP Inspection List**. The *ARP Inspection List Page* opens:

ARP Inspection List Page

The screenshot shows the Cisco Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch configuration interface. The left sidebar contains a tree view with the following items: System, Admin, Statistics, Bridging, Security Suite (expanded), Passwords Management, Authentication, Access Method, Traffic Control, 802.1X, Access Control, DoS Prevention, DHCP Snooping, ARP Inspection (expanded), Properties, Trusted Interfaces, **ARP Inspection List** (highlighted), VLAN Settings, and Quality of Service. The main content area is titled 'ARP Inspection List'. It features a 'Static ARP Table' section with a table that has two columns: 'IP Address' and 'MAC Address'. Above the table are 'Delete' and 'Add' buttons. Below the table are 'Delete' and 'Add' buttons. The page also includes a 'Logout About Help' link in the top right corner and a copyright notice '© 2009 Cisco Systems, Inc. All rights reserved.' at the bottom.

The *ARP Inspection List Page* contains the following fields:

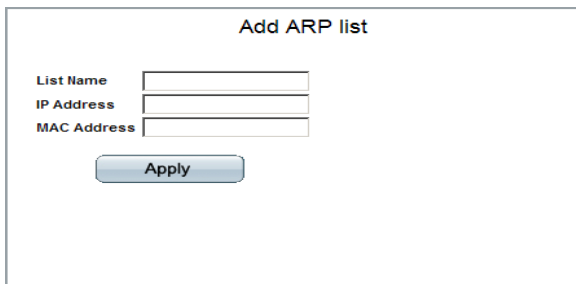
- **ARP Inspection List Name** — Name of the Inspection List.
 - *Select List* — Contains a list of existing user-defined ARP Inspection Lists.
 - *Add* — Defines a new ARP Inspection List. The list's name can contain up to 32 characters.
 - *Delete* — Removes the selected list. Only lists that were added by the **New** box above can be removed. To remove a list, the user selects the list name and selects this field's check box.

Static ARP Table

- **IP Address** — Specifies IP address included in ARP Binding Lists which is checked against ARP requests and replies.
- **MAC Address** — Specifies MAC address included in ARP Binding Lists which is checked against ARP requests and replies.

- STEP 2** Click **Add**. The *Add ARP List Page* opens:

Add ARP List Page



In addition to the fields in the *ARP Inspection List Page*, the *Add ARP List Page* contains the additional field:

- **List Name** — Specifies a name for the new ARP list.

STEP 3 Define the fields.

STEP 4 Click **Apply**. The new ARP Inspection List is added, and the device is updated.

Assigning ARP Inspection VLAN Settings

The *ARP Inspection VLAN Settings Page* contains fields for enabling ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection Lists to enabled VLANs. When a packet passes through an untrusted interface which is enabled for ARP Inspection, the device performs the following checks in order:

- Determines if the packet's IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- If the device does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the device checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- If the packet's IP address is not listed in the ARP Inspection List or the DHCP Snooping database, the device rejects the packet.

To define ARP Inspection on VLANs:

- STEP 1** Click **Security Suite > ARP Inspection > VLAN Settings**. The *ARP Inspection VLAN Settings Page* opens:

ARP Inspection VLAN Settings Page

The *ARP Inspection VLAN Settings Page* contains the following fields:

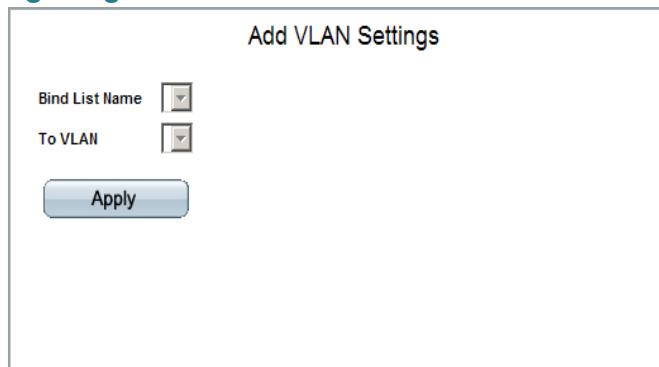
- **VLAN ID** — A user-defined VLAN ID to add to the Enabled VLANs list.
- **Enabled VLANs**— Contains a list of VLANs in which ARP Inspection is enabled.

Enabled VLAN Table

- **VLAN ID** — Indicates the VLAN which is bound to the ARP Inspection List.
- **List Name** — Displays names of static ARP Inspection Lists that were assigned to VLANs. These lists are defined in the *ARP Inspection List Page*.

- STEP 2** Select the VLAN name from the VLAN ID list and click **Add**. This VLAN name then appears in the list. The *Add VLAN Settings Page* opens:

Add VLAN Settings Page



The screenshot shows a web interface titled "Add VLAN Settings". It contains two dropdown menus. The first is labeled "Bind List Name" and the second is labeled "To VLAN". Below these two fields is a button labeled "Apply".

The *Add VLAN Settings Page* contains the following fields:

- **Bind List Name** — Select a static ARP Inspection List to assign to the VLAN. These lists are defined in the *ARP Inspection List Page*.
- **To VLAN** — Select the VLAN which includes the specified *ARP Inspection List*.

STEP 3 Define the fields.

STEP 4 Click **Apply**. The VLAN Settings are modified, and the device is updated.

Configuring Ports

This section contains information for configuring ports and contains the following topics:

- Configuring Ports Settings for Layer 2 Enabled Devices
- Configuring Ports Settings for Layer 3 Enabled Devices

Configuring Ports Settings for Layer 2 Enabled Devices

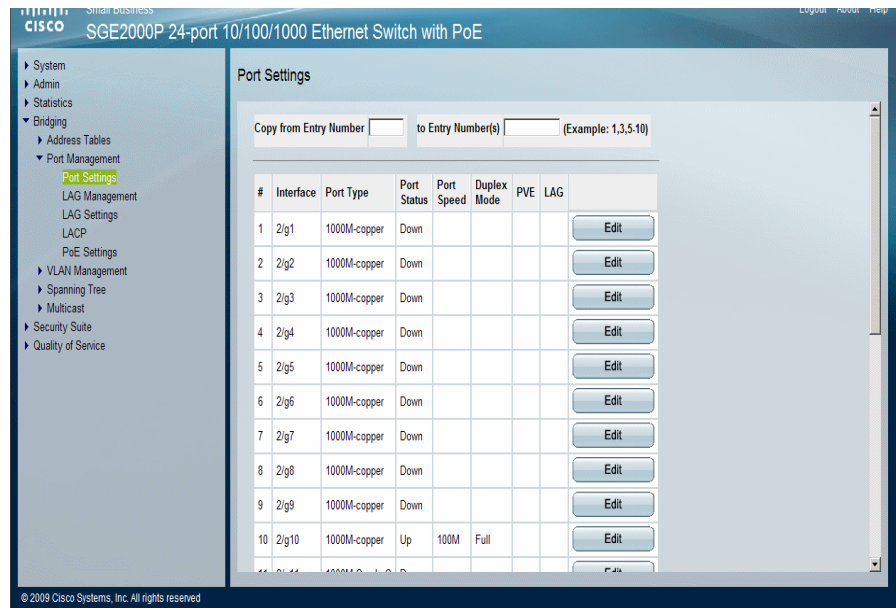
The *Port Settings Page* varies, depending on whether the device is in Layer 2 or Layer 3 mode (definable on the device through the CLI interface).

Layer 2 devices support Private VLAN Edge, which can be enabled for individual ports on the *Edit Port Page*.

The *Port Settings Page* contains fields for defining port parameters. To define port settings (Layer 2):

STEP 1 Click **Bridging > Port Management > Port Settings**. The *Port Settings Page* opens:

Port Settings Page



The Port Settings Page contains the following fields:

- **Copy From Entry Number** — Copies the port configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied port configuration to the specified table entry.
- **Unit Number** — Indicates the stacking member for which the ports are defined.
- **Interface** — Displays the port number.
- **Port Type** — Displays the port type. The possible field values are:
 - *1000M*— Copper (copper cable).
 - *1000M*— ComboC (combo port with copper cable 3).
 - *1000M*— ComboF (combo port with optic fiber cable).
 - *Fiber* — Indicates the port has a fiber optic port connection.
- **Port Status** — Displays the port connection status. The possible field values are:
 - *Up* — Port is connected.

- *Down* — Port is disconnected.
 - **Port Speed** — Displays the current port speed.
 - **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
 - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
 - **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it. PVE is supported in Layer 2 mode.
 - **LAG** — Defines if the port is part of a *Link Aggregation Group* (LAG).
- STEP 2** To copy the settings from one interface to another, enter the specific interface numbers in the **Copy From Entry Number and To Entry Number(s) fields**.
- STEP 3** Define the **Unit number**.
- STEP 4** Click **Apply**. *The Port Settings* are defined, and the device is updated.

Modifying Port Settings

- STEP 1** Click **Bridging > Port Management > Port Settings**. The *Port Settings Page* opens:
- STEP 2** Define the **Unit number**.
- STEP 3** Click a specific entry's **Edit** button. The *Edit Port Page* opens:

Edit Port Page

Edit Port

Port: 2/g1

Description:

Port Type: 1000M-copper

Admin Status: Up

Current Port Status: Down

Reactivate Suspended Port: ☐

Operational Status: Active

Admin Speed: 1000M

Current Port Speed:

Admin Duplex: Full

Current Duplex Mode:

Auto Negotiation: Enable

Current Auto Negotiation:

Admin Advertisement: ☒ Max Capability ☐ 10 Half ☐ 10 Full ☐ 100 Half ☐ 100 Full ☐ 1000 Full

Current Advertisement: Unknown

Neighbor Advertisement: Unknown

Back Pressure: Disable

Current Back Pressure:

Flow Control: Disable

Current Flow Control:

MDI/MDIX: AUTO

Current MDI/MDIX:

LAG:

PVE: None

Apply

The *Edit Port Page* contains the following fields:

- **Port** — Displays the port number.
- **Description** — Specifies the port's user-defined name.
- **Port Type** — Displays the port type. The possible field values are:
 - *1000M*— Copper (copper cable).
 - *1000M*— ComboC (combo port with copper cable 3).
 - *1000M*— ComboF (combo port with optic fiber cable).
 - *Fiber* — Indicates the port has a fiber optic port connection.
- **Admin Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
 - *Up* — Indicates the port is currently operating.

- *Down* — Indicates the port is currently not operating.
- **Current Port Status** — Displays the port connection status.
- **Suspended Port** — Reactivates a port if the port has been disabled through the locked port security option or through Access Control List configurations.
- **Operational Status** — Indicates whether the port is currently active or inactive.
- **Admin Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. You can designate *Admin Speed* only when the port auto-negotiation is disabled.
- **Current Port Speed** — Displays the current port speed.
- **Admin Duplex** — Defines the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
 - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the port current duplex mode.
- **Auto Negotiation** — Enables Auto Negotiation on the port. Auto Negotiation enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the Auto Negotiation status on the port.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the Port. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and Duplex mode settings can be accepted.
 - *10 Half* — Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.
 - *10 Full* — Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
 - *100 Half* — Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.
 - *100 Full* — Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.

- *1000 Full* — Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** — The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — Displays the neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the *Admin Advertisement* field.
- **Back Pressure** — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. The Back Pressure mode is configured for ports currently in the Half Duplex mode.
- **Current Back Pressure** — Displays the Back Pressure mode on the port.
- **Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the port. Select from Enable, Disable, Auto-Negotiation.
- **Current Flow Control** — Displays the current Flow Control setting. Select from Enable, Disable, Auto-Negotiation.
- **MDI/MDIX** — Displays the *Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX)* status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
 - *MDIX* — Use for hubs and switches.
 - *Auto* — Use to automatically detect the cable type.
 - *MDI* — Use for end stations.
- **Current MDI/MDIX** — Displays the current MDI/MDIX setting.
- **LAG** — Defines if the port is part of a *Link Aggregation* Group (LAG).
- **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it. PVE is supported in Layer 2 mode.

STEP 4 Define the relevant fields.

STEP 5 Click **Apply**. *The Port Settings* are modified, and the device is updated.

Configuring Ports Settings for Layer 3 Enabled Devices

To define port settings (Layer 3):

STEP 1 Click **Bridging > Port Management > Port Settings**. The *Port Settings Page* opens:

Port Settings Page

Small Business
SGE2000 24-port 10/100/1000 Ethernet Switch

Logout About Help

System
Admin
Statistics
Bridging
Address Tables
Port Management
Port Settings
LAG Management
LAG Settings
LACP
PoE Settings
VLAN Management
Spanning Tree
Multicast
Routing
Security Suite
Quality of Service

Port Settings

Copy from Entry Number to Entry Number(s) (Example: 1,3,5,10)

| # | Interface | Port Type | Port Status | Port Speed | Duplex Mode | LAG | |
|----|-----------|--------------|-------------|------------|-------------|-----|------|
| 1 | g1 | 1000M-copper | Down | | | | Edit |
| 2 | g2 | 1000M-copper | Down | | | | Edit |
| 3 | g3 | 1000M-copper | Down | | | | Edit |
| 4 | g4 | 1000M-copper | Down | | | | Edit |
| 5 | g5 | 1000M-copper | Down | | | | Edit |
| 6 | g6 | 1000M-copper | Down | | | | Edit |
| 7 | g7 | 1000M-copper | Down | | | | Edit |
| 8 | g8 | 1000M-copper | Down | | | | Edit |
| 9 | g9 | 1000M-copper | Down | | | | Edit |
| 10 | g10 | 1000M-copper | Down | | | | Edit |
| 11 | g11 | 1000M-ComboC | Down | | | | Edit |
| 12 | g12 | 1000M-ComboC | Down | | | | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *Port Settings Page* contains the following fields:

- **Copy From Entry Number** — Copies the port configuration from the specified table entry.

- **To Entry Number(s)** — Assigns the copied port configuration to the specified table entry.
- **Unit Number** — Indicates the stacking member for which the ports are defined.
- **Interface** — Displays the port number.
- **Port Type** — Displays the port type. The possible field values are:
 - *1000M*— Copper (copper cable).
 - *1000M*— ComboC (combo port with copper cable 3).
 - *1000M*— ComboF (combo port with optic fiber cable).
 - *Fiber* — Indicates the port has a fiber optic port connection.
- **Port Status** — Displays the port connection status. The possible field values are:
 - *Up* — Port is connected.
 - *Down* — Port is disconnected.
- **Port Speed** — Displays the current port speed.
- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
 - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **LAG** — Defines if the port is part of a *Link Aggregation Group* (LAG).

STEP 2 To copy the settings from one interface to another, enter the specific interface numbers in the **Copy From Entry Number and To Entry Number(s)** fields.

STEP 3 Define the **Unit number**.

STEP 4 Click **Apply**. The Port Settings are defined, and the device is updated.

Modifying Port Settings

- STEP 1** Click **Bridging > Port Management > Port Settings**. The *Port Settings Page* opens:
- STEP 2** Define the **Unit number**.
- STEP 3** Click a specific entry's **Edit** button. The *Edit Port Page* opens:

Edit Port Page

Edit Port

Port: g2

Description:

Port Type: 1000M-copper

Admin Status: Up

Current Port Status: Down

Reactivate Suspended Port: ☐

Operational Status: Active

Admin Speed: 1000M

Current Port Speed:

Admin Duplex: Full

Current Duplex Mode:

Auto Negotiation: Enable

Current Auto Negotiation:

Admin Advertisement: ☒ Max Capability ☐ 10 Half ☐ 10 Full ☐ 100 Half ☐ 100 Full ☐ 1000 Full

Current Advertisement: Unknown

Neighbor Advertisement: Unknown

Back Pressure: Disable

Current Back Pressure:

Flow Control: Disable

Current Flow Control:

MDI/MDIX: AUTO

Current MDI/MDIX:

LAG:

Apply

The *Edit Port Page* contains the following fields:

- **Port** — Displays the port number.
- **Description** — Specifies the port's user-defined name.
- **Port Type** — Displays the port type. The possible field values are:
 - *1000M*— Copper (copper cable).

- *1000M*— ComboC (combo port with copper cable 3).
 - *1000M*— ComboF (combo port with optic fiber cable).
 - *Fiber* — Indicates the port has a fiber optic port connection.
- **Admin Status** — Enables or disables traffic forwarding through the port.
- **Current Port Status** — Displays the port connection status.
- **Reactivate Suspended Port** — Reactivates a port if the port has been disabled through the locked port security option or through Access Control List configurations.
- **Operational Status** — Indicates whether the port is currently active or inactive.
- **Admin Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. You can designate admin speed only when the port auto-negotiation is disabled.
- **Current Port Speed** — Displays the current port speed.
- **Admin Duplex** — Defines the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
 - *Full*— Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
 - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the port current duplex mode.
- **Auto Negotiation** — Enables Auto Negotiation on the port. Auto Negotiation enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the Auto Negotiation status on the port.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the Port. The possible field values are:
 - *Max Capability*— Indicates that all port speeds and Duplex mode settings can be accepted.
 - *10 Half* — Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.

- *10 Full* — Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
 - *100 Half* — Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.
 - *100 Full* — Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.
 - *1000 Full* — Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** — Displays the current advertisement status. The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the *Admin Advertisement* field.
- **Neighbor Advertisement** — Displays the neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the *Admin Advertisement* field.
- **Back Pressure** — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. The Back Pressure mode is configured for ports currently in the Half Duplex mode.
- **Current Back Pressure** — Displays the Back Pressure mode on the port.
- **Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the port. Select from *Enable*, *Disable*, *Auto-Negotiation*.
- **Current Flow Control** — Displays the current Flow Control setting. Select from *Enable*, *Disable*, *Auto-Negotiation*.
- **MDI/MDIX** — Displays the *Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX)* status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
 - *MDIX* — Use for hubs and switches.
 - *Auto* — Use to automatically detect the cable type.

- *MDI* — Use for end stations.
- **Current MDI/MDIX** — Displays the current MDI/MDIX setting.
- **LAG** — Defines if the port is part of a *Link Aggregation* (LAG).

STEP 4 Define the relevant fields.

STEP 5 Click **Apply**. The Port Settings are modified, and the device is updated.

Configuring VLANs

A VLAN is a logical group that allow devices connected to the VLAN to communicate to each other at the Ethernet MAC layer regardless of the physical LAN segment of the bridged network to which they are attached. A physical bridged network can support a maximum of 4094 VLANs. Each VLAN is configured a unique VID (VLAN ID) of value 1 to 4094.

VLAN packets are distinguished with a 4 byte VLAN tag. Packets having the same VID (VLAN ID) in the VLAN tag belong to the same VLAN. A VLAN tag also contains priority information. The VLAN tag of a packet is either inserted by the source of the packet, or inserted by a VLAN bridge based on the PVID (Port VID) of the ingress port. On any given link, there can be at most one VLAN whose traffic is untagged on the link. When a VLAN-aware device receives an untagged packet, the VLAN of the packet is derived from the PVID (Port VID) configured at the ingress port.

VLANs function at layer 2. All traffic (unicast/broadcast/multicast) of a VLAN stays within the VLAN. Devices attached to different VLANs cannot have direct connectivity at the Ethernet MAC layer to each other. Devices from different VLANs can have communication with each other only through layer 3 routers.

An IP router, for example, is required to route IP traffic between VLANs if each VLAN represents an IP subnet. The IP router can be a traditional router where each of its interfaces connect to only one VLAN. Traffic to and from a traditional IP router must be VLAN untagged. The IP router can be a VLAN-aware router where each of its interfaces can connect to one or more VLANs. Traffic to and from a VLAN-aware IP router can be VLAN tagged or untagged.

Adjacent VLAN aware devices exchange VLAN information to each other using Generic VLAN Registration Protocol (GVRP). As a result, VLAN information are propagated through a bridged network.

The VLAN Management section contains the following topics:

- Defining VLAN Properties
- Defining VLAN Membership
- Assigning Ports to Multiple VLANs
- Defining VLAN Interface Settings

- Defining GVRP Settings
- Defining Multicast TV VLAN
- Defining CPE VLAN Mapping
- Defining Protocol Groups
- Defining a Protocol Port

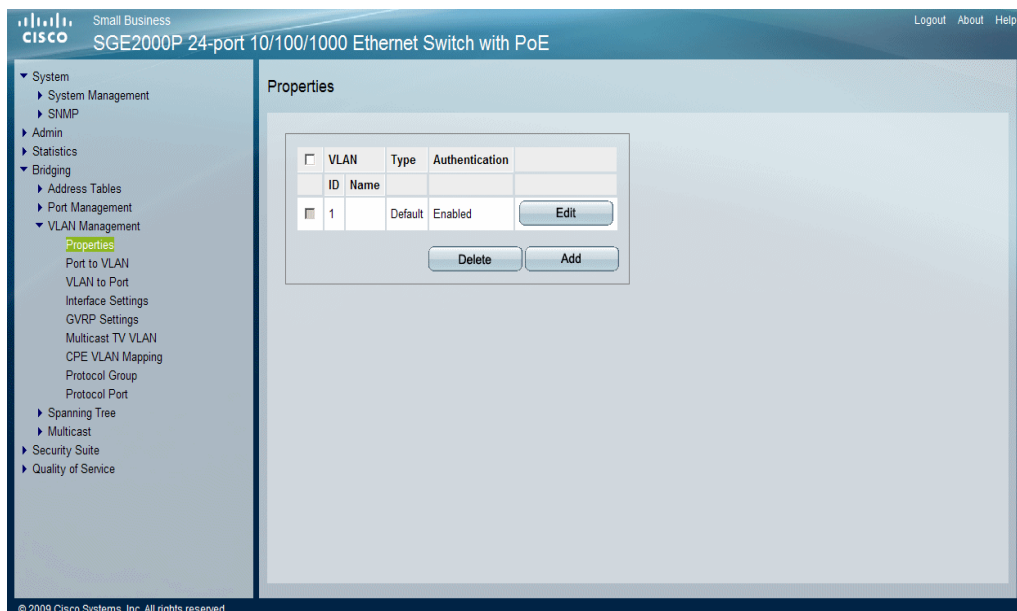
Defining VLAN Properties

The *VLAN Properties Page* provides information and global parameters for configuring and working with VLANs.

To define VLAN properties:

- STEP 1** Click **Bridging > VLAN Management > Properties**. The *VLAN Properties Page* opens:

VLAN Properties Page



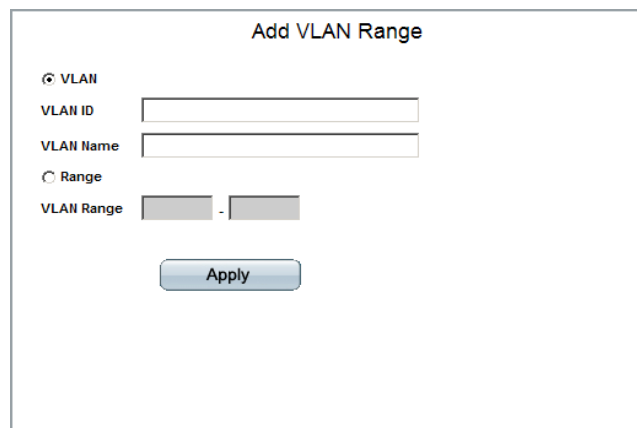
The *VLAN Properties Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Displays the user-defined VLAN name.

- **Type** — Displays the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GVRP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Authentication** — Indicates whether unauthorized users can access a VLAN. The possible field values are:
 - *Enabled* — Disables unauthorized users to use the VLAN.
 - *Disabled* — Enables unauthorized users from using the VLAN.

STEP 2 Click the **Add** button. The *Add VLAN Range Page* opens:

Add VLAN Range Page



The screenshot shows a web interface titled "Add VLAN Range". It contains two main sections: "VLAN" and "Range". The "VLAN" section has two text input fields: "VLAN ID" and "VLAN Name". The "Range" section has a radio button labeled "Range" and a "VLAN Range" field consisting of two text boxes separated by a hyphen. At the bottom of the form is an "Apply" button.

The *Add VLAN Range Page* allows network administrators to define and configure new VLANs, and contains the following fields:

- **VLAN** — Specifies that a specific VLAN is to be defined. The possible field values are:
 - **VLAN ID** — Defines the VLAN ID.
 - **VLAN Name** — Defines a VLAN name.
- **Range** — Specifies that a range of VLAN IDs is to be defined. The possible field values are:
 - **VLAN Range** — Defines the lower and upper bounds of the VLAN range.

STEP 3 Define the relevant fields.

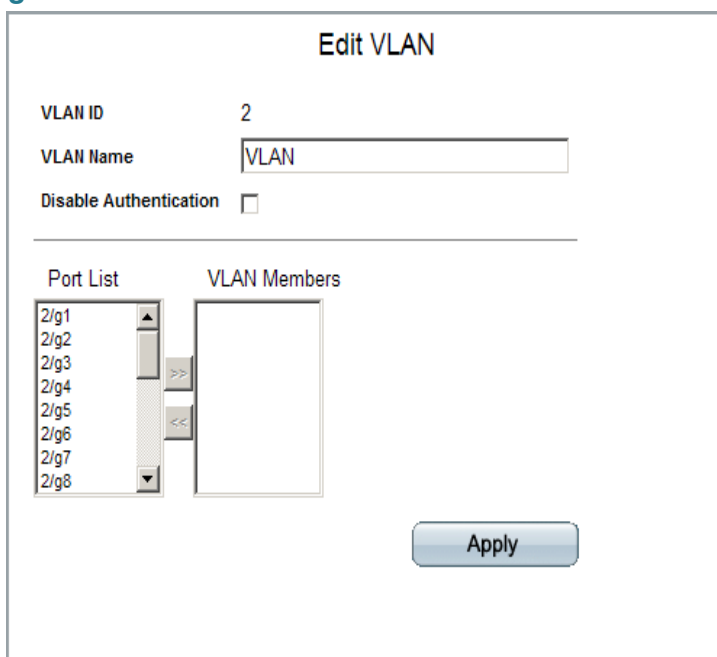
STEP 4 Click **Apply**. The VLAN settings are defined, and the device is updated.

Modifying VLANs

STEP 1 Click **Bridging > VLAN Management > Properties**. The *VLAN Properties Page* opens.

STEP 2 Click **Edit**. The *Edit VLAN Page* opens:

Edit VLAN Page



The screenshot shows the 'Edit VLAN' configuration page. At the top, the title 'Edit VLAN' is centered. Below it, there are three fields: 'VLAN ID' with the value '2', 'VLAN Name' with the value 'VLAN', and 'Disable Authentication' with an unchecked checkbox. A horizontal line separates these fields from the port selection section. This section has two columns: 'Port List' on the left and 'VLAN Members' on the right. The 'Port List' column contains a list of ports: 2/g1, 2/g2, 2/g3, 2/g4, 2/g5, 2/g6, 2/g7, and 2/g8. Between the two columns are two arrow buttons: a right-pointing arrow (>>) and a left-pointing arrow (<<). The 'VLAN Members' column is currently empty. At the bottom right of the form is an 'Apply' button.

The *Edit VLAN Page* contains information for enabling VLAN guest authentication, and includes the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Defines the VLAN name.
- **Disable Authentication** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
 - *Checked* — Enables unauthorized users to use the Guest VLAN.
 - *Unchecked* — Disables unauthorized users from using the Guest VLAN.

- **Unit Number** — Displays the stacking member for which the VLAN parameters are displayed.
- **Port List** — Available ports on the device. Select ports from this list to include in the VLAN.
- **VLAN Members** — Ports included in the VLAN.

STEP 3 Define the relevant fields.

STEP 4 In the Port List, select the ports to include in the VLAN and click the adjacent right arrow. The selected ports then appear in the VLAN Members list.

STEP 5 Click **Apply**. The VLAN Settings are defined, and the device is updated.

Defining VLAN Membership

The ***Port to VLAN Page*** contains a table that maps VLAN parameters to ports. Ports are assigned VLAN membership by toggling through the Port Control settings.

- STEP 1** Click **Bridging > VLAN Management > Port to VLAN**. The *Port to VLAN* Page opens:

Port to VLAN Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Log out About Help

System
Admin
Statistics
Bridging
 Address Tables
 Port Management
 VLAN Management
 Properties
 Port to VLAN
 VLAN to Port
 Interface Settings
 GVRP Settings
 Multicast TV VLAN
 CPE VLAN Mapping
 Protocol Group
 Protocol Port
 Spanning Tree
 Multicast
 Security Suite
 Quality of Service

Port to VLAN

VLAN ID: 1
VLAN Name:
VLAN Type: Default

Ports LAGs

| Interface | Interface Status | Type | |
|-----------|------------------|--------|------|
| 2/g1 | Excluded | System | Edit |
| 2/g2 | Untagged | System | Edit |
| 2/g3 | Untagged | System | Edit |
| 2/g4 | Untagged | System | Edit |
| 2/g5 | Untagged | System | Edit |
| 2/g6 | Untagged | System | Edit |
| 2/g7 | Untagged | System | Edit |
| 2/g8 | Untagged | System | Edit |

© 2009 Cisco Systems, Inc. All rights reserved.

The Port to VLAN Page contains the following fields:

- **VLAN ID** — Selects the VLAN ID.
- **VLAN Name** — Displays the VLAN name.
- **VLAN Type** — Indicates the VLAN type. The possible field values are:
 - *Dynamic* — Indicates the VLAN was dynamically created through GVRP.
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Ports of Unit** — Indicates that ports on the specified stacking member are described in the page.
- **LAGs** — Indicates that LAGs are described in the page.
- **Interface** — Displays the interface configuration being displayed.

- **Interface Status** — Indicates the interface's membership status in the VLAN. The possible field values are:
 - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
 - *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
 - *Exclude* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
 - *Forbidden* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

Modifying VLAN Membership

STEP 2 Click the **Edit** button. The *Edit Interface Status Page* opens:

Edit Interface Status Page

Edit Interface Status

VLAN ID 1

VLAN Name

Interface 2/g2

Interface Status Untagged

Type ☒ Dynamic ☐ Static

Apply

The *Edit Interface Status Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Displays the VLAN name.
- **Interface** — Defines the port or LAG attached to the VLAN.
- **Interface Status** — Defines the current interface's membership status in the VLAN. The possible field values are:
 - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.

- *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
- *Exclude* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
- *Forbidden* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. VLAN Membership is modified, and the device is updated.

Assigning Ports to Multiple VLANs

A port can be configured as a untagged or tagged port member of a VLAN. A port can be port members of multiple VLANs. By default, all ports are assigned to VLAN 1 as untagged port member.

All intermediate VLAN-aware devices carrying VLAN traffic along the path between any end nodes must be either configured with the VLAN port memberships manually by an operator or dynamically learnt from GVRP.

The untagged port membership configured between two VLAN aware devices that have no other VLAN aware device in between should be to the same VLAN. Otherwise, traffic will leak from one VLAN to another VLAN.

VLAN tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices. If none of the intermediate network devices to an end node support VLAN, then the port on the last device that reaches the end node must be untagged VLAN member.

The *VLAN To Port Page* contains fields for configuring VLANs to ports. The network administrator allows the user to assign a single port to multiple VLANs.

To add VLAN membership to a port:

STEP 1 Click **VLAN Management > VLAN to Port**. The *VLAN To Port Page* opens:

VLAN To Port Page

Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch

Unit No. 1

| Port | Mode | Join VLAN | VLANs | LAG |
|-------|--------|-----------|-------|-----|
| 1/g1 | Access | Join VLAN | 10 | |
| 1/g2 | Access | Join VLAN | 10 | |
| 1/g3 | Access | Join VLAN | 10 | |
| 1/g4 | Access | Join VLAN | 10 | |
| 1/g5 | Access | Join VLAN | 10 | |
| 1/g6 | Access | Join VLAN | 10 | |
| 1/g7 | Access | Join VLAN | 10 | |
| 1/g8 | Access | Join VLAN | 10 | |
| 1/g9 | Access | Join VLAN | 10 | |
| 1/g10 | Access | Join VLAN | 10 | |

© 2009 Cisco Systems, Inc. All rights reserved.

The *VLAN To Port Page* contains the following fields:

- **Unit No.** — Indicates that ports on the specified stacking member
- **Port** — Displays the port number.
- **Mode** — Indicates the port mode. The possible values are:
 - *General* — The port can be tagged and untagged with members of one or more VLANs. (full 802.1Q mode).
 - *Access* — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. Also, it is not possible to enable/disable ingress filtering on an access port.
 - *Trunk* — The port can be member of one or more VLANs. It is an untagged member of at most one VLAN, and is a tagged member of all other VLANs it is a member of.

- **Customer** — The port can be a member of one or more double tagged Multicast TV VLAN. Refer to "Define Customer VLAN using Q-in-Q" for details.
- **Join VLAN** — Defines the VLANs to which the interface is joined. Pressing the Join VLAN button displays the *Join VLAN to Port Screen*.

STEP 2 Select the VLAN to which to add the port, select the VLANs to be tagged or untagged and click **Add**. To remove the VLAN allocation to the port, select the VLAN already assigned to the port and click **Remove**.

- **VLANs** — Specifies the VLAN in which the port is a member.
- **LAG** — if the port is a member of a LAG, the LAG number is displayed. A member of a LAG cannot be configured to a VLAN, but that same LAG can be configured to a VLAN.

STEP 3 In the *VLAN To Port* table, click **Join VLAN** in the relevant port entry. The *Join VLAN To Port Screen* opens.

Join VLAN To Port Screen

STEP 4 Define the selected VLAN as *Tagged* or *Untagged*.

STEP 5 From the left list, select the relevant VLAN and click **Add**. The selected VLAN then appears in the right list. Up to 20 VLANs at a single time may be joined to the port.

STEP 6 Click **Save & Close** to save the modifications and close the *Join VLAN To Port Screen* (clicking **Save** keeps the *Join VLAN To Port Screen* open).

Defining GVRP Settings

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

The Global System LAG information displays the same field information as the ports, but represents the LAG GVRP information.

To define GVRP.

STEP 1 Click **Bridging > VLAN Management > GVRP Settings**. The *GVRP Settings Page* opens:

GVRP Settings Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

System
Admin
Statistics
Bridging
Address Tables
Port Management
VLAN Management
Properties
Port to VLAN
VLAN to Port
Interface Settings
GVRP Settings
Multicast TV VLAN
CPE VLAN Mapping
Protocol Group
Protocol Port
Spanning Tree
Multicast
Security Suite
Quality of Service

GVRP Settings

GVRP Global Status: Disable

Copy from Entry Number: to Entry Number(s): (Example: 1,3,5-10)

☒ Ports ☐ LAGs

| # | Interface | GVRP State | Dynamic VLAN Creation | GVRP Registration | |
|---|-----------|------------|-----------------------|-------------------|----------------------|
| 1 | 2/g1 | Disabled | Enabled | Enabled | Edit |
| 2 | 2/g2 | Disabled | Enabled | Enabled | Edit |
| 3 | 2/g3 | Disabled | Enabled | Enabled | Edit |
| 4 | 2/g4 | Disabled | Enabled | Enabled | Edit |
| 5 | 2/g5 | Disabled | Enabled | Enabled | Edit |
| 6 | 2/g6 | Disabled | Enabled | Enabled | Edit |
| 7 | 2/g7 | Disabled | Enabled | Enabled | Edit |
| 8 | 2/g8 | Disabled | Enabled | Enabled | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *GVRP Settings Page* contains the following fields:

- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
 - *Enable* — Enables GVRP on the device.
 - *Disable* — Disables GVRP on the device.

- **Copy From Entry Number** — Copies GVRP parameters from the specified table entry.
- **To Entry Number(s)** — Assigns the copied GVRP parameters to the specified table entry.
- **Ports of Unit** — Indicates the port number and stacking member for which GVRP parameters are displayed.
- **LAGs** — Indicates the LAG number for which GVRP parameters are displayed.
- **Interface** — Interface described by the GVRP settings entry.
- **GVRP State** — Indicates if GVRP is enabled on the interface. The possible field values are:
 - *Enabled* — Enables GVRP on the selected interface.
 - *Disabled* — Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
 - *Enabled* — Enables Dynamic VLAN creation on the interface.
 - *Disabled* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
 - *Enabled* — Enables GVRP registration on the device.
 - *Disabled* — Disables GVRP registration on the device.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The GVRP Settings are defined, and the device is updated.

Modifying GVRP Settings

STEP 1 Click **Bridging > VLAN Management > GVRP Settings**. The *GVRP Settings Page* opens:

STEP 2 Click the **Edit** button. The *Edit GVRP Page* opens:

Edit GVRP Page

Edit GVRP

Interface ☒ Port 1/g1 ☐ LAG 1

GVRP State

Dynamic VLAN Creation

GVRP Registration

Apply

The *Edit GVRP Page* contains the following fields:

- **Interface** — Port or LAG described by the GVRP settings entry.
- **GVRP State** — Indicates if GVRP is enabled on the interface. The possible field values are:
 - *Enable* — Enables GVRP on the selected interface.
 - *Disable* — Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
 - *Enable* — Enables Dynamic VLAN creation on the interface.
 - *Disable* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
 - *Enable* — Enables GVRP registration on the device.
 - *Disable* — Disables GVRP registration on the device.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. GVRP settings are modified, and the device is updated.

Defining VLAN Interface Settings

The *VLAN Interface Setting Page* provides parameters for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the *VLAN Port Settings* page. All untagged packets arriving to the device are tagged by the ports PVID.

The varies, depending on whether the device is in Layer 2 or Layer 3 mode (definable on the device through the CLI interface).

Layer 2 devices support Multicast TV VLAN, which can be enabled for individual ports on the *Edit VLAN Ports Page*.

STEP 1 Click **Bridging > VLAN Management > Interface Settings**. The *VLAN Interface Setting Page* opens:

VLAN Interface Setting Page

Small Business
SGE2000P 48-port 10/100/1000 Ethernet Switch

Logout About Help

System
Admin
Statistics
Bridging
Address Tables
Port Management
VLAN Management
Properties
Port to VLAN
VLAN to Port
Interface Settings
GVRP Settings
Multicast TV VLAN
CPE VLAN Mapping
Protocol Group
Protocol Port
Spanning Tree
Multicast
Security Suite
Quality of Service

Interface Settings

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

Ports Of Unit LAGs

| Interface | Interface VLAN Mode | PVID | Frame Type | Ingress Filtering | Multicast TV VLAN | |
|-----------|---------------------|------|------------|-------------------|-------------------|------|
| 1/g1 | Access | 1 | Admit All | Enable | | Edit |
| 1/g2 | Access | 1 | Admit All | Enable | | Edit |
| 1/g3 | Access | 1 | Admit All | Enable | | Edit |
| 1/g4 | Access | 1 | Admit All | Enable | | Edit |
| 1/g5 | Access | 1 | Admit All | Enable | | Edit |
| 1/g6 | Access | 1 | Admit All | Enable | | Edit |
| 1/g7 | Access | 1 | Admit All | Enable | | Edit |
| 1/g8 | Access | 1 | Admit All | Enable | | Edit |
| 1/g9 | Access | 1 | Admit All | Enable | | Edit |
| 1/g10 | Access | 1 | Admit All | Enable | | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *VLAN Interface Setting Page* contains the following fields:

- **Copy From Entry Number** — Copies VLAN configuration from the specified table entry.

- **To Entry Number(s)** — Assigns the copied VLAN configuration to the specified table entry.
- **Ports of Unit** — Indicates that ports on the specified stacking member are described in the page.
- **LAGs** — Indicates that LAGs are described in the page.
- **Interface** — The port number included in the VLAN.
- **Interface VLAN Mode** — Indicates the port mode. Possible values are:
 - *General* — The port can be tagged and untagged with members of one or more VLANs. (full 802.1Q mode).
 - *Access* — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
 - *Trunk* — The port can be member of one or more VLANs. It is an untagged member of at most one VLAN, and is a tagged member of all other VLANs it is a member of.
 - *Customer* — The port can be a member of one or more double tagged Multicast TV VLAN's. Refer to *Define Customer VLAN using Q-in-Q* for details.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values for General, Access, and Trunk Interface VLAN Mode are:
 - *SGE devices* — 1-4094 and 4095
 - *SFE devices* — 1-4093 and 4095

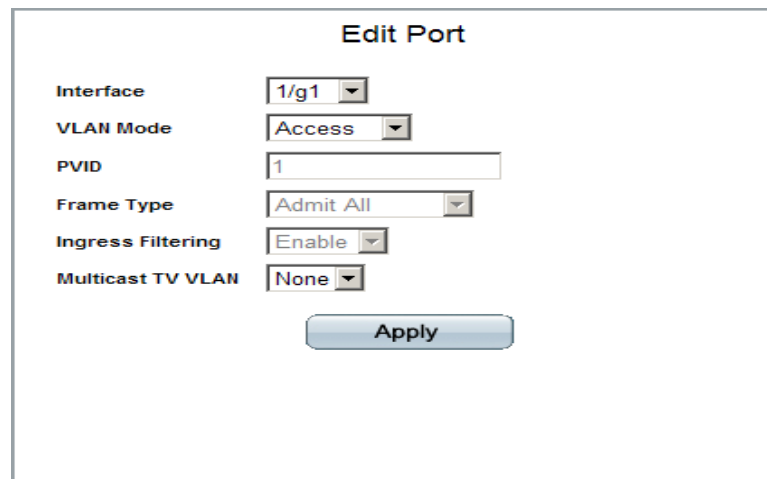
Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Packet type accepted on the port. Possible values are:
 - *Admit Tag Only* — Indicates that only tagged packets are accepted on the port.
 - *Admit All* — Indicates that both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** — Ingress filtering discards packets which do not include an ingress port. The possible values are:
 - *Enable* — Ingress filtering is activated on the port.

- *Disable* — Ingress filtering is not activated on the port.
- **Multicast TV VLAN** — Indicates if a Multicast TV VLAN is enabled on the device. Multicast TV VLANs enable VLANs to receive Multicast TV transmissions from ports that are not Access ports. The possible values are:
 - *Enable* — Multicast TV VLAN is activated on the port.
 - *Disable* — Multicast TV VLAN is not activated on the port.

Modifying VLAN Interface Settings

STEP 2 Click the **Edit** button. The *Edit VLAN Ports Page* opens:

Edit VLAN Ports Page



The screenshot shows the 'Edit Port' configuration page. It contains the following fields and values:

| Field | Value |
|-------------------|-----------|
| Interface | 1/g1 |
| VLAN Mode | Access |
| PVID | 1 |
| Frame Type | Admit All |
| Ingress Filtering | Enable |
| Multicast TV VLAN | None |

At the bottom right of the form is an 'Apply' button.

The *Edit VLAN Ports Page* contains the following fields:

- **Interface** — The port or LAG associated with this VLAN interface configuration.
- **VLAN Mode** — Indicates the port mode. Possible values are:
 - *General* — The port can be tagged and untagged with members of one or more VLANs. (full 802.1Q mode).
 - *Access* — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
 - *Trunk* — The port can be member of one or more VLANs. It is an untagged member of at most one VLAN, and is a tagged member of all other VLANs it is a member of.

- *Customer* — The port can be member of one or more double tagged Multicast TV VLAN. Refer to "Define Customer VLAN using Q-in-Q" for details.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values for General, Access, and Trunk Interface VLAN Mode are:
 - *SGE devices* — 1-4094 and 4095
 - *SFE devices* — 1-4093 and 4095

Packets classified to the Discard VLAN are dropped.

- **Frame Type** — Packet type accepted on the port. Possible values are:
 - *Admit All* — Indicates that both tagged and untagged packets are accepted on the port.
 - *Admit Tag Only* — Indicates that only tagged packets are accepted on the port.
- **Ingress Filtering** — Ingress filtering discards packets which do not include an ingress port. The possible values are:
 - *Enable* — Ingress filtering is activated on the port.
 - *Disable* — Ingress filtering is not activated on the port.
- **Multicast TV VLAN** — Indicates if a Multicast TV VLAN is enabled on the device. Multicast TV VLANs enable VLANs to receive Multicast TV transmissions from ports that are not Access ports. The possible values are:
 - *Enable* — Multicast TV VLAN is activated on the port.
 - *Disable* — Multicast TV VLAN is not activated on the port.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The VLAN Interface settings are modified, and the device is updated.

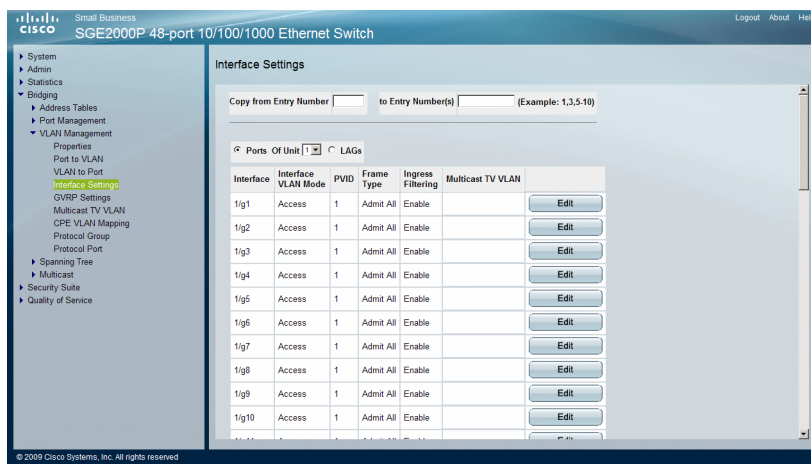
Defining Customer VLANs Using QinQ

QinQ, also known as Double Tagging, allows network managers to add an additional tag to previously tagged packets received from ports that are in Customer Interface VLAN mode, therefore creating more VLAN space and expanding service to VLAN users. The additional tag is inserted into packets received from the customer ports before the packets are transmitted into Multicast TV VLAN through the service provider network.

The *VLAN Interface Setting Page* provides parameters defining VLANs supporting QinQ.

To define VLANs supporting QinQ:

- STEP 1** Click **Bridging > VLAN Management > Interface Setting**. The *VLAN Interface Setting Page* opens.



- STEP 2** For the relevant interface, click Edit. The *Edit VLAN Ports Page* opens.

- STEP 3** Set the **VLAN Mode** field to **Customer**.

- STEP 4** Define the **PVID** field.

- STEP 5** Click **Apply**. The VLAN interface settings are saved, and the device is updated.

Defining Multicast TV VLAN

An access port can be configured as a member of a Multicast TV VLAN. See *Defining VLAN Interface Setting*. This is required to supply multicast transmissions to Level 2-isolated subscribers, without replicating the multicast transmissions for each subscriber VLAN. IGMP snooping is supported for those transmissions.

Any VLAN can be a Multicast-TV VLAN. A port assigned to a Multicast-TV VLAN:

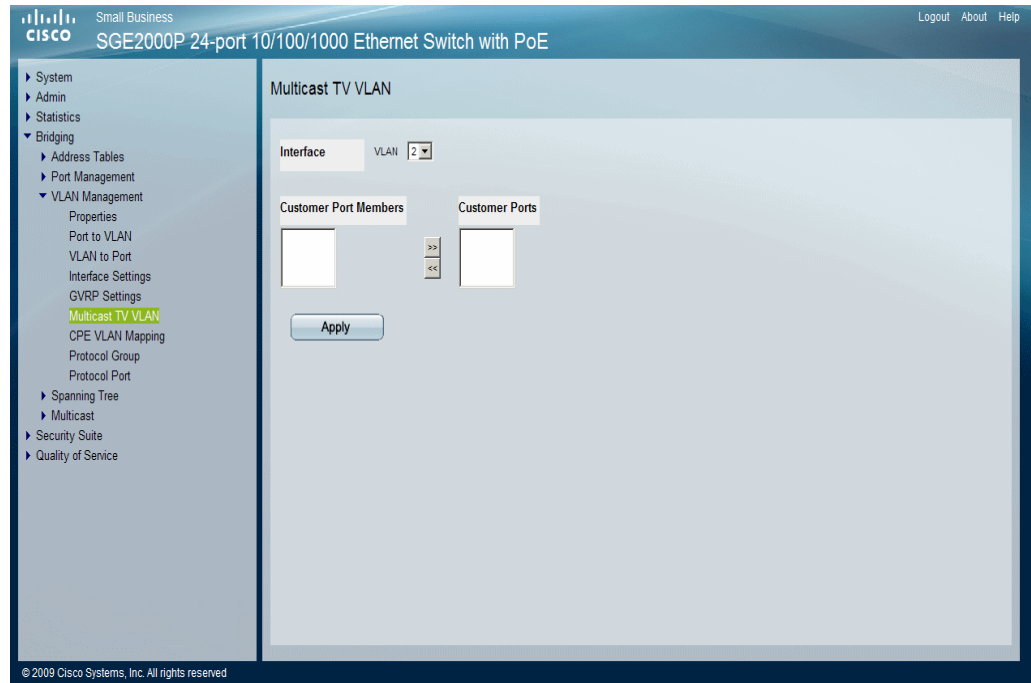
- Joins the Multicast-TV VLAN.
- Packets passing through egress ports in the Multicast TV VLAN are untagged.
- The port's Frame Type parameter is set to **Admit All**, allowing untagged packets (see "Defining VLAN Interface Settings").

The Multicast TV VLAN configuration is defined per port. Customer ports are configured to be member of Multicast TV VLAN using the *Multicast TV VLAN* Page.

To define the Multicast TV VLAN configuration:

- STEP 1** Click **Bridging > VLAN Management > Multicast TV VLAN**. The *Multicast TV VLAN Page* opens:

Multicast TV VLAN Page



The *Multicast TV VLAN Page* contains the following fields:

- **Interface** — Defines the VLAN to which the ports are assigned.
- **Customer Port Members** — Defines the ports already assigned to the Multicast TV VLAN.
- **Customer Ports** — Lists the ports available for assigning to the Multicast TV VLAN.

- STEP 2** Define the ports which are members of the Multicast TV VLAN. Select ports from the Customer Ports list and click the left arrow button to move the ports to the Customer Ports Member list.

- STEP 3** Click **Apply**. Multicast TV VLAN settings are modified, and the device is updated.

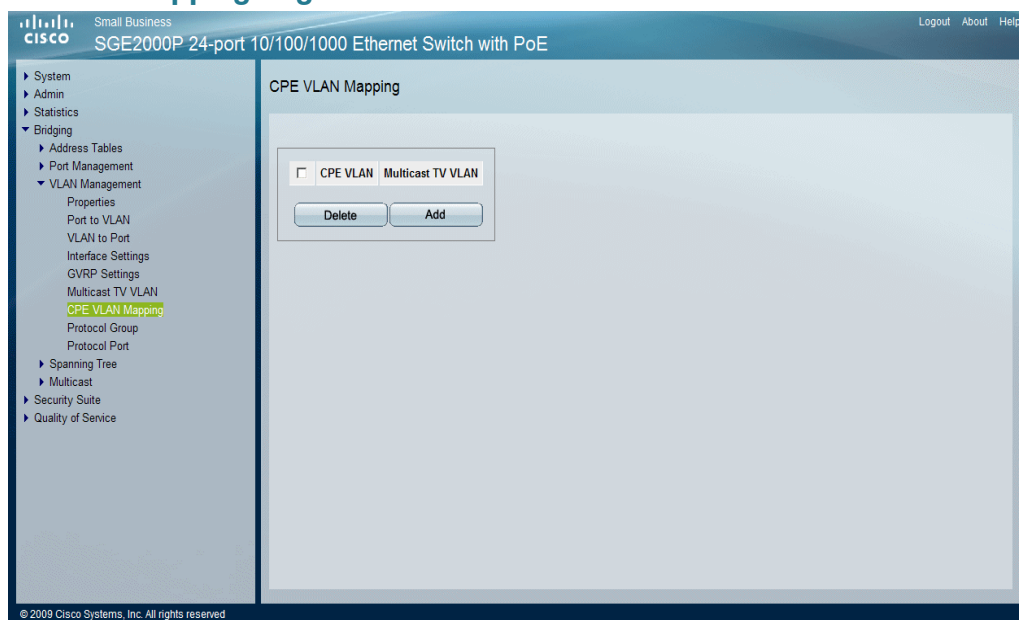
Defining CPE VLAN Mapping

Network managers can map CPE VLANs to Multicast TV VLANs in the *CPE VLAN Mapping Page*. Once the CPE VLAN is mapped to the Multicast VLAN, the VLAN can participate in IGMP snooping.

To map CPE VLANs:

- STEP 1** Click **Bridging > VLAN Management > CPE VLAN Mapping**. The *CPE VLAN Mapping Page* opens:

CPE VLAN Mapping Page

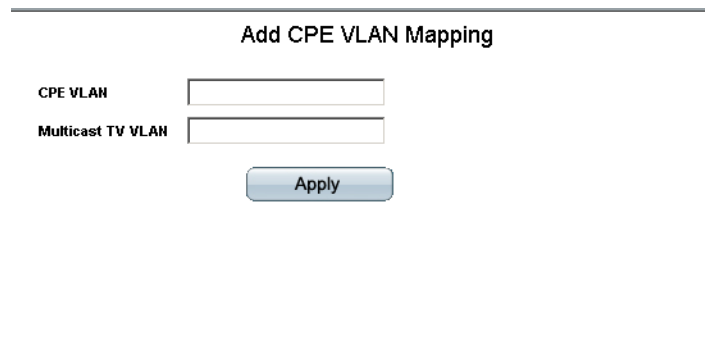


The *CPE VLAN Mapping Page* contains the following fields:

- **CPE VLAN** — Indicates the CPE VLAN which is mapped to the Multicast TV VLAN.
- **Multicast TV VLAN** — Indicates the Multicast TV VLAN which is mapped to the CPE VLAN.

- STEP 2** Click **Add**. The *Add CPE VLAN Mapping Page* opens:

Add CPE VLAN Mapping Page



The screenshot shows a web interface for adding CPE VLAN mapping. It features a title bar 'Add CPE VLAN Mapping'. Below the title, there are two text input fields. The first field is labeled 'CPE VLAN' and the second is labeled 'Multicast TV VLAN'. Below these fields is a blue 'Apply' button.

The *Add CPE VLAN Mapping Page* contains the following fields:

- **CPE VLAN** — Defines the CPE VLAN which is mapped to the Multicast TV VLAN.
- **Multicast TV VLAN** — Defines the Multicast TV VLAN which is mapped to the CPE VLAN.

STEP 3 Define the mapping.

STEP 4 Click **Apply**. CPE VLAN Mapping is modified, and the device is updated.

Defining Protocol Groups

The *Protocol Group Page* contains information defining protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface. Protocol Groups are supported in Layer 3 mode.

- STEP 1** Click **Bridging > VLAN Management > Protocol Group (Layer 2)**. The *Protocol Group Page* (Layer 2) opens:

Protocol Group Page

The screenshot shows the Cisco Small Business SGE2000P 48-port 10/100/1000 Ethernet Switch configuration page. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging (expanded), Address Tables, Port Management, VLAN Management (expanded), Properties, Port to VLAN, VLAN to Port, Interface Settings, CVRP Settings, Multicast TV VLAN, CPE VLAN Mapping, Protocol Group (highlighted), Protocol Port, Spanning Tree, Multicast, Security Suite, and Quality of Service. The main content area is titled 'Protocol Group' and contains a table with the following data:

| <input type="checkbox"/> | Frame Type | Protocol Value | Group ID (Hex) | |
|--------------------------|------------|----------------|----------------|-------------------------------------|
| <input type="checkbox"/> | Ethernet | 0800 | 1 | <input type="button" value="Edit"/> |

Below the table are buttons for and .

The *Protocol Group Page* contains the following fields:

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Displays the User-defined protocol name.
- **Group ID (Hex)** — Defines the Protocol group ID to which the interface is added. Range is 1-2147483647.

- STEP 2** Click the **Add** Button. The *Add Protocol Group Page* opens:

Add Protocol Group Page

The screenshot shows the 'Add Protocol Group' configuration page. It contains the following fields and controls:

- Frame Type:** A text label followed by the value 'Ethernet'.
- Protocol Value:** A section with two radio buttons. The first is 'Protocol Value' (selected) followed by a dropdown menu showing 'IP'. The second is 'Ethernet-Based Protocol Value' followed by an empty text input field and the text '(Hex Format)'.
- Group ID:** A text input field containing the number '1'.
- Apply:** A blue button with the text 'Apply'.

The *Add Protocol Group Page* provides information for configuring new VLAN protocol groups. The *Add Protocol Group Page* contains the following fields.

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Defines the User-defined protocol value. The options are as follows:
 - *Protocol Value* — The possible values are IP, IPX, IPv6, or ARP.
 - *Ethernet-Based Protocol Value* — Specify the value in hexadecimal format.
- **Group ID** — Defines the Protocol group ID to which the interface is added.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The Protocol Group is added, and the device is updated.

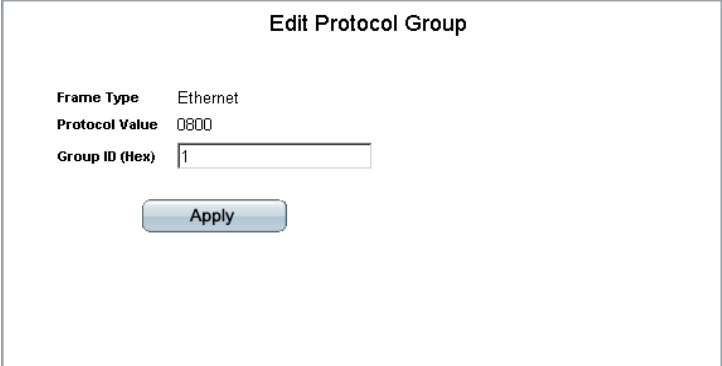
Modifying Protocol Groups

The *Edit Protocol Group Page* provides information for configuring existing VLAN protocol groups

STEP 1 Click **Bridging > VLAN Management > Protocol Group**. The *Protocol Group Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Protocol Group Page* opens:

Edit Protocol Group Page



The screenshot shows a web interface titled "Edit Protocol Group". It contains three configuration fields: "Frame Type" set to "Ethernet", "Protocol Value" set to "0800", and "Group ID (Hex)" with a text input field containing the value "1". Below these fields is a blue "Apply" button.

The *Edit Protocol Group Page* contains the following fields.

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Displays the User-defined protocol value.
- **Group ID (Hex)** — Defines the Protocol group ID to which the interface is added. The possible value range is 1-2147483647 in hexadecimal format.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The Protocol group is modified, and the device is updated.

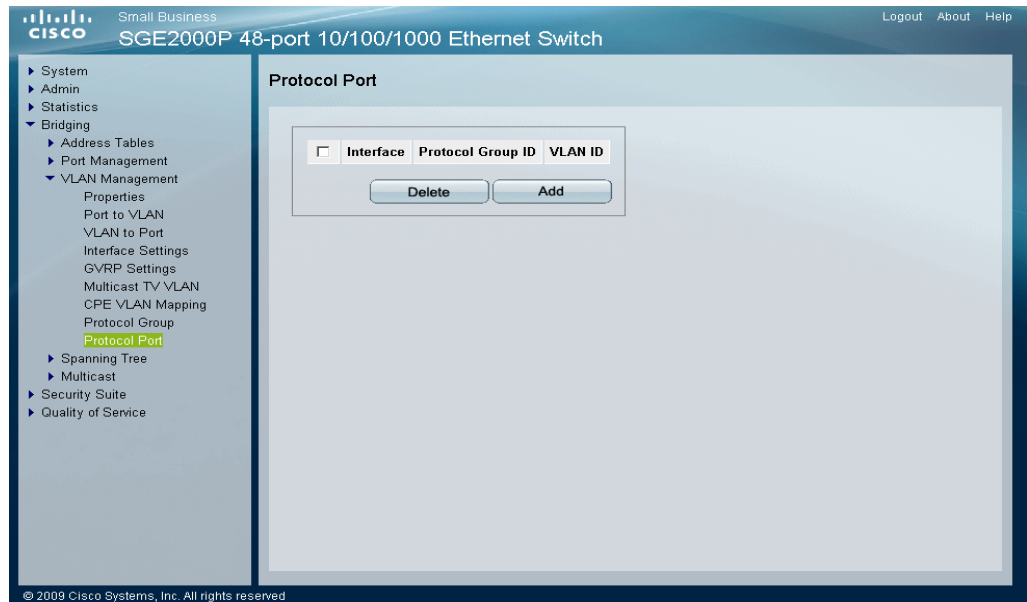
Defining a Protocol Port

The *Protocol Port Page* adds interfaces to Protocol groups. Protocol ports are supported in Layer 3 mode.

To define the protocol port:

- STEP 1** Click **Bridging > VLAN Management > Protocol Port**. The *Protocol Port Page* opens:

Protocol Port Page



The *Protocol Port Page* contains the following fields.

- **Interface** — Port or LAG number added to a protocol group.
- **Protocol Group ID** — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID. Protocol ports can either be attached to a VLAN ID or a VLAN name.

- STEP 2** Click the **Add** Button. The *Add Protocol Port to VLAN Page* opens:

The *Add Protocol Port to VLAN Page* provides parameters for adding protocol port configurations.

Add Protocol Port to VLAN Page

The screenshot shows a web-based configuration interface titled "Add Protocol Port to VLAN". It contains the following fields:

- Interface:** Two radio buttons, "Port" (selected) and "LAG". Next to "Port" is a dropdown menu showing "1/g1". Next to "LAG" is a dropdown menu showing "1".
- Group ID:** A dropdown menu showing "1".
- VLAN ID:** A radio button (selected) and a dropdown menu showing "1".
- VLAN Name:** A radio button and a dropdown menu.

An "Apply" button is located at the bottom right of the form.

The *Add Protocol Port to VLAN Page* contains the following fields.

- **Interface** — Port or LAG number added to a protocol group.
- **Group ID** — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID.
- **VLAN Name** — Attaches the interface to a user-defined VLAN Name.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The protocol ports are mapped to VLANs, and the device is updated.

Configuring IP Information

This section provides information for defining device IP addresses, and includes the following topics:

- IP Addressing
- Layer 3 IP Addressing
- Domain Name System

IP Addressing

The IP Addressing section contains the topics:

- Managing IPv6
- Defining IPv4 Interface (Layer 2)
- Defining IPv4 Interface (Layer 3)
- Enabling ARP Proxy (Layer 3)
- Defining UDP Relay (Layer 3)
- Defining DHCP Relay (Layer 2)
- Defining DHCP Relay Interfaces
- Defining DHCP Relay (Layer 3)
- ARP
- Defining IP Routing

Managing IPv6

The Internet Protocol version 6 (IPv6) is a network layer protocol for packet-switched internetworks. IPv6 was designed to eventually replace IPv4, the predominantly deployed Internet protocol.

The main improvement IPv6 presents is address size, increasing from 32-bit to 128-bit addresses. The larger address size introduces greater flexibility in assigning IP addresses.

IPv6 addresses are normally written as eight groups of four hexadecimal digits, for example FE80:0000:9C00:876A:130B. The abbreviated form is also acceptable, where a group of zeroes can be left out: FE80:9C0:876A:130B.

For IPv4-only nodes to communicate with IPv6 nodes, an intermediary transition mechanism is required. The transition mechanism enables IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach the IPv6 Internet over the IPv4 infrastructure.

The tunneling mechanism implemented is ISATAP. This protocol treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address.

The switch detects IPv6 frames by the IPv6 ether-type. The switch then can assign the frame to a specific VLAN as defined by the user.

The IPv6 Configuration section contains the following topics:

- Defining IPv6 Interface
- Defining Default Gateway
- Configuring ISATAP Tunnels
- Viewing IPv6 Neighbors Information
- Viewing IPv6 Routes Table

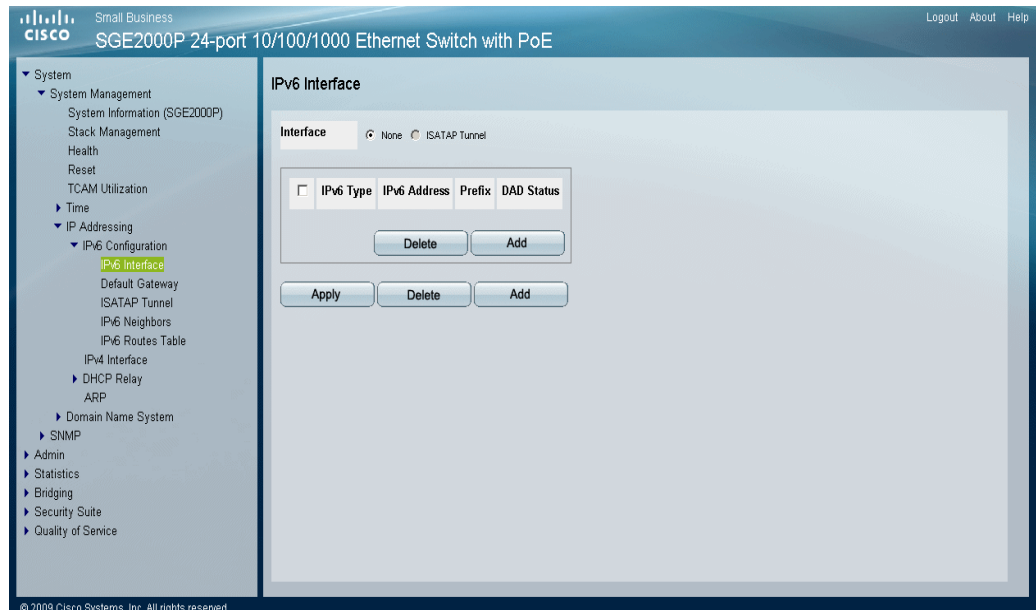
Defining IPv6 Interface

The *IPv6 Interface Page* provides parameters for defining IPv6 interfaces.

To define IPv6 interfaces:

- STEP 1** Click **System > System Management > IP Addressing > IPv6 Configuration > IPv6 Interface** . The *IPv6 Interface Page* opens:

IPv6 Interface Page



The *IPv6 Interface Page* contains the following fields:

- **Interface** — Indicates the Link Local Interface. The possible field values are:
 - *VLAN* — Indicates VLAN is the Link Local interface.
 - *ISATAP Tunnel* — Indicates a ISATAP tunnel is a Link Local interface.
- **IPv6 Type** — Displays the IPv6 Type. The possible field values are:
 - **Link-Local** — Indicates the IPv6 address is link-local.
 - **Global Unicast** — Indicates the IPv6 address is global Unicast.
- **IPv6 Address** — Indicates the IPv6 address assigned to the interface. Up to five IP addresses can be set per interface, with the limitation that up to 128 addresses can be set per system. **The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.**
- **Prefix** — Indicates the length of the IPv6 prefix. The length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The possible field values are 5-128.
- **DAD Status** — Displays the current DAD status. The possible field values are:

- *Duplicate* — Indicates the IPv6 address is being used by another host on the network.
- *Preferred* — Indicates the DAD Status is set to active.
- *Tentative* — Indicates the system is in process of IPv6 address duplication verification.

STEP 2 Click the **Add** button. The *Add IPv6 Address Interface Page* opens:

The *Add IPv6 Address Interface Page* provides information for adding an IPv6 address to an interface.

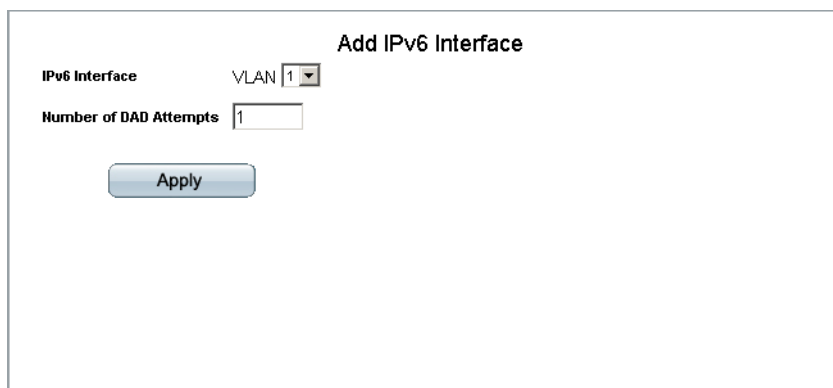
Add IPv6 Address Interface Page

The *Add IPv6 Address Interface Page* contains the following fields:

- **Interface** — Indicates the interface to which the address is added. The possible field value is:
 - *VLAN* — Indicates the VLAN for which the address is added.
- **IPv6 Type** — Displays the IPv6 Type. The possible field values are:
 - **Link-Local** — Indicates the IPv6 address is link-local.
 - **Global Unicast** — Indicates the IPv6 address is global Unicast.
- **IPv6 Address** — Indicates the IPv6 address assigned to the interface. Up to five IP addresses can be set per interface, with the limitation that up to 128 addresses can be set per system. **The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.**
- **Prefix Length** — Specifies the length of the IPv6 prefix. The range is 5 -128 (64 in the case EUI-64 parameter is used). The *Prefix* field is applicable only when the IPv6 Static IP Address is defined as an Global IPv6 Address.

STEP 3 Click the **Add** button. The *Add IPv6 Interface Page* opens:

Add IPv6 Interface Page



STEP 4 Select an IPv6 Interface and define the number of DAD Attempts.

STEP 5 Click **Apply**. The IPv6 Interface is added, and the device is updated.

Defining Default Gateway

The *Default Gateway Page* provides information for configuring default gateways for IPv6 enabled interfaces. The default gateway address is an interface that serves as an access point to another network.

Unlike IPv4, the IPv6 Default Gateway can have multiple IPv6 addresses which may include up to one user-defined static address and multiple dynamic addresses learned via router solicitation message. The user-configured Default Gateway has a higher precedence over automatically advertised addresses.

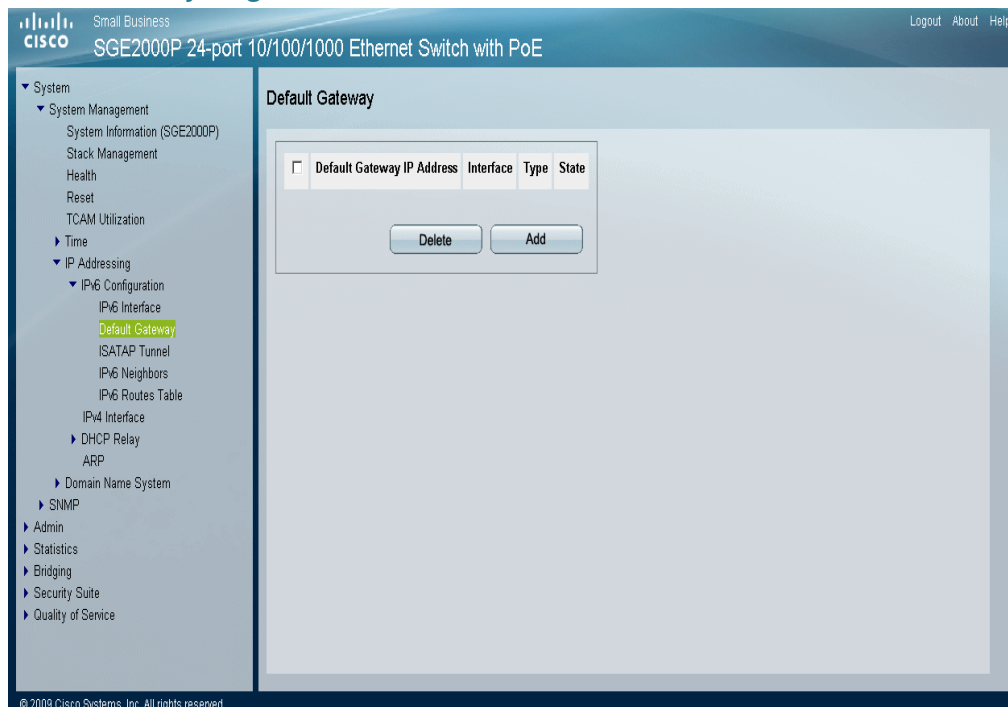
The IPv6 Default Gateway IP address is configured as a Link Local IPv6 type in order to maintain uniqueness opposite neighboring networks.

- When removing an IP interface, all of its Default Gateway IP Addresses are removed.
- Dynamic IP Addresses cannot be removed.
- An Alert message appears once a user attempts to insert more than one user defined address.
- An Alert message appears when attempting to insert a none Link Local type address (i.e 'fe80:').

To define the Default Gateway:

- STEP 1** Click **System > System Management > IP Addressing > IPv6 Configuration > Default Gateway**. The *Default Gateway Page* opens:

Default Gateway Page



The *Default Gateway Page* contains the following fields:

- **Default Gateway IP Address** — Defines the Link Local IP Address of the Default Gateway.
- **Interface** — Specifies the outgoing interface through which the Default Gateway can be reached, which is the VLAN ID on which the IPv6 interface is defined.
- **Type** — Specifies the means by which the default gateway was configured. Possible field values are:
 - *Static* — Indicates the default gateway is user-defined.
 - *Dynamic* — Indicates the default gateway is dynamically configured.
- **State** — Specifies the Default Gateway status. Possible field values are:
 - *Incomplete* — Indicates address resolution is in process. Default Gateway has not yet responded.

- *Reachable* — Indicates that a positive confirmation was received within the last Reachable Time.
- *Stale* — Indicates that the previously known neighbor is no longer reachable. No action is taken to verify its reachability, until traffic needs to be sent.
- *Delay* — Indicates previously known neighbor is no longer reachable. Device is in Delay state for a predefined Delay Time that if no reachability confirmation is received, the state changes to Probe.
- *Probe* — Indicates the neighbor is no longer reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

STEP 2 Click the **Add** button. The *Add Static Default Gateway Page* opens:

The *Add Static Default Gateway Page* provides information for adding a static Default Gateway.

Add Static Default Gateway Page



The screenshot shows a web-based configuration page titled "Add Static Default Gateway". It contains four labeled fields: "Supported IP Format" with the value "Version 6", "IPv6 Address Type" with the value "Link Local", "Link Local Interface" (which is empty), and "Default Gateway IP Address" (which is empty). Below these fields is a blue "Apply" button.

The *Add Static Default Gateway Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version is IPv6.
- **IPv6 Address Type** — Indicates the IPv6 address is link local IP address, that uniquely identifies hosts on a single network link. A Link-local address has a prefix of 'FE80'. The link-local addresses are not routable and can be used for communication on the same network only.
- **Link Local Interface** — Indicates the Link Local Interface. The possible field values are:
 - *VLAN* — Indicates the VLAN is the Link local interface.

- **Default Gateway IP Address** — Defines the Static Default Gateway IP Address.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The *Default Gateway* is defined, and the device is updated.

Configuring ISATAP Tunnels

The *Intra-Site Automatic Tunnel Access Protocol* (ISATAP) enables encapsulating IPv6 packets within IPv4 packets for transmission over IPv4 networks. ISATAP is considered a single IPv6 interface. When enabling ISATAP, the automatically generated Link Local IPv6 address is assigned to the interface and the interface becomes active.

When defining ISATAP tunnels, note the following:

- IPv6 Link Local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, and the interface state becomes *Active*.
- If a ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host name cache.
- When ISATAP router IPv4 address is not resolved via DNS process, the status of the ISATAP IP interface remains *Active*. The system does not have a default gateway for ISATAP traffic until the DNS procedure is resolved.

- STEP 1** To define an IPv6 ISATAP tunnel: **Click > System > System Management > IP Addressing > IPv6 Configuration > ISATAP Tunnel.** The *ISATAP Tunnel Page* opens:

ISATAP Tunnel Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE web interface. The left sidebar shows the navigation tree with 'ISATAP Tunnel' highlighted under 'IPv6 Configuration'. The main content area is titled 'ISATAP Tunnel' and contains the following configuration fields:

- ISATAP Status:** A dropdown menu set to 'Disable'.
- Tunnel Router's Domain Name:** A text field containing 'ISATAP' with a 'Use Default' checkbox.
- Query Interval (10-3600):** A text field containing '10' with a 'Use Default' checkbox.
- ISATAP Solicitation Interval (10-3600):** A text field containing '10' with a 'Use Default' checkbox.
- ISATAP Robustness (1-20):** A text field containing '3' with a 'Use Default' checkbox.

An 'Apply' button is located at the bottom of the configuration area.

The *ISATAP Tunnel Page* contains the following fields:

- **ISATAP Status** — Enables IPv6 over IPv4 ISATAP tunneling. Once ISATAP is enabled, an ISATAP interface is created. The possible field values are:
 - *Enable* — Enables ISATAP tunnel on the device.
 - *Disable* — Disables ISATAP tunnel on the device. This is the default value.
- **Tunnel Router's Domain Name** — Specifies a global string that represents a specific automatic tunnel router domain name. The default value is **ISATAP**.
 - *Use Default* — Selecting the check box that returns settings to default.
- **Query Interval (10-3600)** — Specifies the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name. The range is 10 - 3600 seconds. The default is 10 seconds.
 - *Use Default* — Selecting the check box that returns settings to default.

- **ISATAP Solicitation Interval (10-3600)** — Specifies the interval between ISATAP router solicitations messages when there is no active ISATAP router. The range is 10 - 3600 seconds. The default is 10.
 - *Use Default* — Selecting the check box that returns settings to default.
- **ISATAP Robustness (10-20)** — Specifies the number of DNS Query/ Router Solicitation refresh messages that the device sends. The range is 1 - 20 seconds. The default is 3.
 - *Use Default* — Selecting the check box that returns settings to default.

STEP 2 Define the relevant fields.

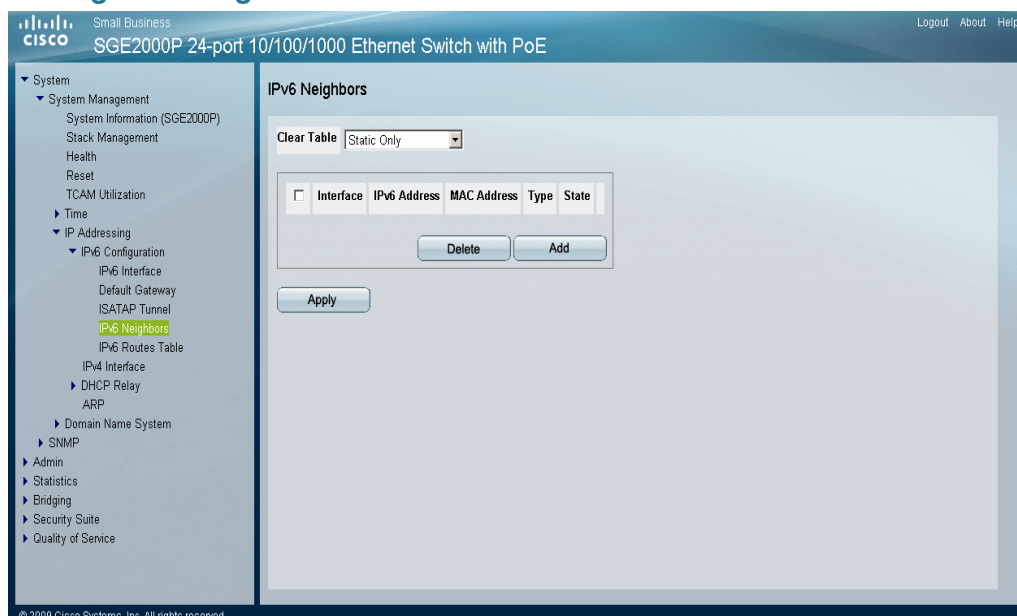
STEP 3 Click **Apply**. The ISATAP tunnel is defined, and the device is updated.

Viewing IPv6 Neighbors Information

The *IPv6 Neighbors Page* enables detecting same subnet node Link Layer addresses, and for maintaining reachability information about the active neighbors paths. To define IPv6 Neighbors:

- STEP 1** Click **System > System Management > IP Addressing > IPv6 Configuration > IPv6 Neighbors**. The *IPv6 Neighbors Page* opens:

IPv6 Neighbors Page



The *IPv6 Neighbors Page* contains the following fields:

- **Clear Table** — Deletes the entries in the IPv6 Neighbor Table. The possible field values are:
 - *Static Only* — Deletes the static IPv6 address entries from the IPv6 Neighbor Table.
 - *Dynamic Only* — Deletes the dynamic IPv6 address entries from the IPv6 Neighbor Table.
 - *All Static and Dynamic* — Deletes the static and dynamic address entries IPv6 address entries from the IPv6 Neighbor Table.
- **Interface** — Indicates the neighboring IPv6 interface type. The possible field values are:
 - *VLAN* — Displays the neighboring IPv6 VLAN number.
- **IPv6 Address** — Indicates the **IPv6 network assigned to the interface**.
- **MAC Address** — Indicates the MAC address mapped to the specified IPv6 address.

- **Type** — Displays the type of the neighbor discovery cache information entry. The possible field values are:
 - *Static* — Shows static neighbor discovery cache entries.
 - *Dynamic* — Shows dynamic neighbor discovery cache entries.
- **State** — Specifies the IPv6 Neighbor status. The possible values are:
 - *Incomplete* — Indicates Address Resolution is in process. The neighbor has not yet responded.
 - *Reachable* — Indicates the neighbor is known to be reachable.
 - *Stale* — Indicates the previously known neighbor is no longer reachable. No action is taken to verify its reachability, until traffic need to be sent.
 - *Delay* — Indicates the previously known neighbor is no longer reachable. The Interface is in Delay state for a predefined Delay Time that if no reachability confirmation is received, the state will change to Probe.
 - *Probe* — Indicates the neighbor is no longer known to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

STEP 2 Click the **Edit** button. The *Edit IPv6 Neighbors Page* opens:

Edit IPv6 Neighbors Page

Interface VLAN 5

IPv6 Address fe80::213:19ff:fe2f:326a

MAC Address 00:13:19:2f:32:6a

Type ☐ Static ☒ Dynamic

Apply

The *Edit IPv6 Neighbors Page* contains the following fields:

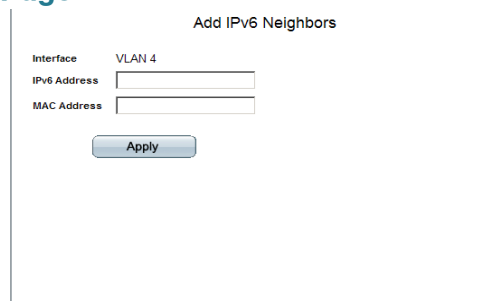
- **Interface** — Displays the neighboring IPv6 VLAN number.

- **IPv6 Address** — Defines the currently configured **IPv6 network assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.**
- **MAC Address** — Indicates the MAC address mapped to the specified IPv6 address.
- **Type** — Select the type of the neighbor discovery cache information entry. The possible field values are:
 - *Static* — Shows static neighbor discovery cache entries.
 - *Dynamic* — Shows dynamic neighbor discovery cache entries.

STEP 3 Click the **Add** button. The *Add IPv6 Neighbors Page* opens:

The *Add IPv6 Neighbors Page* provides information for adding a static default gateway.

Add IPv6 Neighbors Page



The *Add IPv6 Neighbors Page* contains the following fields:

- **Interface** — Indicates the neighboring IPv6 interface type. The possible field values are:
 - *VLAN* — Displays the neighboring IPv6 VLAN..
- **IPv6 Address** — Indicates **the IPv6 network assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.**
- **MAC Address** — Indicates the MAC address mapped to the specified IPv6 address.

STEP 4 Define the relevant fields.

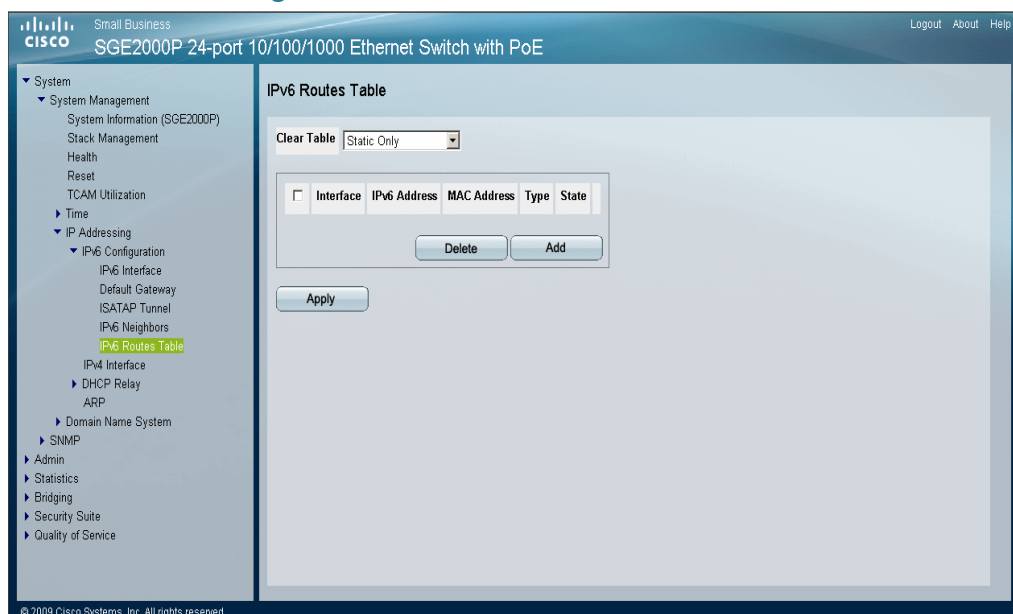
STEP 5 Click **Apply**. The device is updated.

Viewing IPv6 Routes Table

The *IPv6 Routes Table Page* allows network managers to view IPv6 network routes. To view IPv6 routing entries:

- STEP 1** Click >System > System Management > IP Addressing > IPv6 Configuration > IPv6 Routes Table. The *IPv6 Routes Table Page* opens:

IPv6 Routes Table Page



The *IPv6 Routes Table Page* contains the following fields:

- **Clear Table** — Deletes the entries in the IPv6 Routes Table. The possible field values are:
 - *Static Only* — Deletes the static IPv6 address entries from the IPv6 Routes Table.
 - *Dynamic Only* — Deletes the dynamic IPv6 address entries from the IPv6 Routes Table.
 - *All Dynamic and Static* — Deletes the static and dynamic address entries IPv6 address entries from the IPv6 Routes Table.
- **Interface** _ — Indicates the interface that is used to forward the packet.
- **IPv6 Address** — Displays the destination IPv6 address.

- **Next Hop** — Displays the address to which the packet is forwarded (typically the address of a neighboring router). This can be either a Link Local or Global address.
- **Metric** — Indicates the value used for comparing this route to other routes with the same destination in the IPv6 route table.
- **Route Type** — Defines whether the destination is directly attached and the means by which the entry was learned. The following values are:
 - *Local* — Indicates the destination is directly connected. The entry was added statically. This type of route will typically have a Prefix Length of 64 and no Next Hop address in the Next Hop field.
 - *Dynamic* — Indicates the destination is not directly attached. Entry was learned dynamically via the ICMP protocol.

Layer 2 IP Addressing

The IP address and default gateway can be either dynamically or statically configured. In Layer 2, a static IP address is configured on the *IPv4 Interface Page*. The Management VLAN is set to VLAN 1 by default, but can be modified.

When the system is in stacking mode with a Backup Master present, configure the IP address as a static address. This prevents disconnecting from the network during a Stacking Master switchover.

Layer 3 IP Addressing

In Layer 3 mode, multiple IP addresses can be configured on ports, LAGs or VLANs. This provides greater network flexibility than Layer 2 mode where only a single IP address is configured on VLANs only. A predefined Default Gateway is not provided in Layer 3. To manage the device remotely, a default route is defined. The Default Route is the route with the next hop of 0.0.0.0. The Default Route is defined in the *IP Static Routing Page*.

The IP Addressing section contains the following topics:

- Defining IPv4 Interface (Layer 2)
- Defining IPv4 Interface (Layer 3)
- Enabling ARP Proxy (Layer 3)
- Defining UDP Relay (Layer 3)

- Defining DHCP Relay (Layer 3)
- ARP

Defining IPv4 Interface (Layer 2)

The *IPv4 Interface Page* contains fields for assigning IPv4 addresses. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces.

STEP 1 Click **System > System Management > IP Addressing > IPv4 Interface**. The *IPv4 Interface Page* opens:

IPv4 Interface Page

The screenshot shows the Cisco Small Business SGE2000P web interface. The left sidebar contains a navigation tree with the following items: System, System Management, System Information (SGE2000P), Stack Management, Health, Reset, TCAM Utilization, Time, IP Addressing, IPv6 Configuration, IPv6 Interface, Default Gateway, ISATAP Tunnel, IPv6 Neighbors, IPv6 Routes Table, IPv4 Interface (highlighted), DHCP Relay, ARP, Domain Name System, SNMP, Admin, Statistics, Bridging, Security Suite, and Quality of Service. The main content area is titled 'IPv4 Interface' and contains the following fields: 'Supported IP Format' (Version 4), 'Get Dynamic IP from DHCP Server' (radio button), 'Static IP Address' (radio button), 'Management VLAN' (dropdown menu), 'IP Address' (text field), 'Network Mask' (text field), 'Prefix Length' (text field), 'User Defined Default Gateway' (text field), 'Active Default Gateway' (text field), and 'Remove User Defined' (checkbox). An 'Apply' button is at the bottom.

The *IPv4 Interface Page* contains the following fields:

- **Supported IP Format** — Displays the supported IP format: Version 4.
- **Get Dynamic IP from DHCP Server** — Retrieves the IP addresses using DHCP.
- **Static IP Address** — Permanent IP addresses are defined by the administrator. IP addresses are either configured on the Default VLAN or are user-defined.
- **Management VLAN** — Sets the management VLAN. The Management VLAN is used to access the switch through telnet and / or the web GUI. Management VLAN is set to 1by default.

- **IP Address** — The currently configured IP address.
- **Network Mask** — Displays the currently configured IP address mask.
- **Prefix Length** — Specifies the length of the IPv6 prefix. The range is 5 -128 (64 in the case EUI-64 parameter is used). The *Prefix* field is applicable only when the IPV6 Static IP Address is defined as a Global IPv6 Address.
- **User Defined Default Gateway** — Manually defined default gateway IP address.
- **Active Default Gateway** — Active default gateway's IP Address.
- **Remove User Defined** — Removes the selected IP address from the interface. The possible field values are:
 - *Checked* — Removes the IP address from the interface.
 - *Unchecked* — Maintains the IP address assigned to the Interface.

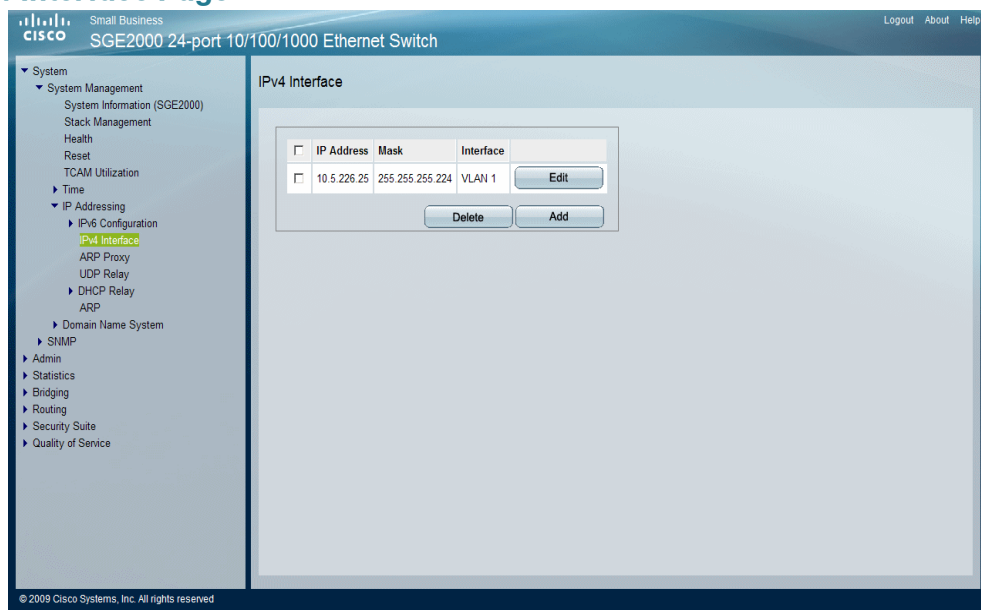
STEP 2 Click **Apply**. The IP Interface settings are defined, and the device is updated.

Defining IPv4 Interface (Layer 3)

The *IPv4 Interface Page* contains fields for assigning IPv4 addresses. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces. This section is applicable to Layer 3 devices only.

STEP 1 Click **System > System Management > IP Addressing > IPv4 Interface**. The *IPv4 Interface Page* opens:

IPv4 Interface Page



The *IPv4 Interface Page* contains the following fields:

- **IP Address** — Displays the currently configured IP address.
- **Mask** — Displays the currently configured IP address mask.
- **Interface** — Displays the interface used to manage the device.

STEP 2 Click the **Add** button. The *Add IP Interface Page* opens:

Add IP Interface Page

The screenshot shows the 'Add IP Interface' page. It contains the following fields and controls:

- Interface**: Radio buttons for Port (selected), LAG, and VLAN. The selected value is 91.
- IP Address**: A text input field.
- Network Mask**: A text input field.
- Prefix Length**: A text input field.
- Apply**: A button to save the configuration.

The *Add IP Interface Page* contains the following fields:

- **Interface** — Specifies the interface to be associated with this IP configuration.
- **IP Address** — Defines the currently configured IP address.
- **Network Mask** — Defines the currently configured IP address mask.
- **Prefix Length** — Specifies the length of the IPv6 prefix. The range is 5 -128 (64 in the case EUI-64 parameter is used). The *Prefix* field is applicable only when the IPV6 Static IP Address is defined as an Global IPv6 Address.

STEP 3 Define the relevant fields.

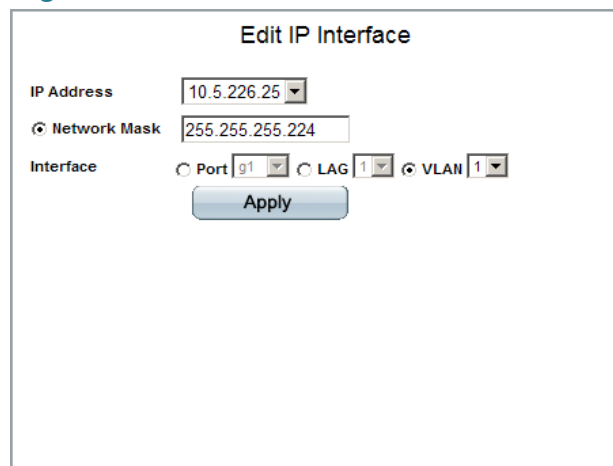
STEP 4 Click **Apply**. The new IP interface configuration is defined, and the device is updated.

Modifying IP Interface Settings

STEP 1 Click **System > System Management > IP Addressing > IP Interface**. The *IPv4 Interface Page* opens:

STEP 2 Click the **Edit** button. The *Edit IP Interface Page* opens:

Edit IP Interface Page



The screenshot shows the 'Edit IP Interface' configuration page. It contains the following fields and controls:

- IP Address**: A text box with the value '10.5.226.25' and a dropdown arrow.
- Network Mask**: A text box with the value '255.255.255.224' and a radio button icon to its left.
- Interface**: A section with three options: 'Port' (selected with a radio button), 'LAG' (with a radio button), and 'VLAN' (with a radio button). Each option has a dropdown menu showing a value (91, 1, and 1 respectively).
- Apply**: A blue button at the bottom.

The *Edit IP Interface Page* contains the following fields:

- **IP Address** — Defines the currently configured IP address.
- **Network Mask** — Defines the currently configured IP address mask.
- **Interface** — Specifies the interface associated with this IP configuration.

STEP 3 Define the relevant fields.

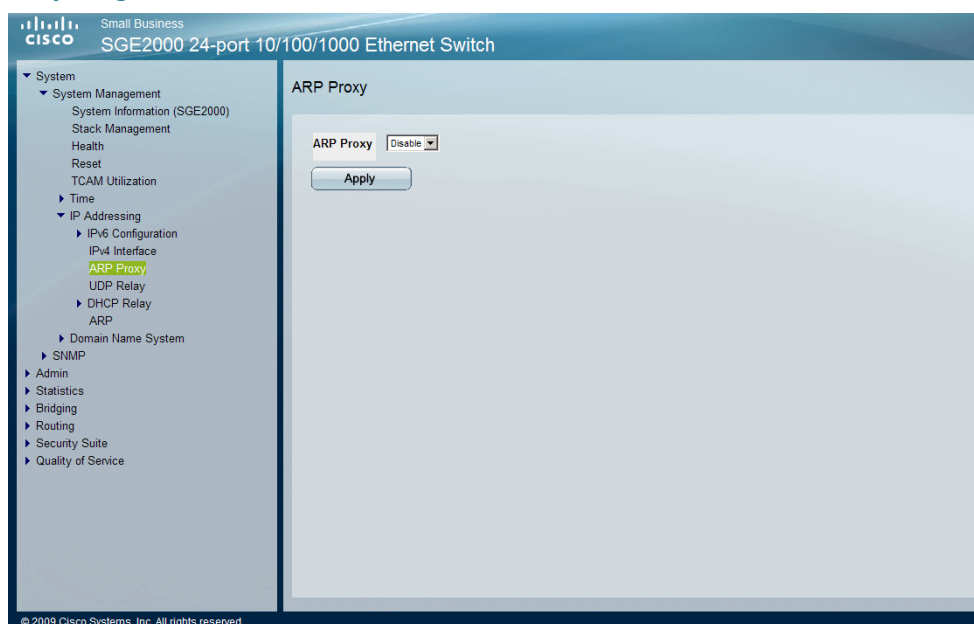
STEP 4 Click **Apply**. The IP interface configuration is defined, and the device is updated.

Enabling ARP Proxy (Layer 3)

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. The *ARP Proxy Page* allows network managers to enable ARP Proxy on the switch. This section is applicable to Layer 3 devices only.

STEP 1 Click **System > System Management > IP Addressing > ARP Proxy**. The *ARP Proxy Page* opens:

ARP Proxy Page



The *ARP Proxy Page* contains the following field.

- **ARP Proxy** — Defines the ARP Proxy status. The possible values are:
 - *Enable* — Enables the device to respond to ARP requests for located nodes.
 - *Disable* — The device responds with its own MAC address.

STEP 2 Select **ARP Proxy**.

STEP 3 Click **Apply**. ARP Proxy is enabled, and the device is updated.

Defining UDP Relay (Layer 3)

The UDP Relay allows UDP packets to reach other networks. This feature enables browsing from workstations to servers on different networks. This section is applicable to Layer 3 devices only.

To define UDP Relay:

STEP 1 Click **System > System Management > IP Addressing > UDP Relay**. The *Defining UDP Relay Page* opens:

Defining UDP Relay Page

| Source IP Interface | UDP Destination Port | Destination Address |
|--|----------------------|---------------------|
| <input type="checkbox"/> 255.255.255.255 | 7 | 255.255.255.255 |

Delete Add

The *Defining UDP Relay Page* contains the following fields:

- **Source IP Interface** — Indicates the input IP interface that relays UDP packets. If this field is 255.255.255.255, UDP packets from all interfaces are relayed. The following address ranges are
 - 0.0.0.0 to 0.255.255.255.
 - 127.0.0.0 to 127.255.255.255.

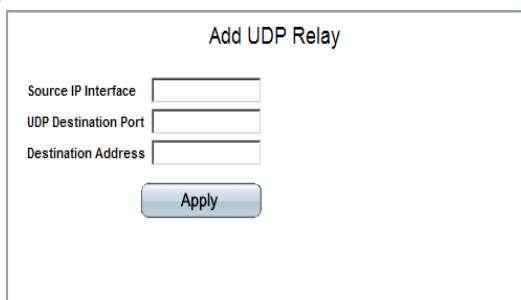
- **UDP Destination Port**— Indicate the destination UDP port ID number of the relayed UDP packets. The following table lists UDP Port allocations.

| UDP Port Number | Acronym | Application |
|-----------------|--------------------------|----------------------------------|
| 7 | Echo | Echo |
| 11 | SysStat | Active User |
| 15 | NetStat | Netstat |
| 17 | Quote | Quote of the day |
| 19 | CHARGEN | Character Generator |
| 20 | FTP-data | FTP Data |
| 21 | FTP | FTP |
| 37 | Time | Time |
| 42 | NAMESERVE | Host Name Server |
| 43 | NICNAME | Who is |
| 53 | DOMAIN | Domain Name Serve |
| 69 | FTP | Trivial File Transfer |
| 111 | SUNRPC | Sun Microsystems Rpc |
| 123 | NTP | Network Time |
| 123 | NTP | Network Tim |
| 137 | NetBiosNameService | NT Server to Station Connections |
| 138 | NetBiosDatagramService | NT Server to Station Connections |
| 139 | NetBios SessionServiceNT | Server to Station Connections |
| 161 | SNMP | Simple Network Management |
| 162 | SNMP-trap | Simple Network Management Traps |
| 513 | who | Unix Rwho Daemon |
| 525 | timed | Time Daemon |
| 514 | syslog | System Log |

- **Destination Address**— The IP interface that receives UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

STEP 2 Click the **Add** button. The *Add UDP Relay Page* opens:

Add UDP Relay Page



The *Add UDP Relay Page* contains the following fields:

- **Source IP Interface** — Indicates the input IP interface that relays UDP packets. If this field is 255.255.255.255, UDP packets from all interfaces are relayed. The following address ranges are
 - 0.0.0.0 to 0.255.255.255.
 - 127.0.0.0 to 127.255.255.255.
- **UDP Destination Port**— Indicate the destination UDP port ID number of the relayed UDP packets. The following table lists UDP Port allocations
- **Destination Address**— The IP interface that receives UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The UDP Relay Settings are defined, and the device is updated.

Defining DHCP Relay (Layer 2)

The *DHCP Server Page* enables users to establish a DHCP configuration with multiple DHCP servers to ensure redundancy.

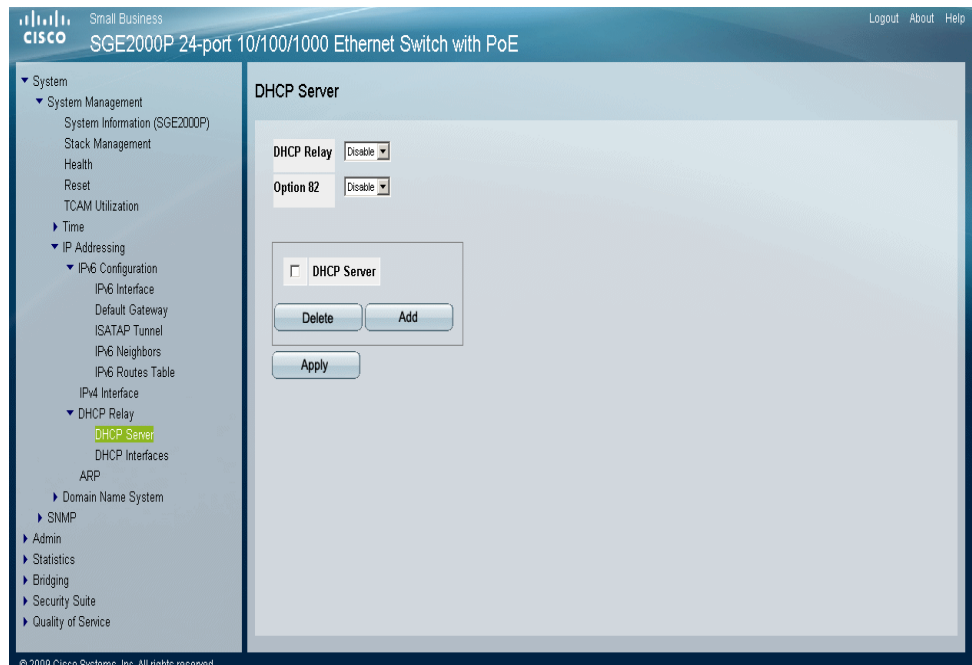
The DHCP servers act as a DHCP relay if the parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to respond first.

The table on this page lists ports and LAGs on which DHCP relay has been enabled.

To define the DHCP Relay configuration:

- STEP 1** Click **System > System Management > IP Addressing > DHCP Relay > DHCP Server**. The *DHCP Server Page* opens:

DHCP Server Page



The *DHCP Server Page* Server contains the following fields:

- **DHCP Relay** — Enable or disable DHCP Relay on the device. The possible values are:
 - *Enable* — Enable DHCP Relay on the device.
 - *Disable* — Disable DHCP Relay on the device.
- **Option 82** — Indicates if DHCP Option 82 with data insertion is enabled on the device. DHCP with Option 82 attaches authentication messages to the packets sent from the host. DHCP passes the configuration information to hosts on a TCP/IP network. This permits network administrators to limit address allocation to authorized hosts. DHCP with Option 82 can be enabled only if DHCP snooping is enabled. The possible field values are:
 - **Enable** — Enables DHCP Option 82 with data insertion on the device. If DHCP Option 82 with data insertion is enabled the DHCP server can insert information into DHCP requests. The DHCP information is used to assign IP addresses to network interfaces.

- **Disable** — Disables DHCP Option 82 with data insertion on the device. This is the default value.

- **DHCP Server** — Port or LAG on which DHCP Relay has been enabled.

STEP 2 Click the **Add** button. The *Add DHCP Server Page* opens:

Add DHCP Server Page

The screenshot shows a web form titled "Add DHCP Server". It contains two labels: "Supported IP Format" and "DHCP Server IP Address". The "Supported IP Format" label has a dropdown menu currently showing "Version 4". The "DHCP Server IP Address" label has an adjacent text input field. Below these fields is a blue "Apply" button.

The *Add DHCP Server Page* contains the following field:

- **Support IP Format** — Provides the supported IP format: Version 6 or Version 4.
- **DHCP Server IP Address** — Defines the IP address assigned to the DHCP server.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The DHCP Server is defined, and the device is updated.

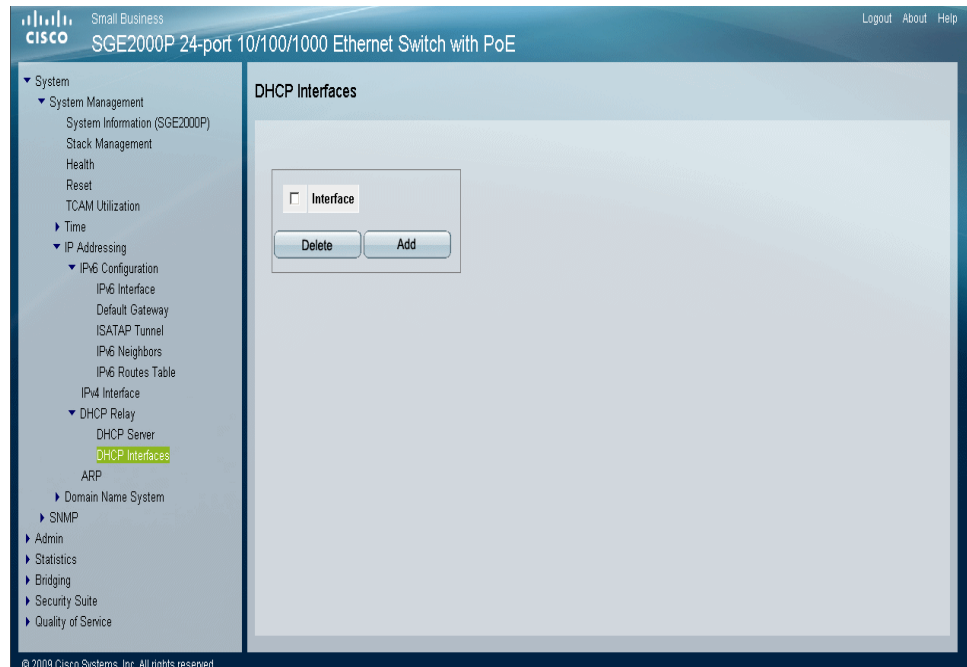
Defining DHCP Relay Interfaces

Enabling Relay functionality provides multiple interfaces to be configured for establishing a DHCP Configuration with multiple DHCP servers to ensure redundancy. IP Addresses are controlled and distributed one-by-one to avoid storming the device.

To define the DHCP Relay configuration:

- STEP 1** Click **System > System Management > IP Addressing > DHCP Relay > DHCP Interfaces**. The *DHCP Interfaces Page* opens:

DHCP Interfaces Page

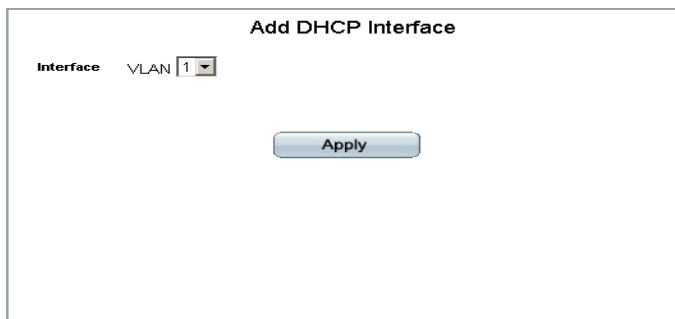


The *DHCP Interfaces Page* contains the following fields:

- **Interface** — Displays the interface selected for relay functionality.
- **Check Box** — Removes DHCP relay from an interface. The possible field values are:
 - *Checked* — Removes the selected DHCP Relay interface.
 - *Unchecked* — Maintains the selected DHCP Relay interface.

- STEP 2** Click the **Add** button. The *Add DHCP Interface Page* opens:

Add DHCP Interface Page



The *Add DHCP Interface Page* contains the following field:

- **Interface** — Selects the interface to define DHCP Relay. The possible field values are:
 - **Ports** — Defines the DHCP Relay on the selected port.
 - **LAGs** — Defines the DHCP Relay on the selected LAG.
 - **VLAN** — Defines the DHCP Relay on the selected VLAN.

STEP 3 Select the Interface on which to define a DHCP Relay.

STEP 4 Click **Apply**. A DHCP Relay Interface is defined, and the device is updated.

Defining DHCP Relay (Layer 3)

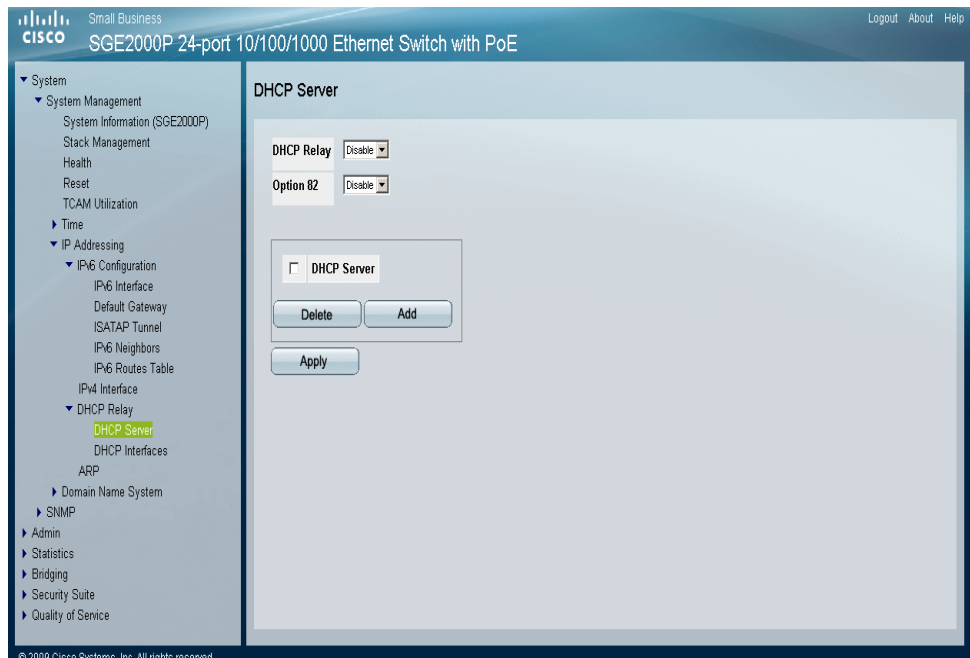
The *DHCP Server Page* enables users to establish a DHCP configuration with multiple DHCP servers to ensure redundancy. IP Addresses are controlled and distributed one-by-one to avoid overloading the device.

The DHCP servers act as a DHCP relay if the parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to respond first.

To define the DHCP Relay (Layer 3) configuration:

- STEP 1** Click **System > System Management > IP Addressing > DHCP Relay > DHCP Server**. The *DHCP Server Page* opens:

DHCP Server Page



The *DHCP Server Page* contains the following fields:

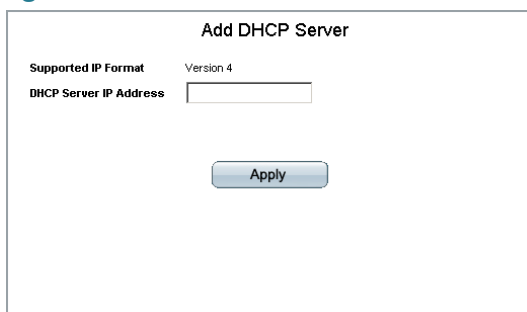
- **DHCP Relay** — Enable or disable DHCP Relay on the device. The possible values are:
 - *Enable* — Enable DHCP Relay on the device.
 - *Disable* — Disable DHCP Relay on the device.
- **Option 82** — Indicates if DHCP Option 82 with data insertion is enabled on the device. DHCP with Option 82 attaches authentication messages to the packets sent from the host. DHCP passes the configuration information to hosts on a TCP/IP network. This permits network administrators to limit address allocation to authorized hosts. DHCP with Option 82 can be enabled only if DHCP snooping is enabled. The possible field values are:
 - **Enable** — Enables DHCP Option 82 with data insertion on the device. If DHCP Option 82 with data insertion is enabled the DHCP server can insert information into DHCP requests. The DHCP information is used to assign IP addresses to network interfaces.

- **Disable** — Disables DHCP Option 82 with data insertion on the device. This is the default value.

- **DHCP Server** — Defines the address of the remote DHCP server to track across the VLANs.

STEP 2 Click the **Add** button. The *Add DHCP Server Page* opens:

Add DHCP Server Page

The screenshot shows a web form titled "Add DHCP Server". It contains two fields: "Supported IP Format" with a dropdown menu currently showing "Version 4", and "DHCP Server IP Address" with an empty text input box. Below these fields is a blue "Apply" button.

The *Add DHCP Server Page* contains the following field:

- **Support IP Format** — Provides the supported IP format: Version 6 or Version 4.
- **DHCP Server IP Address** — Defines the DHCP server IP address.

STEP 3 Specify the IP address of the server.

STEP 4 Click **Apply**. DHCP is enabled , and the device is updated.

ARP

The *Address Resolution Protocol* (ARP) is the method for finding a host's Link Layer (MAC) address when only its Internet Layer (IP) address is known. The ARP table is used to maintain a correlation between each MAC address and its corresponding IP address. The ARP table can be filled in statically by the user. When a static ARP entry is defined, a permanent entry is put in the table, which the system uses to translate IP addresses to MAC addresses.

To define ARP:

STEP 1 Click **System > System Management > IP Addressing > ARP**. The *ARP Page* opens:

ARP Page

Small Business
Cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

System Management

System Information (SGE2000P)

Stack Management

Health

Reset

TCAM Utilization

Time

IP Addressing

IPV6 Configuration

IPV6 Interface

Default Gateway

ISATAP Tunnel

IPV6 Neighbors

IPV6 Routes Table

IPV4 Interface

DHCP Relay

DHCP Server

DHCP Interfaces

ARP

Domain Name System

SNMP

Admin

Statistics

Bridging

Security Suite

Quality of Service

ARP

ARP Entry Age Out: 60000 (Sec)

Clear ARP Table Entries: All

| <input type="checkbox"/> | Interface | IP Address | MAC Address | Status | |
|-------------------------------------|-----------|--------------|-------------------|---------|------|
| <input checked="" type="checkbox"/> | VLAN 1 | 10.5.234.14 | 00:13:20:8b:bd:1e | Dynamic | Edit |
| <input checked="" type="checkbox"/> | VLAN 1 | 10.5.234.253 | 00:18:74:75:f1:80 | Dynamic | Edit |
| <input checked="" type="checkbox"/> | VLAN 1 | 10.5.234.254 | 00:1b:d4:6d:1b:00 | Dynamic | Edit |

Delete Add

Apply

© 2009 Cisco Systems, Inc. All rights reserved.

The *ARP Page* contains the following fields.

- **ARP Entry Age Out** — Defines the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 1 - 40000000, where zero indicates that entries are never cleared from the cache. The default value is 60,000 seconds.
- **Clear ARP Table Entries**— Indicates the type of ARP entries that are cleared on all devices. The possible values are:
 - *All* — All ARP entries are cleared.
 - *Dynamic* — Only dynamic ARP entries are cleared.
 - *Static* — Only static ARP entries are cleared.
 - *None* — ARP Entries are not cleared.

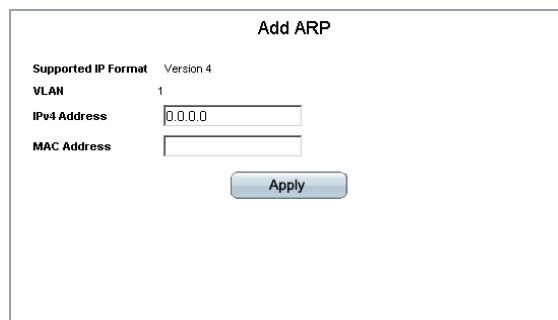
ARP Table

- **Interface** — Indicates the interface for which the ARP parameters are defined.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address.

- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Indicates the ARP Table entry status. Possible field values are:
 - *Dynamic* — Indicates the ARP entry was learned dynamically.
 - *Static* — Indicates the ARP entry is a static entry.

STEP 2 Click **Add**. The *Add ARP Page* opens:

Add ARP Page



The screenshot shows the 'Add ARP' configuration page. It has a title 'Add ARP' at the top right. Below the title, there are three fields: 'Supported IP Format' with a dropdown menu showing 'Version 4', 'VLAN' with a text box containing '1', and 'IPv4 Address' with a text box containing '0.0.0.0'. There is also a 'MAC Address' field with an empty text box. At the bottom right of the form is an 'Apply' button.

The *Add ARP Page* contains the following fields:

- **Supported IP Format** — Indicates the IP address format supported by the host. The possible field values are:
 - *Version 4* — Indicates that the host supports IPv4 addresses only.
- **VLAN** — Indicates the ARP-enabled interface.
- **IPv4 Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.

STEP 3 Define the relevant fields.

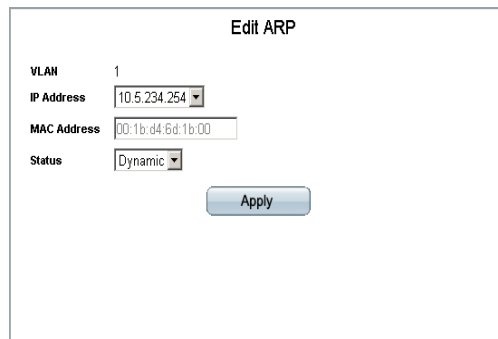
STEP 4 Click **Apply**. The ARP Settings are defined, and the device is updated.

Modifying ARP Settings

STEP 1 Click **System > System Management > IP Addressing > ARP**. The *ARP Page* opens:

STEP 2 Click the **Edit** button. The *Edit ARP Page* opens:

Edit ARP Page



The *Edit ARP Page* contains the following fields:

- **VLAN** — Indicates the ARP-enabled interface.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Defines the ARP Table entry status. Possible field values are:
 - *Dynamic* — Indicates the ARP entry is learned dynamically.
 - *Static* — Indicates the ARP entry is a static entry.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The ARP Settings are modified, and the device is updated.

Defining IP Routing

If the switch has been defined as a router, network managers can define up to 32 static IP routes.

To define IP Routing:

STEP 1 Click **Routing > IP Static Routing**. The *IP Static Routing Page* opens:

IP Static Routing Page

Small Business
cisco SGE2000 24-port 10/100/1000 Ethernet Switch

System
Admin
Statistics
Bridging
Routing
IP Static Routing
Security Suite
Quality of Service

IP Static Routing

| <input type="checkbox"/> | Dest. IP Address | Prefix Length | Next Hop | Route Type | Metric |
|-------------------------------------|------------------|---------------|------------|------------|--------|
| <input checked="" type="checkbox"/> | 10.5.226.0 | /27 | | Local | |
| <input type="checkbox"/> | 0.0.0.0 | /0 | 10.5.226.1 | Remote | 1 |

Delete Add

Apply

© 2009 Cisco Systems, Inc. All rights reserved.

The *IP Static Routing Page* contains the following fields:

- **Dest. IP Address** — Defines the destination IP address.
- **Prefix Length** — Specifies the IP route prefix length for the destination IP address, preceded by a forward slash. the prefix length.
- **Next Hop** — Indicates the next hop's IP address or IP alias on the route.
- **Route Type** — Defines the route type. The possible field values are:
 - *Reject* — Rejects the route, and stops routing to the destination network via all gateways.
 - *Remote* — Indicates the route is a remote path.
- **Metric** — Indicates the administrative distance to the next hop. The range is 1-255. The default value is 1.

STEP 2 Click the **Add** button. The *Add IP Static Route Page* opens:

Add IP Static Route Page

Add IP Static Route

Destination IP Address Network Mask

Prefix Length (/xx)

Next Hop

Route Type

Metric (1-255)

Apply

In addition to the fields in the *IP Static Routing Page*, the *Add IP Static Route Page* contains the following additional fields:

- **Destination IP Address** — Defines the destination IP address.
- **Network Mask** — Defines the currently configured IP address mask.
- **Prefix Length** — Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash (/).
- **Next Hop** — Defines the next hop's IP address or IP alias on the route.
- **Route Type** — Defines the route type. The possible field values are:
 - *Reject* — Rejects the route, and stops routing to the destination network via all gateways.
 - *Remote* — Indicates the route is a remote path.
- **Metric(1-255)** — Defines the administrative distance to the next hop. The range is 1-255. The default value is 1.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The IP Static route is added, and device is updated.

Domain Name System

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated into 192.87.56.2. DNS servers maintain databases of domain names and their corresponding IP addresses. The Domain Name System contains the following windows:

- Defining DNS Servers
- Mapping DNS Hosts

Defining DNS Servers

The *DNS Servers Page* contains fields for enabling and activating specific DNS servers.

To enable a DNS server:

- STEP 1** Click **System > System Management > IP Addressing > Domain Name System > DNS Servers**. The *DNS Servers Page* opens:

DNS Servers Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE management interface. The left sidebar contains a navigation tree with the following structure:

- System
 - System Management
 - System Information (SGE2000P)
 - Stack Management
 - Health
 - Reset
 - TCAM Utilization
 - Time
 - IP Addressing
 - IPv6 Configuration
 - IPv4 Interface
 - DHCP Relay
 - ARP
 - Domain Name System
 - DNS Servers** (highlighted)
 - Host Mapping
 - SNMP
 - Admin
 - Statistics
 - Bridging
 - Security Suite
 - Quality of Service

The main content area is titled "DNS Servers" and contains the following fields and controls:

- Enable DNS:** A checkbox that is checked.
- Default Parameters:** A section containing:
 - Default Domain Name:** A text input field.
 - Type:** A dropdown menu.
 - Remove:** A checkbox that is unchecked.
- Server Selection:** A section with two radio buttons:
 - ☐ DNS Server
 - ☒ Active Server
- Buttons:** "Delete", "Add", and "Apply" buttons.

The *DNS Servers Page* contains the following fields.

- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:
 - *Checked* — Translates the domains into IP addresses.
 - *Unchecked* — Disables translating domains into IP addresses.

Default Parameters

- **Default Domain Name** — Specifies the user-defined DNS server name (1 -158 characters).
- **Type** — Displays the IP address type. The possible field values are:
 - *Dynamic* — The IP address is dynamically created.
 - *Static* — The IP address is a static IP address.
- **Remove** — Removes DNS servers. The possible field values are:
 - *Checked* — Removes the selected DNS server
 - *Unchecked* — Maintains the current DNS server list.

DNS Server Details

- **DNS Server** — Displays the DNS server's IP address, up to four DNS servers can be defined.
- **Active Server** — Specifies the DNS server that is currently active.

STEP 2 Click the **Add** button. The *Add DNS Server Page* opens:

Add DNS Server Page

The *Add DNS Server Page* allows system administrators to define new DNS servers. The *Add DNS Server Page* page contains the following fields.

- **Supported IP Format**— Select version 6 for IPv6 or version 4 for IPv4.

- **IPv6 Address Type** — Indicates the IPv6 Type. The possible field values are:
 - *Link-Local* — Indicates the IPv6 address is link-local.
 - *Global Unicast* — Indicates the IPv6 address is global Unicast.
- **Link Local Interface** — Indicates the IPv6 link-local interface. The possible field values are:
 - *VLAN* — Indicates that the IPv6 link-local interface is defined as a VLAN used.
 - *ISATAP* — Indicates that the IPv6 link-local interface is defined as a virtual IPv6 local link via ISATAP.
- **DNS Server IP Address** — Enter the DNS server's IP address.
- **Set DNS Server Active** — Defines active status of the new DNS Server. The possible values are:
 - *Checked* — This new server becomes the active DNS Server.
 - *Unchecked* — This new server is not the active DNS Server.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The DNS server is added, and the device is updated.

Mapping DNS Hosts

The *Host Mapping Page* provides information for defining DNS Host Mapping.

To add a host map:

- STEP 1** Click **System > System Management > IP Addressing > Domain Name System > Host Mapping**. The *Host Mapping Page* opens:

Host Mapping Page

The *Host Mapping Page* contains the following fields:

- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.

- STEP 2** Click the **Add** button. The *Add Host Name Page* opens:

The *Add Host Name Page* provides information for defining DNS Host Mapping.

Add Host Name Page

The *Add Host Name Page* contains the following fields:

- **Supported IP Format** — Indicates the IP address format supported by the host. The possible field values are:
 - *Version 6* — Indicates that the host supports IPv6 addresses.
 - *Version 4* — Indicates that the host supports IPv4 addresses only.
- **IPv6 Address Type** — Indicates the IPv6 Type. The possible field values are:
 - *Link-Local* — Indicates the IPv6 address is link-local.
 - *Global Unicast* — Indicates the IPv6 address is global Unicast.
- **Link Local Interface** — Indicates the IPv6 link-local interface. The possible field values are:
 - *VLAN* — Indicates that VLAN is the IPv6 link-local interface.
 - */ISATAP* — Indicates that the IPv6 link-local interface is defined as a virtual IPv6 local link via ISATAP.
- **Host Name** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.
- **IP Address 2 (optional)** — Indicates the second IPv6 network assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.

- **IP Address 3 (optional)** — Indicates the third IPv6 network assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.
- **IP Address 4 (optional)** — Indicates the fourth IPv6 network assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The DNS Host settings are defined, and the device is updated.

Defining Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frames source address. Frames addressed to a destination MAC address that is not associated with any port, are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

This section contains information for defining both static and dynamic Forwarding Database entries, and includes the following topics:

- Defining Static Addresses
- Defining Dynamic Addresses

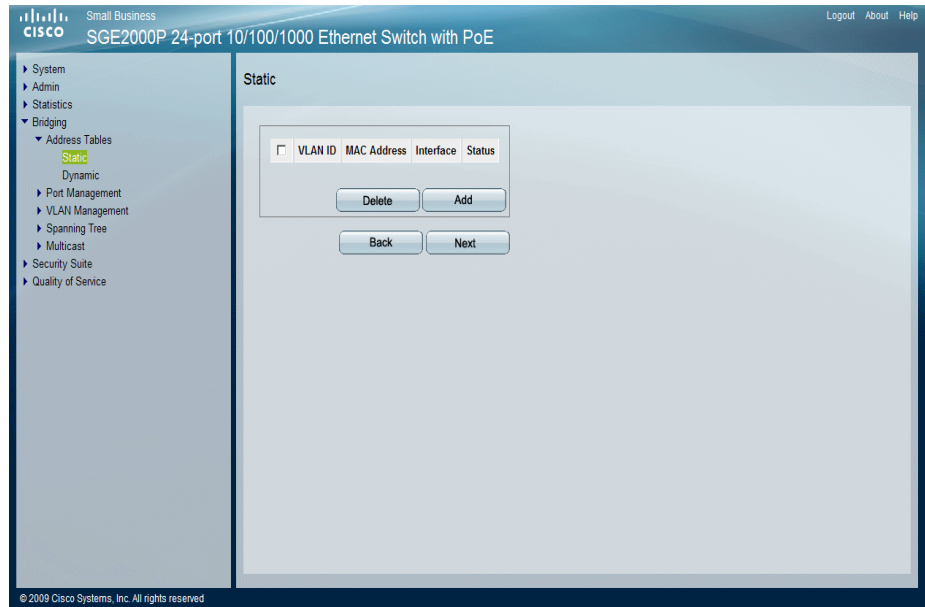
Defining Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and cannot be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

To define static addresses:

STEP 1 Click **Bridging > Address Tables > Static**. The *Static Page* opens:

Static Page



The *Static Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
 - *Port* — The specific port number to which the forwarding database parameters refer.
 - *LAG* — The specific LAG number to which the forwarding database parameters refer.
- **Status** — Displays how the entry was created. The possible field values are:
 - *Permanent* — The MAC address is permanent.
 - *Delete on Reset* — The MAC address is deleted when the device is reset.
 - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
 - *Secure* — The MAC Address is defined for locked ports.

STEP 2 Click the **Add** button. The *Add Static MAC Address Page* opens:

Add Static MAC Address Page

The *Add Static MAC Address Page* contains the following fields:

- **Interface** — Displays the interface to which the entry refers:
 - *Ports* — The specific port number to which the forwarding database parameters refer.
 - *LAGs* — The specific LAG number to which the forwarding database parameters refer.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **VLAN Name** — Displays the VLAN name to which the entry refers.
- **Status** — Displays how the entry was created. The possible field values are:
 - *Permanent* — The MAC address is permanent.
 - *Delete on Reset* — The MAC address is deleted when the device is reset.
 - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
 - *Secure* — The MAC Address is defined for locked ports.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Defining Dynamic Addresses

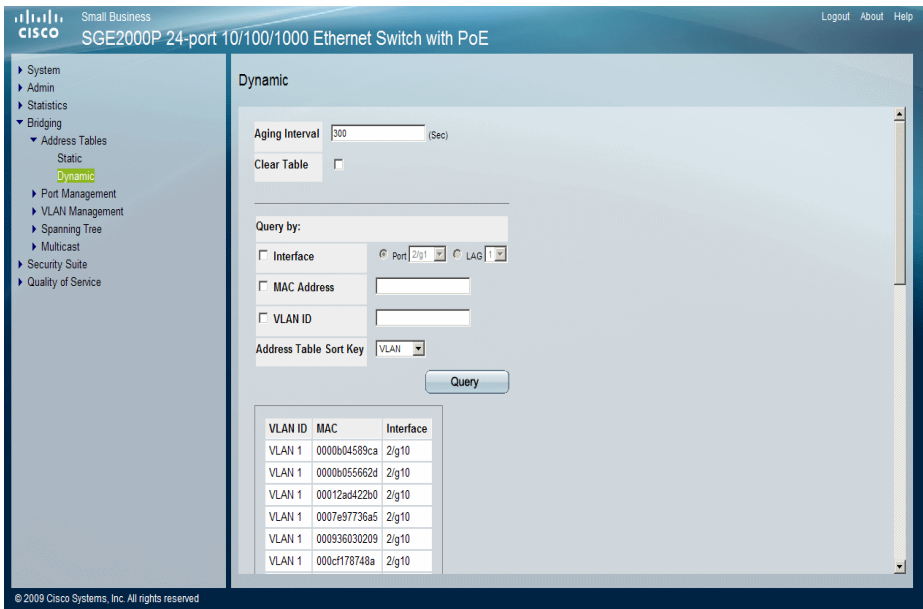
The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

The *Dynamic Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.

To define a dynamic address:

STEP 1 Click **Bridging > Address Tables > Dynamic**. The *Dynamic Page* opens:

Dynamic Page



The *Dynamic Page* contains the following fields:

- **Aging Interval** — Specifies the amount of time the MAC address remains in the Dynamic MAC Address table before it is timed out, if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** — If checked, clears the MAC address table.

Query By

In the Query By section, select the preferred option for sorting the addresses table:

- **Interface** — Specifies the interface for which the table is queried. The query can search for specific ports or LAGs.
- **MAC Address** — Specifies the MAC address for which the table is queried.
- **VLAN ID** — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** — Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.

STEP 2 Define the relevant fields.

STEP 3 Click **Query**. The Dynamic MAC Address Table is queried, and the results are displayed.

Configuring Multicast Forwarding

The Multicast section contains the following topics:

- IGMP Snooping
- Defining Multicast Group
- Configuring IGMP Snooping Mapping
- Defining Multicast TV Membership
- Defining Multicast Forwarding
- Defining Unregistered Multicast Settings

IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

To enable IGMP Snooping:

STEP 1 Click **Bridging > Multicast > IGMP Snooping**. The *IGMP Snooping Page* opens:

IGMP Snooping Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Address Tables
Port Management
VLAN Management
Spanning Tree
Multicast
IGMP Snooping
Multicast Group
Multicast TV VLAN-IGMP Mapping
Multicast TV Membership
Forward
Unregistered Multicast
Security Suite
Quality of Service

IGMP Snooping

Enable IGMP Snooping Status ☐

| VLAN ID | IGMP Snooping Status | Host Timeout | MRouter Timeout | Leave Timeout | |
|---------|----------------------|--------------|-----------------|---------------|------|
| 1 | Disabled | 260 | 300 | 10 | Edit |
| 2 | Disabled | 260 | 300 | 10 | Edit |

Apply

© 2009 Cisco Systems, Inc. All rights reserved

The *IGMP Snooping Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates that the device monitors network traffic to determine which hosts want to receive multicast traffic. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
 - *Checked* — Enables IGMP Snooping on the device.
 - *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the specific VLAN. The possible field values are:
 - *Enabled* — IGMP Snooping is enabled on the VLAN.
 - *Disabled* — IGMP Snooping is not enabled on the VLAN.
- **Host Timeout** — Indicates the amount of the time the Host waits to receive a message before it times out. The default value is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.

- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an *Immediate Leave* value. The default timeout is 10 seconds.

STEP 2 Define the relevant fields.

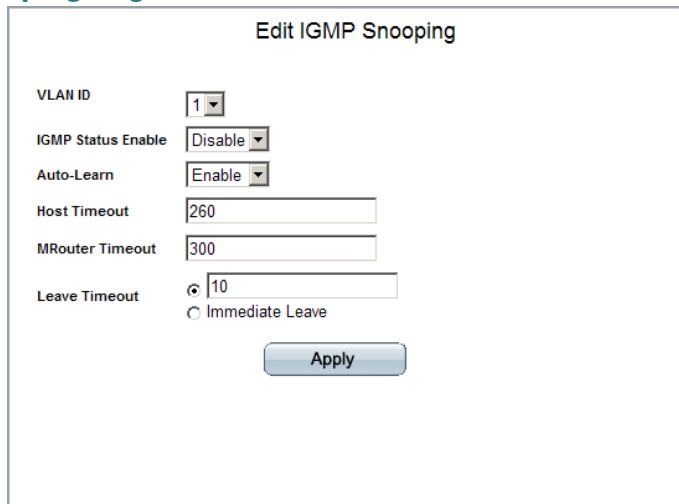
STEP 3 Click **Apply**. The IGMP Snooping Parameters are updated, and the device is updated.

Modifying IGMP Snooping

STEP 1 Click **Bridging > Multicast > IGMP Snooping**. The *IGMP Snooping Page* opens:

STEP 2 Click the **Edit** button. The *Edit IGMP Snooping Page*.

Edit IGMP Snooping Page



The screenshot shows the 'Edit IGMP Snooping' configuration page. It contains the following fields and options:

- VLAN ID**: A dropdown menu with '1' selected.
- IGMP Status Enable**: A dropdown menu with 'Disable' selected.
- Auto-Learn**: A dropdown menu with 'Enable' selected.
- Host Timeout**: A text input field with '260'.
- MRouter Timeout**: A text input field with '300'.
- Leave Timeout**: A radio button selected next to a text input field with '10', and an 'Immediate Leave' radio button option.
- Apply**: A button at the bottom right.

The *Edit IGMP Snooping Page* contains the following fields:

- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Status Enable** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
 - *Enable* — Enables IGMP Snooping on the VLAN.
 - *Disable* — Disables IGMP Snooping on the VLAN.

- **AutoLearn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. The possible field values are:
 - *Enable* — Enables auto learn.
 - *Disable* — Disables auto learn.
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an *Immediate Leave* value. The default timeout is 10 seconds.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

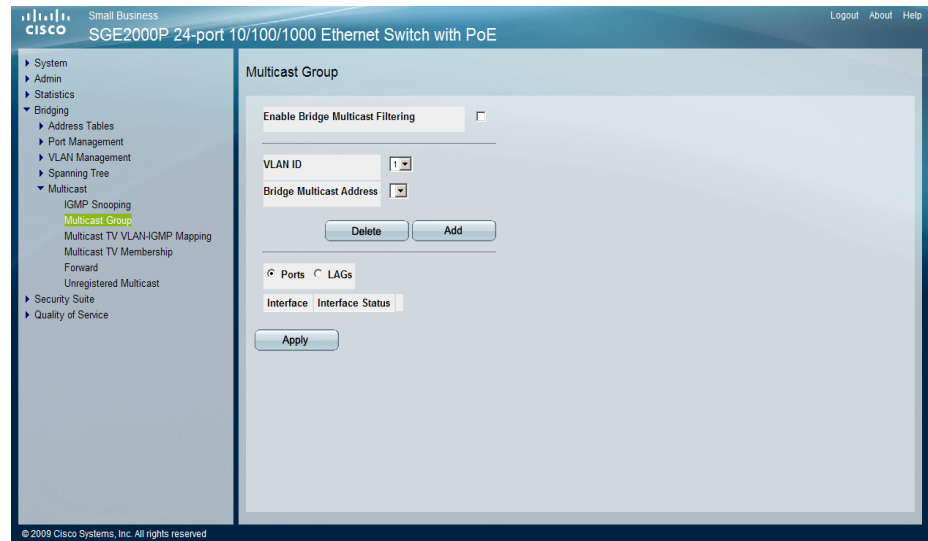
Defining Multicast Group

The *Multicast Group Page* displays the ports and LAGs that are members of Multicast service groups. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The *Multicast Group Page* permits new Multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific Multicast service address group.

To define Multicast group:

STEP 1 Click **Bridging > Multicast > Multicast Group**. The *Multicast Group Page* opens:

Multicast Group Page



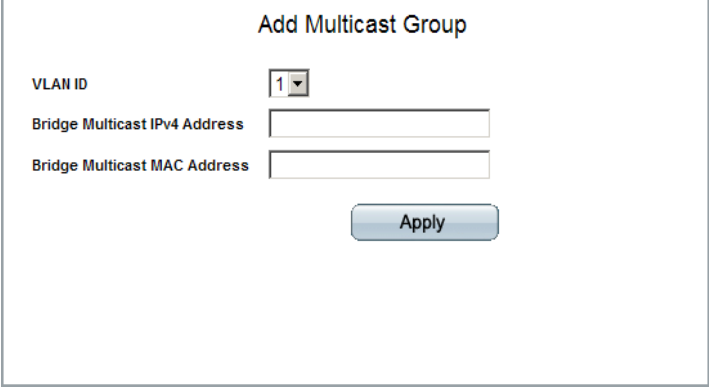
The *Multicast Group Page* contains the following fields:

- **Enable Bridge Multicast Filtering** — Indicates if Bridge Multicast Filtering is enabled on the device. Bridge Multicast Filtering can be enabled only if IGMP Snooping is enabled. The possible field values are:
 - *Checked* — Enables Multicast Filtering on the device.
 - *Unchecked* — Disables Multicast Filtering on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address or IP address.
- **Ports** — Displays the Multicast Group status of all of the specified stacking member's ports.
- **LAGs** — Displays the Multicast Group status of all of the device's LAGs.
- **Interface** — Displays the interface on which the Multicast service is configured.
- **Interface Status** — Displays the interface status. The options are as follows:
 - *Static* — Attaches the interface to the Multicast group as static member in the Static Row. The interface has joined the Multicast group statically in the Current Row.

- *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
- *None* — The interface is not part of a Multicast group.

STEP 2 Click the **Add** button. The *Add Multicast Group Page* opens:

Add Multicast Group Page



The *Add Multicast Group Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Bridge Multicast IP Address** — Displays the IP address attached to the Multicast Group.
- **Bridge Multicast MAC Address** — Displays the MAC address attached to the Multicast Group.

STEP 3 Define the relevant fields.

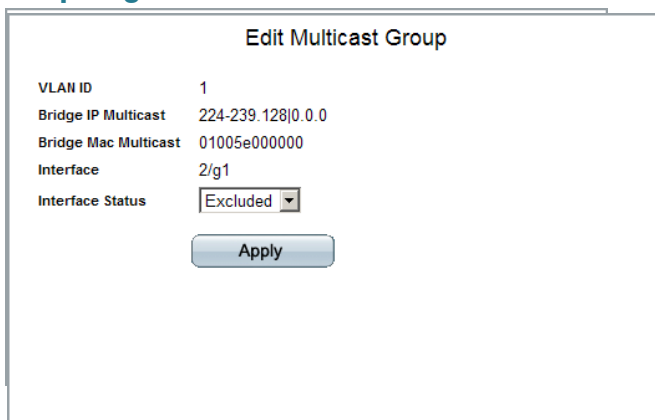
STEP 4 Click **Apply**. The Multicast Group is added, and the device is updated.

Modifying a Multicast Group

STEP 1 Click **Bridging > Multicast > Multicast Groups**. The *Multicast Group Page* opens:

STEP 2 Click the **Edit** button. The *Edit Multicast Group Page* opens.

Edit Multicast Group Page



The screenshot shows a web-based configuration page titled "Edit Multicast Group". It contains the following fields and values:

| Field | Value |
|----------------------|-------------------|
| VLAN ID | 1 |
| Bridge IP Multicast | 224-239.128 0.0.0 |
| Bridge Mac Multicast | 01005e000000 |
| Interface | 2/g1 |
| Interface Status | Excluded |

Below the fields is an "Apply" button.

The *Edit Multicast Group Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Bridge IP Multicast** — Displays the IP address attached to the Multicast Group.
- **Bridge MAC Multicast** — Displays the MAC address attached to the Multicast Group.
- **Interface** — Displays the interface attached to the Multicast Group.
- **Interface Status** — Defines the interface status. The options are as follows:
 - *Static* — Attaches the interface to the Multicast group as static member in the Static Row. The interface has joined the Multicast group statically in the Current Row.
 - *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
 - *None* — The interface is not part of a Multicast group.

STEP 3 Change the **Interface Status**.

STEP 4 Click **Apply**. The Multicast Group parameters are saved, and the device is updated.

Configuring IGMP Snooping Mapping

Multicast TV allows subscribers to join the same Multicast stream, even if the subscribers are not members of the same VLAN, eliminating television traffic duplication. IGMP snooping is supported for those transmissions.

Ports which receive Multicast Transmissions, or *Receiver Ports*, can be defined in any VLAN, and not just in the Multicast VLAN. Receiver ports can only receive Multicast transmissions, they cannot initiate a Multicast TV transmission.

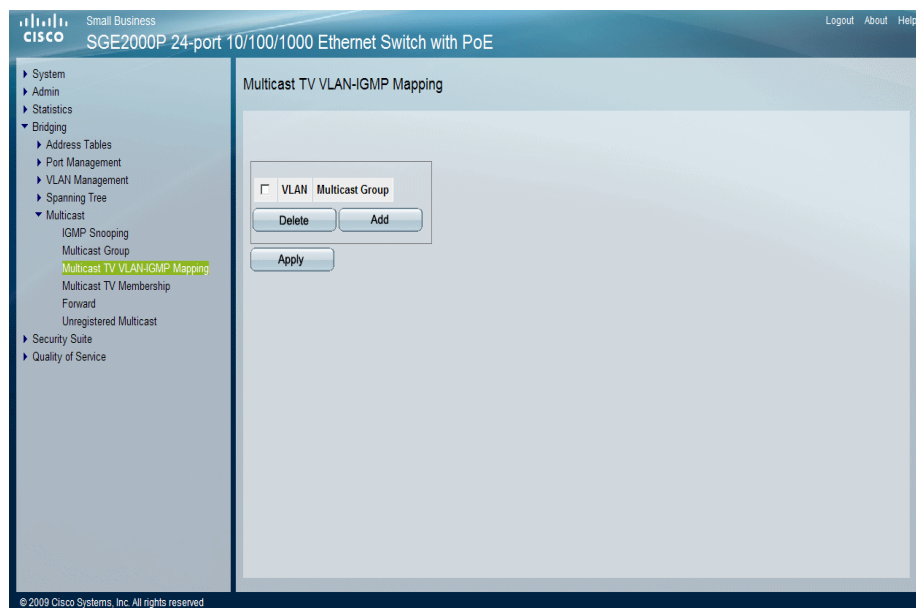
Multicast TV source ports must be a Multicast VLAN members.

IGMP messages are used to indicate which ports are requesting to join or leave the Multicast group. The *Multicast TV VLAN-IGMP Snooping Mapping Page* allows network managers to map IGMP snooping to VLANs.

To define IGMP Snooping mapping:

- STEP 1** Click **Bridging > Multicast > Multicast TV VLAN-IGMP Snooping Mapping**. The *Multicast TV VLAN-IGMP Snooping Mapping Page* opens:

Multicast TV VLAN-IGMP Snooping Mapping Page



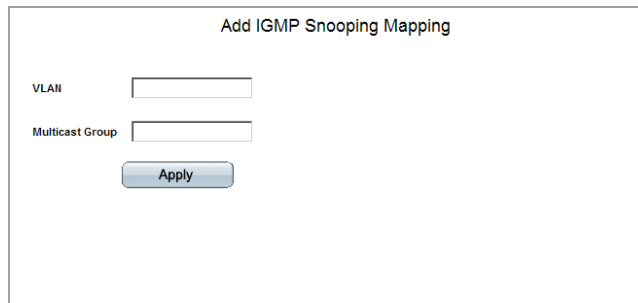
The *Multicast TV VLAN-IGMP Snooping Mapping Page* contains the following fields:

- **VLAN** — Indicates the Multicast TV VLAN for which the IGMP Snooping mapping is enabled.

- **Multicast Group** — Indicates the Multicast group IP address for which the IGMP Snooping is enabled.

STEP 2 Click the **Add** button. The *Add IGMP Snooping Mapping Page* opens:

Add IGMP Snooping Mapping Page



The *Add IGMP Snooping Mapping Page* contains the following fields:

- **VLAN** — Defines the Multicast TV VLAN on which to enable IGMP Snooping.
- **Multicast Group** — Defines the Multicast group IP address on which to enable IGMP Snooping.

STEP 3 Define the fields.

STEP 4 Click **Apply**. IGMP Snooping is enabled on the specified Multicast TV VLAN, and the device is updated.

Defining Multicast TV Membership

The *Multicast TV Membership Page* allows network managers to display the ports associated with a Multicast TV VLAN.

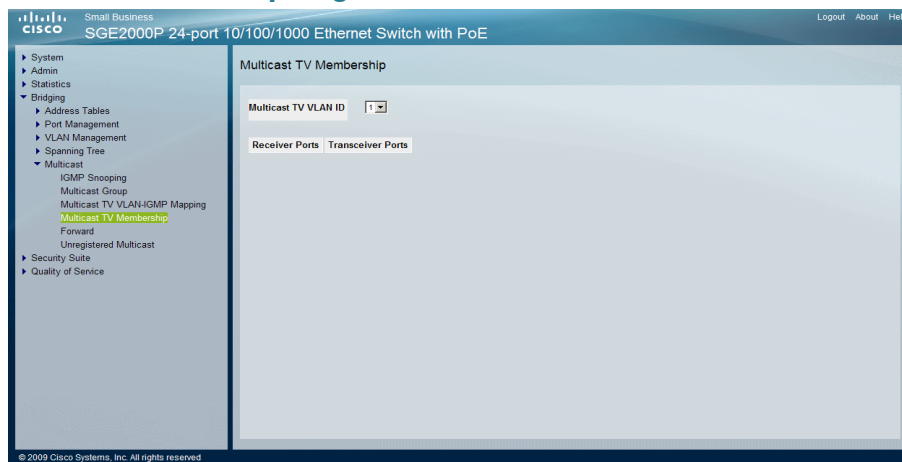


NOTE Ports and trunks are assigned to Multicast VLAN in the *VLAN Interface Setting Page (Layer 2)*.

To view Multicast TV VLAN membership:

- STEP 1** Click **Bridging > Multicast > Multicast TV Membership**. The *Multicast TV Membership Page* opens:

Multicast TV Membership Page



The *Multicast TV Membership Page* contains the following fields:

- **Multicast TV VLAN ID** — Indicates the Multicast VLAN ID in which the source ports and receiver ports are members.
- **Receiver Ports** — Indicates the port on which Multicast TV transmissions are received.
- **Transceiver Ports** — Indicates the source port from which the Multicast TV transmission originates. The source port is learned through the IGMP messages.

- STEP 2** Select a Multicast TV VLAN to view.

- STEP 3** Click **Apply**. The ports that belong to the selected VLAN are displayed in the table.

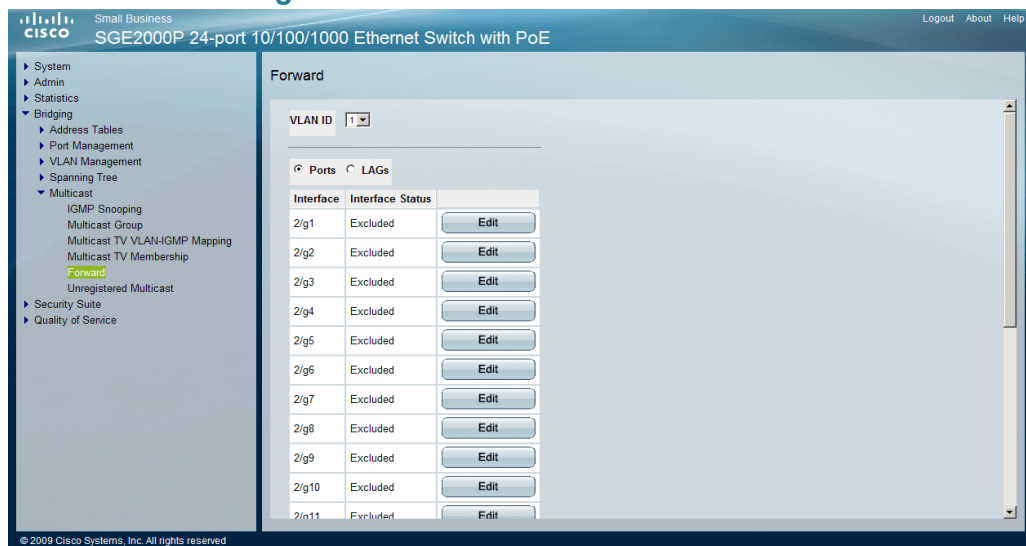
Defining Multicast Forwarding

The *Multicast Forward Page* contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

To define Multicast forward settings:

STEP 1 Click **Bridging > Multicast > Forward**. The *Multicast Forward Page* opens:

Multicast Forward Page



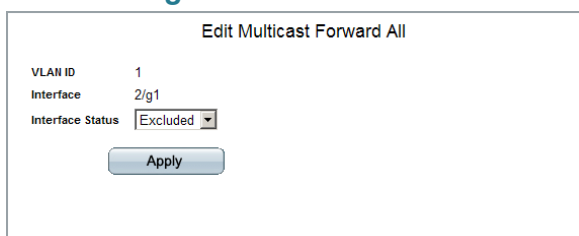
The *Multicast Forward Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Ports** — Displays the Multicast Forwarding status of all of the specified stacking member's ports.
- **LAGs** — Displays the Multicast Forwarding status of all of the device's LAGs.
- **Interface** — Indicates the port or LAG whose Multicast forwarding configuration is described.
- **Interface Status** — Displays the interface status. The options are as follows:
 - *Static* — Attaches the port to the Multicast group as static member.
 - *Forbidden* — Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
 - *Excluded* — The port is not part of a Multicast group.
 - *Dynamic* — Attaches the port to the Multicast group as dynamic member.

Modifying Multicast Forwarding

STEP 2 Click the **Edit** button. The *Edit Multicast Forward All Page* opens:

Edit Multicast Forward All Page



Edit Multicast Forward All

VLAN ID 1

Interface 2/g1

Interface Status Excluded

Apply

The *Edit Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Interface** — Displays the port or LAG attached to the Multicast Group.
- **Interface Status** — Displays the interface status of the port or LAG. The options are as follows:
 - *Static* — Attaches the interface to the Multicast group as a static member.
 - *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP snooping designated the interface to join a Multicast group.
 - *Excluded* — The interface is not part of a Multicast group.
 - *Dynamic* — Attaches the interface or LAG dynamically to the Multicast group.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Defining Unregistered Multicast Settings

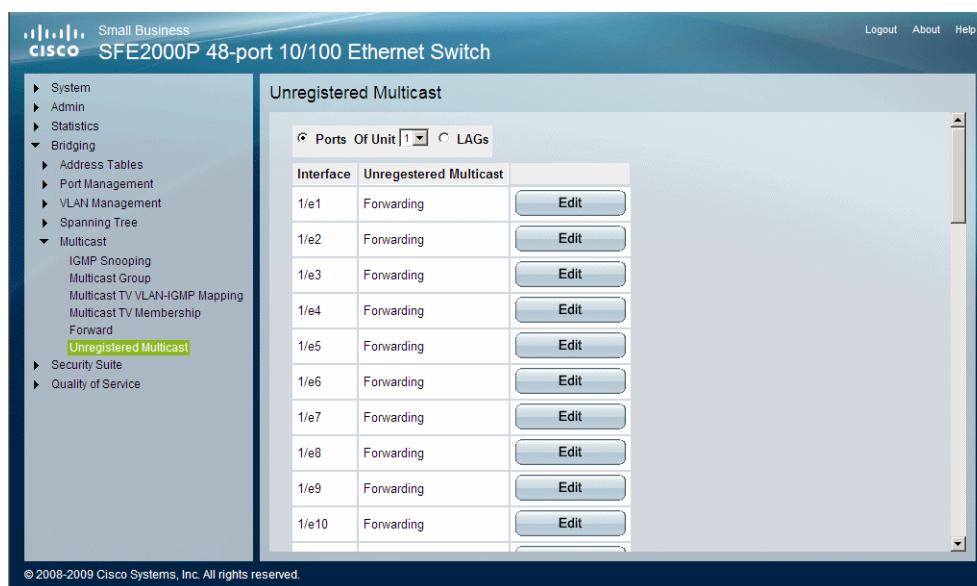
Multicast frames are generally forwarded to all ports in the VLAN. If IGMP Snooping is enabled, the device learns about the existence of Multicast groups and monitors which ports have joined what Multicast group. Multicast groups can also be statically enabled. This enables the device to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

The *Unregistered Multicast Page* contains fields to handle Multicast frames that belong to Unregistered Multicast groups. Unregistered Multicast groups are the groups that are not known to the device. All Unregistered Multicast frames are still forwarded to all ports on the VLAN. After a port has been set to Forwarding/Filtering, then this port's configuration is valid for any VLAN it is a member of (or will be a member of).

To define unregistered Multicast settings:

- STEP 1** Click **Bridging > Multicast > Unregistered Multicast**. The *Unregistered Multicast Page* opens:

Unregistered Multicast Page



The *Unregistered Multicast Page* contains the following fields:

- **Ports** — Indicates the port for which the unregistered Multicast parameters are displayed.
- **EtherChannels** — Specifies the EtherChannel for which the Unregistered Multicast settings are displayed.
- **Interface** — Displays the interface ID.
- **Unregistered Multicast** — Indicates the forwarding status of the selected interface. The possible values are:
 - *Forwarding* — Enables forwarding of Unregistered Multicast frames to the selected VLAN interface. This is the default setting.

- *Filtering* — Enables filtering of Unregistered Multicast frames to the selected VLAN interface.

STEP 2 Click **Edit**. The *Edit Unregistered Multicast Page* opens:

STEP 3 Define the *Unregistered Multicast* field.

STEP 4 Click **Apply**. The settings are saved and the device is updated.

Configuring Spanning Tree

The *Spanning Tree Protocol* (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following Spanning Tree versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops.
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
- **Multiple STP** — Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge.

Defining Spanning Tree

The Spanning Tree section contains the following topics:

- Defining STP Properties
- Defining Spanning Tree Interface Settings
- Defining Rapid Spanning Tree

Defining STP Properties

The *STP Properties Page* contains parameters for enabling STP on the device. The *STP Properties Page* is divided into three areas, Global Settings, Bridge Settings, and Designated Root.

STEP 1 Click **Bridging > Spanning Tree > Properties**. The *STP Properties Page* opens:

STP Properties Page

The screenshot shows the Cisco Small Business SGE2000P web interface. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging (expanded), Address Tables, Port Management, VLAN Management, Spanning Tree (expanded), Properties (highlighted), Interface Settings, RSTP, MSTP, Multicast, Security Suite, and Quality of Service. The main content area is titled 'Properties' and contains two sections: 'Global Settings' and 'Bridge Settings'.

Global Settings

- Spanning Tree State:
- STP Operation Mode:
- BPDU Handling:
- Path Cost Default Values:

Bridge Settings

- Priority:
- ☒ Hello Time: (Sec)
- ☐ Max Age: (Sec)
- ☐ Forward Delay: (Sec)

Designated Root

- Bridge ID: 32768-00:15:12:35:ac:88
- Root Bridge ID: 234-00:1a:e3:35:38:40
- Root Port: 2/g10

© 2009 Cisco Systems, Inc. All rights reserved.

The *STP Properties Page* contains the following fields:

Global Settings

The Global Settings area contains device-level parameters.

- **Spanning Tree State** — Indicates if STP is enabled on the device. The possible field values are:
 - *Enable* — Enables STP on the device. This is the default value.
 - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Indicates the STP mode that is enabled on the device. The possible field values are:
 - *Classic STP* — Enables Classic STP on the device. This is the default value.
 - *Rapid STP* — Enables Rapid STP on the device.
 - *Multiple STP* — Enables Multiple STP on the device.

- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
 - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface.
 - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
- **Path Cost Default Values** — Specifies the method used to assign default path costs to STP ports. The possible field values are:
 - *Short* — Specifies 1 through 65,535 range for port path costs.
 - *Long* — Specifies 1 through 200,000,000 range for port path costs. The default path costs assigned to an interface varies according to the selected method. This is the default value.

The Bridge Settings area contains the following fields:

- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc. The range is 0 to 61440.
- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.
- **Max Age** — Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds that the device can wait without receiving a configuration message, before attempting to redefine its own configuration. The default max age is 20 seconds. The range is 6 to 40 seconds.
- **Forward Delay** — Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a learning state before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.

The Designated Root area contains the following fields:

- **Bridge ID** — Identifies the Bridge Priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.

- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root.
- **Root Path Cost** — The cost of the path from this bridge to the root.
- **Topology Changes Counts** — Indicates the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format, for example, 2 days 5 hours 10 minutes and 4 seconds.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. STP is enabled, and the device is updated.

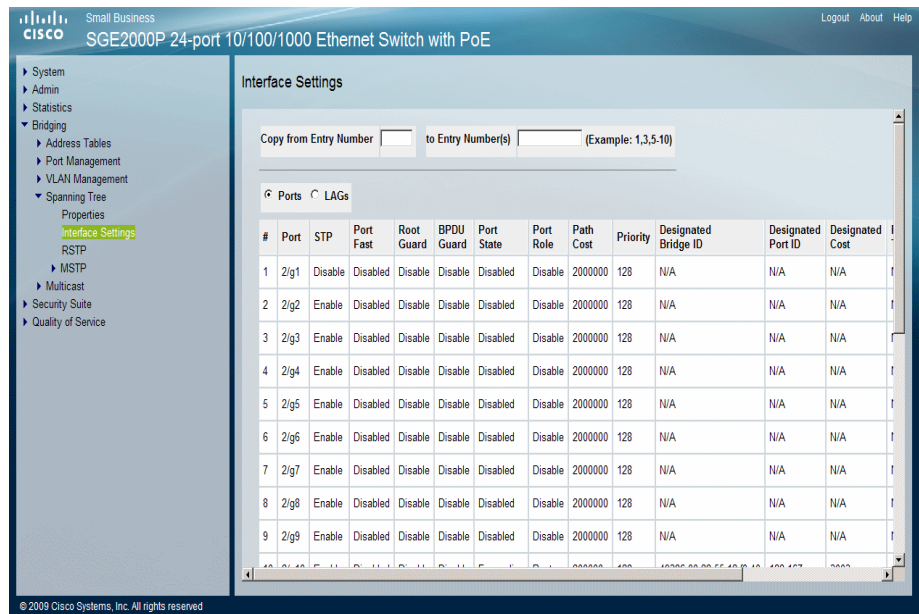
Defining Spanning Tree Interface Settings

Network administrators can assign STP settings to specific interfaces in the *STP Interface Settings Page*.

To assign STP settings to an interface:

STEP 1 Click **Bridging > Spanning Tree > Interface Settings**. The STP *Interface Settings Page* opens:

Interface Settings Page



The STP *Interface Settings Page* contains the following fields:

- **Copy From Entry Number** — Indicates the port from which the STP interface setting are copied.
- **To Entry Numbers** — Indicates the port to which the STP interface setting are copied.
- **Ports** — Display the STP Interface settings of the specified stacking member's ports.
- **LAGs** — Display the STP Interface settings of device LAGs.
- **Port** — Indicates the port or LAG on which STP is enabled.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
 - *Enable* — Indicates that STP is enabled on the port.
 - *Disable* — Indicates that STP is disabled on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol

convergence. STP convergence can take 30-60 seconds in large networks. The possible values are:

- *Enabled* — Port Fast is enabled.
 - *Disabled* — Port Fast is disabled.
 - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root. Root Guard may be enabled or disabled.
- **BPDU Guard** — Indicates if BPDU Guard is enabled on the interface. BPDU Guard protects the network from invalid configurations. It is usually used either when fast link ports (ports connected to clients) are enabled or when STP is disabled. If a BPDU message is received, the port shuts down and the device generates an appropriate SNMP trap. The possible field values are:
 - *Enable* — Enables BPDU guard on the selected port or LAG.
 - *Disable* — Disables BPDU guard on the selected port or LAG. This is the default value.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to the root switch.

- *Designated* — The port or LAG through which the designated switch is attached to the LAN.
- *Alternate* — Provides an alternate path to the root switch from the root interface.
- *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
- *Disabled* — The port is not participating in the Spanning Tree.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority range is between 0-240. The priority value is provided in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port's priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Indicates the number of times the port has changed from the **Blocking** state to **Forwarding** state.
- **LAG** — Indicates the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. STP is enabled on the interface, and the device is updated.

Modifying Interface Settings

STEP 1 Click **Bridging > Spanning Tree > Interface Settings**. The *Interface Settings Page* opens:

STEP 2 Click the **Edit** button. The *Edit Interface Settings Page* opens:

Edit Interface Settings Page

| | |
|----------------------|--------------------------|
| Port | 2/g1 |
| STP | Disable |
| Port Fast | Disabled |
| Enable Root Guard | <input type="checkbox"/> |
| Enable BPDU Guard | <input type="checkbox"/> |
| Port State | Disabled |
| Speed | 1000M |
| Path Cost | 2000000 |
| Default Path Cost | <input type="checkbox"/> |
| Priority | 128 |
| Designated Bridge ID | N/A |
| Designated Port ID | N/A |
| Designated Cost | N/A |
| Forward Transitions | N/A |
| LAG | |

Apply

The *Edit Interface Settings Page* contains the following fields:

- **Port** — Selects the port number on which Spanning Tree is configured.
- **STP** — Enables or disables STP on the port. The possible field values are:
 - *Enable* — Enables STP on the port.
 - *Disable* — Disables STP on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. The possible values are:
 - *Enabled* — Enables Port Fast on the port.
 - *Disabled* — Disables Port Fast on the port.

- *Auto* — Enables Port Fast mode a few seconds after the interface becomes active.
- **Enable Root Guard** — Enable the prevention of a devices outside the network core from being assigned the spanning tree root. The possible field values are:
 - *Checked* — Enables Root Guard on the selected port or LAG.
 - *Unchecked* — Disables Root Guard on the selected port or LAG. This is the default value.
- **Enable BPDU Guard** — Protects the network from invalid configurations. The possible field values are:
 - *Checked* — Enables BPDU Guard on the selected port or LAG.
 - *Unchecked* — Disables BPDU Guard on the selected port or LAG. This is the default value.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Speed** — Indicates the speed at which the port is operating.
- **Path Cost** — Defines the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Default Path Cost** — Defines the default path cost as the Path Cost field setting. The possible field values are:
 - *Checked* — Path Cost is the default value.
 - *Unchecked* — Path Cost is user-defined.

- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is provided in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port's priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Indicates the number of times the port has changed from the **Blocking** state to **Forwarding** state.
- **LAG** — Indicates the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The interface settings are modified, and the device is updated.

Defining Rapid Spanning Tree

While the classic spanning tree prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops, and propagating status topology changes. *Rapid Spanning Tree Protocol* (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

STEP 1 Click **Bridging > Spanning Tree > RSTP**. The *RSTP Page* opens:

RSTP Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Address Tables
Port Management
VLAN Management
Spanning Tree
Properties
Interface Settings
RSTP
MSTP
Multicast
Security Suite
Quality of Service

RSTP

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

Ports LAGs

| # | Interface | Port Role | Mode | Fast Link Operational Status | Port Status | Point-to-Point Operational Status | Activate Protocol Migration | |
|----|-----------|-----------|------|------------------------------|-------------|-----------------------------------|-----------------------------|------|
| 1 | 2/g1 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 2 | 2/g2 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 3 | 2/g3 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 4 | 2/g4 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 5 | 2/g5 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 6 | 2/g6 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 7 | 2/g7 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 8 | 2/g8 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 9 | 2/g9 | Disable | STP | Disable | Disabled | Enable | Activate | Edit |
| 10 | 2/g10 | Root | STP | Disable | Forwarding | Enable | Activate | Edit |

© 2009 Cisco Systems, Inc. All rights reserved

The *RSTP Page* contains the following fields:

- **Copy From Entry Number** — Indicate the port from which the STP interface setting are copied.
- **To Entry Numbers** — Indicate the port to which the STP interface setting are copied.
- **Ports** — Display the RSTP configurations of the specified stacking member's ports.
- **LAGs** — Display the RSTP configurations of device LAGs.
- **Interface** — Indicates the port or LAG for which the STP settings are displayed.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root switch.
 - *Designated* — Indicates that the port or LAG via which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.

- *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disable* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
 - *STP* — Indicates that Classic STP is enabled on the port.
 - *Rapid STP* — Indicates that Rapid STP is enabled on the port.
- **Fast Link** — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state. The possible field values are:
 - *Enable* — Fast Link is enabled.
 - *Disable* — Fast Link is disabled.
 - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port Status** — Indicates the RSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Point-to-Point Operational Status** — Indicates the Point-to-Point operating state. The possible values are:
 - *Enable* — Enables Point-to-Point on the interface.
 - *Disable* — Disables Point-to-Point on the interface.

- **Activate Protocol Migration** — Click the *Activate* button to run a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The Rapid Spanning Tree Settings are defined, and the device is updated.

Modifying RTSP

STEP 1 Click **Bridging > Spanning Tree > RSTP**. The *RSTP Page* opens:

STEP 2 Click the **Edit** button. The *Edit Rapid Spanning Tree Page* opens:

Edit Rapid Spanning Tree Page

| Edit Rapid Spanning Tree | |
|--------------------------------------|--|
| Interface | <input checked="" type="radio"/> Port 2/g1 <input type="radio"/> LAG 1 |
| Role | Disable |
| Mode | STP |
| Fast Link Operational Status | Disable |
| Port State | Disabled |
| Point to Point Admin Status | Auto |
| Point to Point Operational Status | Enable |
| Activate Protocol Migration Test | <input type="checkbox"/> |
| <input type="button" value="Apply"/> | |

The *Edit Rapid Spanning Tree Page* contains the following fields:

- **Interface** — Specifies whether Rapid STP is enabled on a port or LAG.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root switch.
 - *Designated* — Indicates that the port or LAG via which the designated switch is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root switch from the root interface.

- *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disable* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
 - *STP* — Indicates that Classic STP is enabled on the port.
 - *Rapid STP* — Indicates that Rapid STP is enabled on the port.
- **Fast Link Operational Status** — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
 - *Enable* — Fast Link is enabled.
 - *Disable* — Fast Link is disabled.
 - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port State** — Indicates the RSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established on the port. Ports defined as Full Duplex are considered Point-to-Point port links. The possible field values are:
 - *Enable* — Device establishes point-to-point, full duplex links.
 - *Disable* — Device establishes shared, half duplex links.

- *Auto* — Device automatically determines the state.
- **Point-to-Point Operational Status** — Indicates the Point-to-Point operating state.
- **Activate Protocol Migration Test** — Enables a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface. The possible field values are:
 - *Checked* — Enable Protocol Migration.
 - *Unchecked* — Disable Protocol Migration.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Defining Multiple Spanning Tree

MSTP provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port is placed in the Forwarding State in another STP instance. The *MSTP Properties* page contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

The MSTP section contains the following :

- Defining MSTP Properties
- Defining MSTP Instance to VLAN
- Defining MSTP Instance Settings
- Defining MSTP Interface Settings

Defining MSTP Properties

The *MSTP Properties Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

To define MSTP:

- STEP 1** Click **Bridging > Spanning Tree > MSTP > Properties**. The *MSTP Properties Page* opens:

MSTP Properties Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE configuration page. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging, Address Tables, Port Management, VLAN Management, Spanning Tree, Properties, Interface Settings, RSTP, MSTP, Properties, Instance To VLAN, Instance Settings, Interface Settings, Multicast, Security Suite, and Quality of Service. The 'MSTP' item is expanded, and the 'Properties' item is selected. The main area displays the 'Properties' form with the following fields: Region Name (00:15:12:35:ac:88), Revision (0), Max Hops (20), and IST Master (32768-00:15:12:35:ac:88). An 'Apply' button is located at the bottom of the form.

The *MSTP Properties Page* contains the following fields:

- **Region Name** — Provides a user-defined STP region name.
- **Revision** — Defines unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration. The possible field range 0-65535.
- **Max Hops** — Indicates the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.
- **IST Master** — Identifies the region's master.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The MSTP properties are defined, and the device is updated.

Defining MSTP Instance to VLAN

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

The VLAN screen enables mapping VLANs to MSTP Instances.

- STEP 1** Click **Bridging > Spanning Tree > MSTP > Instance to VLAN**. The *Instance to VLAN Page* opens:

Instance to VLAN Page

| VLAN | Instance ID (0-15) | VLAN | Instance ID (0-15) | VLAN | Instance ID (0-15) | VLAN | Instance ID (0-15) |
|---------|--------------------|---------|--------------------|---------|--------------------|---------|--------------------|
| VLAN 1 | 0 | VLAN 17 | 0 | VLAN 33 | 0 | VLAN 49 | 0 |
| VLAN 2 | 0 | VLAN 18 | 0 | VLAN 34 | 0 | VLAN 50 | 0 |
| VLAN 3 | 0 | VLAN 19 | 0 | VLAN 35 | 0 | VLAN 51 | 0 |
| VLAN 4 | 0 | VLAN 20 | 0 | VLAN 36 | 0 | VLAN 52 | 0 |
| VLAN 5 | 0 | VLAN 21 | 0 | VLAN 37 | 0 | VLAN 53 | 0 |
| VLAN 6 | 0 | VLAN 22 | 0 | VLAN 38 | 0 | VLAN 54 | 0 |
| VLAN 7 | 0 | VLAN 23 | 0 | VLAN 39 | 0 | VLAN 55 | 0 |
| VLAN 8 | 0 | VLAN 24 | 0 | VLAN 40 | 0 | VLAN 56 | 0 |
| VLAN 9 | 0 | VLAN 25 | 0 | VLAN 41 | 0 | VLAN 57 | 0 |
| VLAN 10 | 0 | VLAN 26 | 0 | VLAN 42 | 0 | VLAN 58 | 0 |
| VLAN 11 | 0 | VLAN 27 | 0 | VLAN 43 | 0 | VLAN 59 | 0 |
| VLAN 12 | 0 | VLAN 28 | 0 | VLAN 44 | 0 | VLAN 60 | 0 |
| VLAN 13 | 0 | VLAN 29 | 0 | VLAN 45 | 0 | VLAN 61 | 0 |
| VLAN 14 | 0 | VLAN 30 | 0 | VLAN 46 | 0 | VLAN 62 | 0 |
| VLAN 15 | 0 | VLAN 31 | 0 | VLAN 47 | 0 | VLAN 63 | 0 |

The *Instance to VLAN Page* contains the following fields:

- **VLAN** — Indicates the VLAN for which the MSTP instance ID is defined.
- **Instance ID (0-15)** — Indicates the MSTP instance ID assigned to the VLAN. The possible field range is 0-15.

- STEP 2** Map the VLANs to Instance IDs.

- STEP 3** Click **Apply**. The MSTP VLAN mapping is defined, and the device is updated.

Defining MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

Network Administrators can define MSTP Instances settings using the *MSTP Instance Settings Page*.

STEP 1 Click **Bridging > Spanning Tree > MSTP > Instance Settings**. The *MSTP Instance Settings Page* opens:

MSTP Instance Settings Page

Small Business
SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
 Address Tables
 Port Management
 VLAN Management
 Spanning Tree
 Properties
 Interface Settings
 RSTP
 MSTP
 Properties
 Instance To VLAN
 Instance Settings
 Interface Settings
 Multicast
 Security Suite
 Quality of Service

Instance Settings

Instance ID: 1

Included VLAN:

Bridge Priority: 32768

Designated Root Bridge ID: 32768-00:15:12:35:ac:08

Root Port: 0

Root Path Cost: 0

Bridge ID: 32768-00:15:12:35:ac:08

Remaining Hops: 20

Apply

© 2009 Cisco Systems, Inc. All rights reserved.

The *MSTP Instance Settings Page* contains the following fields:

- **Instance ID** — Defines the VLAN group to which the interface is assigned.
- **Included VLAN** — Maps the selected VLAN to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440.

- **Designated Root Bridge ID** — Indicates the priority and MAC address of the bridge with the lowest path cost to the instance ID.
- **Root Port** — Indicates the selected instance's root port.
- **Root Path Cost** — Indicates the selected instance's path cost.
- **Bridge ID** — Indicates the priority and MAC address of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The MSTP Instance configuration is defined, and the device is updated.

Defining MSTP Interface Settings

Network Administrators can define MSTP Instances settings using the *MSTP Interface Settings Page*.

- STEP 1** Click **Bridging > Spanning Tree > MSTP > Interface Settings**. The *MSTP Interface Settings Page* opens:

MSTP Interface Settings Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE web interface. The left sidebar contains a navigation tree with the following items: System, Admin, Statistics, Bridging (expanded), Address Tables, Port Management, VLAN Management, Spanning Tree (expanded), Properties, Interface Settings, RSTP, MSTP (expanded), Properties, Instance To VLAN, Interface Settings (highlighted), Multicast, Security Suite, and Quality of Service. The main content area is titled 'Interface Settings' and contains the following fields: Instance ID (dropdown menu), Interface (radio buttons for Port and LAG, with Port selected and 2/p1 in a dropdown), Port State (N/A), Type (N/A), Role (N/A), Mode (N/A), Interface Priority (text box with 128), Path Cost (text box with 2000000 and a Use Default checkbox), Designated Bridge ID (N/A), Designated Port ID (N/A), Designated Cost (N/A), Forward Transitions (N/A), and Remain Hops (N/A). At the bottom are 'Apply' and 'Interface Table' buttons. The footer of the interface reads '© 2009 Cisco Systems, Inc. All rights reserved'.

The *MSTP Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-15.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
 - *Port* — Specifies the port for which the MSTP settings are displayed.
 - *LAG* — Specifies the LAG for which the MSTP settings are displayed.
- **Port State** — Indicates the MSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.

- *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Type** — Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
 - *Boundary Port* — Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
 - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
 - *Internal* — Indicates the port is an internal port.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root device.
 - *Designated* — Indicates the port or LAG via which the designated device is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root device from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
 - *Classic STP* — Indicates that Classic STP is enabled on the port.
 - *Rapid STP* — Indicates that Rapid STP is enabled on the port.
 - *MSTP* — Indicates that MSTP is enabled on the port.
- **Interface Priority** — Defines the interface priority for specified instance. The default value is 128.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range is 1-200,000,000.

- **Designated Bridge ID** — Indicates the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Forward Transitions** — Indicates the number of times the port has changed from Forwarding state to Blocking state.
- **Remain Hops** — Indicates the hops remaining to the next destination.

STEP 2 Click the **Interface Table** button. The *MSTP Interface Table Page* opens:

MSTP Interface Table Page

| Interface Table | | | | | | | | | | |
|--|------|------|------|---------------|-----------|------------|-----------------|----------------------|--------------------|-------------|
| Instance 1 <input checked="" type="radio"/> Ports <input type="radio"/> LAGs | | | | | | | | | | |
| Interface | Role | Mode | Type | Port Priority | Path Cost | Port State | Designated Cost | Designated Bridge ID | Designated Port ID | Remain Hops |
| 2/g1 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g2 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g3 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g4 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g5 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g6 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g7 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g8 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g9 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g10 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g11 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g13 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| 2/g14 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |

The *MSTP Interface Table Page* contains the following fields:

- **Instance** — Defines the VLAN group to which the interface is assigned.
- **Interface** — Indicates the port or LAG for which the MSTP settings are displayed.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root device.

- *Designated* — Indicates the port or LAG via which the designated device is attached to the LAN.
- *Alternate* — Provides an alternate path to the root device from the root interface.
- *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
- *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
 - *Classic STP* — Indicates that Classic STP is enabled on the device.
 - *Rapid STP* — Indicates that Rapid STP is enabled on the device.
- **Type** — Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
 - *Boundary Port* — Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
 - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
 - *Internal* — Indicates the port is an internal port.
- **Port Priority** — Defines the interface priority for specified instance. The default value is 128.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Port State** — Indicates the MSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.

- *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
- *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
- *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Designated Bridge ID** — Indicates the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Remain Hops** — Indicates the hops remaining to the next destination.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Configuring Quality of Service

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, *Quality of Service* (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
 - The ingress interface
 - Packet content
 - A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
 - The assignment of network traffic to a particular hardware queue
 - The assignment of internal resources
 - Traffic shaping

The terms *Class of Service* (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

The QoS facility involves the following elements:

- **Access Control Lists (ACLs)** — Used to decide which traffic is allowed to enter the system, and which is to be dropped. Only traffic that meets this criteria are subject to CoS or QoS settings. ACLs are used in QoS and network security.

- **Traffic Classification** — Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.
- **Assignment to Hardware Queues** — Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong, as defined by the classification mechanism.
- **Traffic Class-Handling Attributes** — Applies QoS/CoS mechanisms to different classes, including: Bandwidth Management

The Quality of Service section contains the following topics:

- Defining General Settings
- Defining QoS Basic Mode

Defining General Settings

The QoS General Settings section contains the following :

- Defining CoS
- Defining QoS Queue
- Mapping CoS to Queue
- Mapping DSCP to Queue
- Configuring Bandwidth

Defining CoS

The *CoS Page* contains fields for enabling or disabling CoS (Basic or Advanced mode). In addition, the default CoS for each port or LAG is definable.

STEP 1 Click **Quality of Service > General > CoS**. The *CoS Page* opens:

CoS Page



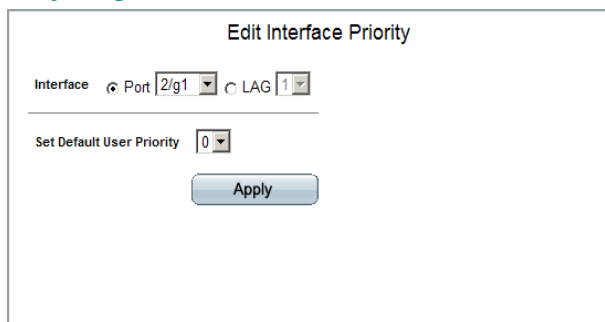
The *CoS Page* contains the following fields:

- **QoS Mode** — Indicates if QoS is enabled on the device. The possible values are:
 - *Advanced* — Enables Advanced mode QoS on the device.
- **Ports** — Indicates that the CoS configuration of the ports on the specified stacking member are described in the page.
- **LAGs** — Indicates that the CoS configuration of the LAGs are described in the page.
- **Interface** — Indicates the interface for which the CoS information is displayed.
- **Default CoS** — Displays the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.
- **Restore Defaults** — Restores the factory CoS default settings to the selected port.
 - *Checked* — Restores the factory QoS default settings to ports after clicking the Apply button.
 - *Unchecked* — Maintains the current QoS settings.

Modifying Interface Priorities

STEP 2 Click the **Edit** button. The *Edit Interface Priority Page* opens:

Edit Interface Priority Page



The *Edit Interface Priority Page* contains the following fields:

- **Interface** — Indicates whether the interface is a port or LAG.
- **Set Default User Priority**— Defines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.

STEP 3 Modify the Interface priority.

STEP 4 Click **Apply**. The Interface priority is set, and the device is updated.

Defining QoS Queue

The *Queue Page* contains fields for defining the QoS queue forwarding types.

STEP 1 Click **Quality of Service > General > Queue**. The *Queue Page* opens:

Queue Page

| Queue | Scheduling | | | % of WRR Bandwidth |
|-------|----------------------------------|-----------------------|------------|--------------------|
| | Strict Priority | WRR | WRR Weight | |
| 1 | <input checked="" type="radio"/> | <input type="radio"/> | 1 | |
| 2 | <input checked="" type="radio"/> | <input type="radio"/> | 2 | |
| 3 | <input checked="" type="radio"/> | <input type="radio"/> | 4 | |
| 4 | <input checked="" type="radio"/> | <input type="radio"/> | 8 | |

Apply

The *Queue Page* contains the following fields:

- **Queue** — Displays the queue for which the queue settings are displayed. The possible field range is 1 - 4.
- **WRR Weight** — Displays the WRR weight assigned to the queue by the user.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the queue. These values represent the % of the WRR Weight configured by the user.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the queue. These values represent the % of the WRR Weight configured by the user.

STEP 2 Define the queues.

STEP 3 Click **Apply**. The queues are defined, and the device is updated.

Mapping CoS to Queue

The *Cos to Queue Page* contains fields for classifying CoS settings to traffic queues.

STEP 1 Click **Quality of Service > General > CoS to Queue**. The *Cos to Queue Page* opens:

Cos to Queue Page

| Class of Service | Queue |
|------------------|-------|
| 0 | 2 |
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 3 |
| 5 | 3 |
| 6 | 4 |
| 7 | 4 |

The *Cos to Queue Page* contains the following fields:

- **Restore Defaults** — Restores all queues to the default CoS settings.
- **Class of Service** — Specifies the CoS VLAN (CoS) priority tag values, where zero is the lowest and 7 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported, where Queue 4 is the highest and Queue 1 is the lowest.

STEP 2 Define the relevant mapping.

STEP 3 Click **Apply**. CoS to queues are mapped, and the device is updated.

Mapping DSCP to Queue

The *DSCP to Queue Page* enables mapping DSCP values to specific queues.

To map DSCP to Queues:

- STEP 1** Click **Quality of Service > General > DSCP to Queue**. The *DSCP to Queue Page* opens:

DSCP to Queue Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE management interface. The left sidebar shows the navigation menu with 'DSCP to Queue' highlighted under 'Quality of Service > General'. The main content area is titled 'DSCP to Queue' and contains a table for mapping DSCP values to queues.

| DSCP In | Queue | DSCP In | Queue | DSCP In | Queue |
|---------|-------|---------|-------|---------|-------|
| 0 | 1 | 25 | 2 | 50 | 4 |
| 1 | 1 | 26 | 2 | 51 | 4 |
| 2 | 1 | 27 | 2 | 52 | 4 |
| 3 | 1 | 28 | 2 | 53 | 4 |
| 4 | 1 | 29 | 2 | 54 | 4 |
| 5 | 1 | 30 | 2 | 55 | 4 |
| 6 | 1 | 31 | 2 | 56 | 4 |
| 7 | 1 | 32 | 3 | 57 | 4 |
| 8 | 1 | 33 | 3 | 58 | 4 |
| 9 | 1 | 34 | 3 | 59 | 4 |
| 10 | 1 | 35 | 3 | 60 | 4 |
| 11 | 1 | 36 | 3 | 61 | 4 |
| 12 | 1 | 37 | 3 | 62 | 4 |
| 13 | 1 | 38 | 3 | 63 | 4 |
| 14 | 1 | 39 | 3 | | |
| 15 | 1 | 40 | 3 | | |
| 16 | 2 | 41 | 3 | | |

The *DSCP to Queue Page* contains the following fields:

- **DSCP In** — Indicates the *Differentiated Services Code Point* (DSCP) value in the incoming packet. The following values are reserved and cannot be changed: **3, 11, 19, 27, 35, 43, 51, and 59**.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The device is updated.

Configuring Bandwidth

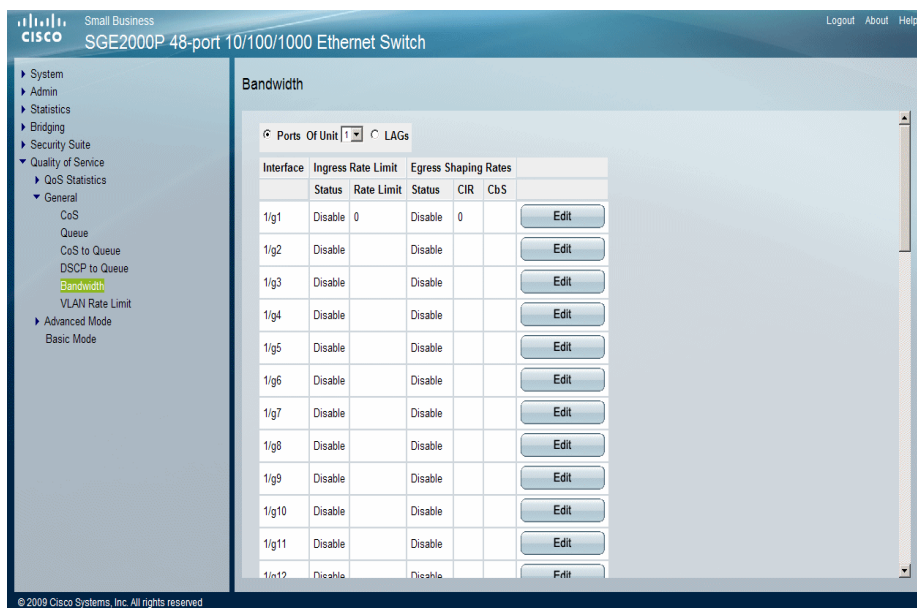
The *Bandwidth Page* allows network managers to define the bandwidth settings for specified egress and ingress interfaces.

Rate Limits and Shaping are defined per interface:

- Rate Limit sets the maximum bandwidth allowed on ingress interfaces.
- Shaping Rate sets the maximum bandwidth allowed on egress interfaces. On GE ports, traffic shape for burst traffic (CbS) can also be defined.

STEP 1 Click **Quality of Service > General > Bandwidth**. The *Bandwidth Page* opens:

Bandwidth Page



The *Bandwidth Page* contains the following fields:

- **Ports of Unit** — Indicates that the bandwidth settings of the ports on the specified stacking member are described in the page.
- **LAG** — Indicates that the bandwidth settings of the LAGs are described in the page.
- **Ingress Rate Limit** — Indicates the traffic limit for ingress interfaces. The possible field values are:
 - *Status* — Enables or disables rate limiting for ingress interfaces. *Disable* is the default value.

- **Rate Limit** — Defines the rate limit for ingress ports. Defines the amount of bandwidth assigned to the interface.
For FE ports, the rate is 62 - 100,000 Kbps.
For GE ports, the rate is 62 - 1,000,000 Kbps.
- **Egress Shaping Rates** — Indicates the traffic shaping type, if enabled, for egress ports. The possible field values are:
 - **CIR** — Defines *Committed Information Rate* (CIR) as the queue shaping type. The possible field values are:
For FE ports, the rate is 64 - 62,500 Kbps.
For GE ports, the rate is 64 - 1,000,000 Kbps.
 - **CbS** — Defines *Committed Burst Size* (CbS) as the queue shaping type. CbS is supported only on GE interfaces. The possible field value is 4096 - 16,769,020 bytes.

Modifying Bandwidth Settings

STEP 2 Click the **Edit** button. The *Edit Bandwidth Page* opens:

Edit Bandwidth Page

The ***Edit Bandwidth Page*** contains the following fields:

- **Interface** — Indicates whether the interface, for which bandwidth settings are edited, is a port or a LAG.
- **Enable Egress Shaping Rate** — Indicates if shaping is enabled on the interface. The possible field values are:
 - *Checked* — Enables egress shaping on the interface.
 - *Unchecked* — Disables egress shaping on the interface.

- **Committed Information Rate (CIR)** — Defines CIR as the queue shaping type. The possible field values are:
 - For FE ports, the rate is 64 - 62,500 Kbps.
 - For GE ports, the rate is 64 - 1,000,000 Kbps.
- **Committed Burst Size (CS)** — Defines CbS as the queue shaping type. CS is supported only on GE interfaces. The possible field value is 4096 - 16,769,020 bytes.
- **Ingress Rate Limit** — Indicates if rate limiting is defined on the interface. The possible field values are:
 - *Checked* — Enables ingress rate limiting on the interface.
 - *Unchecked* — Disables ingress rate limiting on the interface.
- **Ingress Rate Limit** — Defines the amount of bandwidth assigned to the interface.
For FE ports, the rate is 62 - 100,000 Kbps.
For GE ports, the rate is 62 - 1,000,000 Kbps.

STEP 3 Modify the relevant fields.

STEP 4 Click **Apply**. The bandwidth settings are modified, and the device is updated.

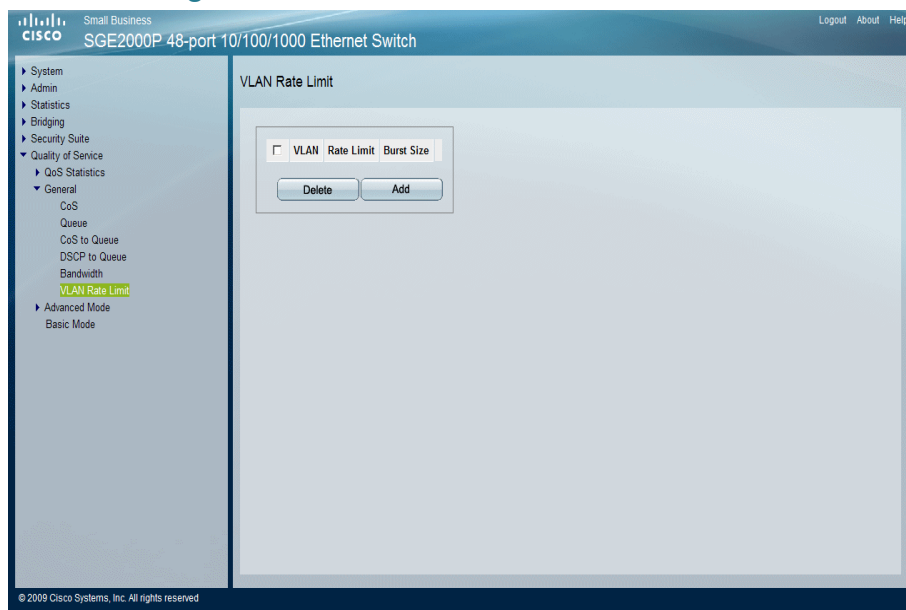
Configuring VLAN Rate Limit

Rate limiting per VLAN allows network administrators to limit traffic on VLANs. Rate limiting is calculated separately for each unit in a stack, and for each packet processor in a unit. QoS rate limiting has priority over VLAN rate limiting. For example, if a packet is subject to QoS rate limits but is also subject to VLAN rate limiting, and the rate limits conflict, the QoS rate limits take precedence.

To define the VLAN Rate Limit:

- STEP 1** Click **Quality of Service > General > VLAN Rate Limit**. The *VLAN Rate Limit Page* opens:

VLAN Rate Limit Page

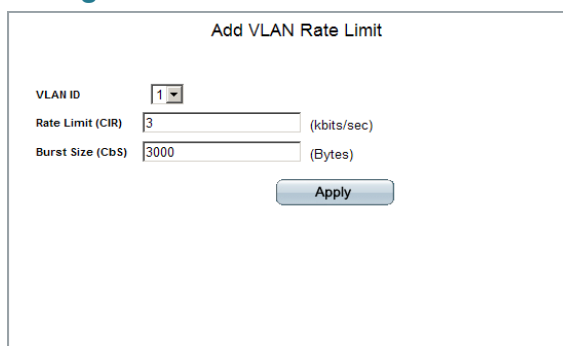


The *VLAN Rate Limit Page* contains the following fields:

- **VLAN** – Indicates the VLAN on which the Rate Limit is applied.
- **Rate Limit** – Defines the maximum rate (CIR) in kbits per second (bps) that forwarding traffic is permitted in the VLAN.
- **Burst Size** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

- STEP 2** Click the **Add** button. The *Add VLAN Rate Limit Page* opens:

Add VLAN Rate Limit Page



The screenshot shows a web form titled "Add VLAN Rate Limit". It contains three input fields: "VLAN ID" with a dropdown menu showing "1", "Rate Limit (CIR)" with a text box containing "3" and the unit "(kbits/sec)", and "Burst Size (CbS)" with a text box containing "3000" and the unit "(Bytes)". An "Apply" button is located at the bottom right of the form.

The *Add VLAN Rate Limit Page* contains the following fields.

- **VLAN ID** – Defines the VLAN on which to apply the Rate Limit.
- **Rate Limit (CIR)** – Defines the maximum rate (CIR) in kbits per second (bps) that forwarding traffic is permitted in the VLAN.
- **Burst Size (CbS)** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

STEP 3 Define the relevant fields.

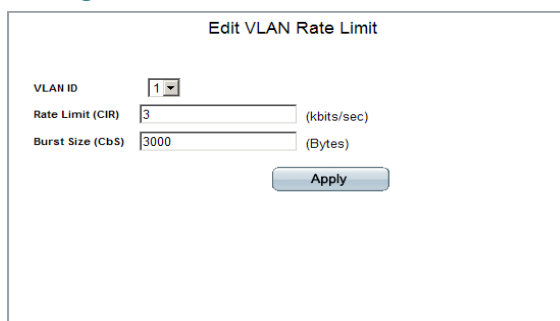
STEP 4 Click **Apply**. The VLAN Rate Limit is added, and the device is updated.

Modifying the VLAN Rate Limit

STEP 1 Click **Quality of Service > General > VLAN Rate Limit**. The *VLAN Rate Limit Page* opens:

STEP 2 Click the **Edit** button. The *VLAN Rate Limit Page* opens:

Edit VLAN Rate Limit Page



The screenshot shows a web interface titled "Edit VLAN Rate Limit". It contains three input fields: "VLAN ID" with a dropdown menu showing "1", "Rate Limit (CIR)" with a text box containing "3" and the unit "(kbits/sec)", and "Burst Size (CbS)" with a text box containing "3000" and the unit "(Bytes)". An "Apply" button is located at the bottom right of the form.

The ***VLAN Rate Limit Page*** contains the following fields:

- **VLAN ID** – Defines the VLAN on which to apply the Rate Limit.
- **Rate Limit (CIR)** – Defines the maximum rate (CIR) in kbits per second (bps) that forwarding traffic is permitted in the VLAN.
- **Burst Size (CbS)** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The VLAN Rate Limit is modified, and the device is updated. Defining Advanced Mode

Defining Advanced QoS Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management. The rules are defined in classification control lists (CCL).

CCLs are set according to the classification defined in the ACL, and they cannot be defined until a valid ACL is defined. When CCLs are defined, ACLs and CCLs can be grouped together in a more complex structure, called policies. Policies can be applied to an interface. Policy ACLs/CCLs are applied in the sequence they appear within the policy. Only a single policy can be attached to a port.

In advanced QoS mode, ACLs can be applied directly to an interface. However, a policy and ACL cannot be simultaneously applied to an interface.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or configuring output shaping for burst size, CIR, or CbS per interface or per queue, can be applied.

The *Advanced Mode* section contains the following topics:

- Configuring DSCP Mapping
- Defining Class Mapping
- Defining Aggregate Policer
- Configuring Policy Table
- Defining Policy Binding

Configuring DSCP Mapping

The *DSCP Mapping Page* enables mapping *Differentiated Services Code Point* (DSCP) values from incoming packets to DSCP values in outgoing packets. The DSCP values can be modified only within the queue range. This information is important when traffic exceeds user-defined limits.

To map DSCP values:

- STEP 1** Click **Quality of Service > Advanced Mode > DSCP Mapping**. The *DSCP Mapping Page* opens:

DSCP Mapping Page



| DSCP In | DSCP Out | DSCP In | DSCP Out | DSCP In | DSCP Out |
|---------|----------|---------|----------|---------|----------|
| 0 | | 25 | | 50 | |
| 1 | | 26 | | 51 | |
| 2 | | 27 | | 52 | |
| 3 | | 28 | | 53 | |
| 4 | | 29 | | 54 | |
| 5 | | 30 | | 55 | |
| 6 | | 31 | | 56 | |
| 7 | | 32 | | 57 | |
| 8 | | 33 | | 58 | |
| 9 | | 34 | | 59 | |
| 10 | | 35 | | 60 | |
| 11 | | 36 | | 61 | |
| 12 | | 37 | | 62 | |
| 13 | | 38 | | 63 | |
| 14 | | 39 | | | |

The *DSCP Mapping Page* contains the following fields:

- **DSCP In** — Indicates the DSCP value in the incoming packet which will be mapped to an outgoing packet.
- **DSCP Out** — Sets a mapped DSCP value in the outgoing packet for the corresponding incoming packet.

- STEP 2** Define the relevant mapping.

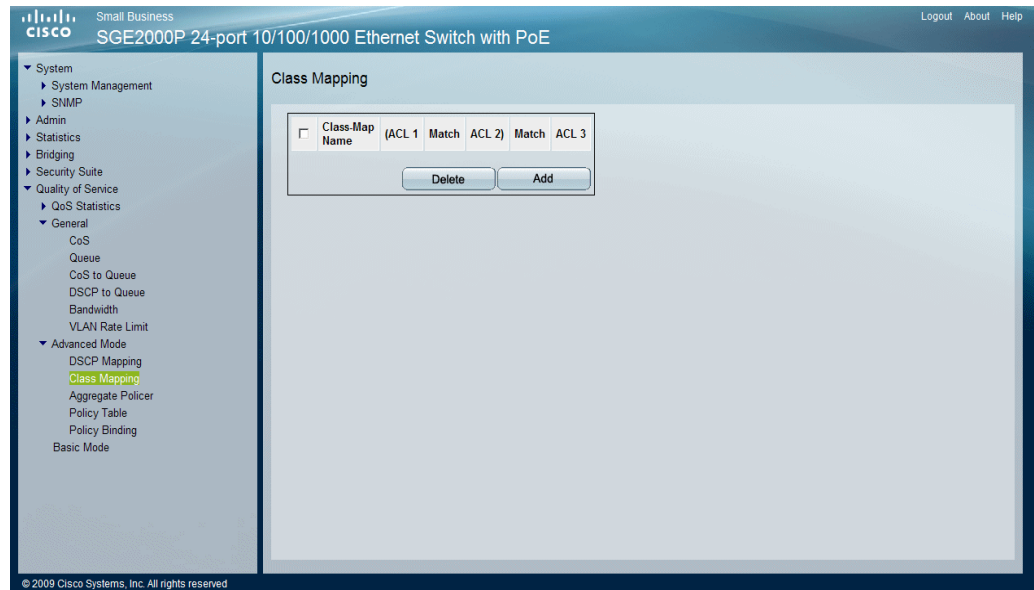
- STEP 3** Click **Apply**. DSCP incoming values are mapped to DSCP outgoing values, and the device is updated.

Defining Class Mapping

The *Class Mapping Page* contains parameters for defining class maps. One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned to packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

STEP 1 Click **Quality of Service > Advanced Mode > Class Mapping**. The *Class Mapping Page* opens:

Class Mapping Page



The *Class Mapping Page* contains the following fields:

- **Class Map Name** — Selects an existing Class Map by name.
- **ACL1** — Contains a list of the user-defined ACLs.
- **Match** — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
 - And — Both the MAC-based and the IP-based ACL must match a packet.
 - Or — Either the MAC-based or the IP-based ACL must match a packet.
- **ACL2** — Contains a list of the user-defined ACLs.

STEP 2 Click the **Add** button. The *Add QoS Class Map Page* opens:

Add QoS Class Map Page

The *Add QoS Class Map Page* contains the following fields.

- **Class Map Name** — Defines a new Class Map name
- **IP ACL** — Matches packets to IP based ACLs first, then matches packets to MAC based ACLs. Select either an IPv4 ACL or an IPv6 ACL.
- **Match** — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
 - *And* — Both the MAC-based and the IP-based ACL must match a packet.
 - *Or* — Either the MAC-based or the IP-based ACL must match a packet.
- **MAC ACL** — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.
- **Preferred ACL** — Defines if packets are first matched to an IP based ACL or a MAC based ACL. The possible field values are:
 - *IP Based ACLs* — Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.
 - *MAC Based ACLs* — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Defining Aggregate Policer

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To define Aggregate Policers:

- STEP 1** Click **Quality of Service > Advanced Mode > Aggregate Policer**. The *Aggregate Policer Page* opens:

Aggregate Policer Page

| Aggregate Policer Name | Ingress CIR | Ingress CBS | Exceed Action |
|--|-------------|-------------|---------------|
| <input type="button" value="Delete"/> <input type="button" value="Add"/> | | | |

The *Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name**— Specifies the Aggregate Policer Name

- **Ingress CIR** — Defines the *Committed Information Rate* (CIR) in bits per second.
- **Ingress CS** — Defines the *Committed Burst Size* (CS) in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
 - *None* — Forwards packets exceeding the defined CIR value.

STEP 2 Click the **Add** button. The *Add QoS Aggregate Policer Page* opens:

Add QoS Aggregate Policer Page

Add QoS Aggregate Policer

Aggregate Policer Name

Ingress Committed Information Rate (CIR) (Kbits per Second)

Ingress Committed Burst Size (CBS) (Bytes per Second)

Exceed Action

Apply

The *Add QoS Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name** — Specifies the Aggregate Policer Name.
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in bits per second.
- **Ingress Committed Burst Size (CS)** — Defines the CS in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.

STEP 3 Define the relevant fields.

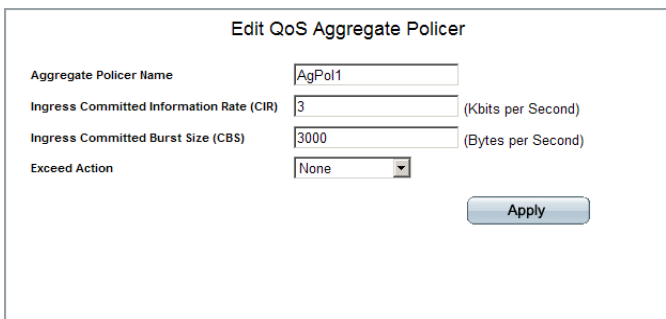
STEP 4 Click **Apply**. The Aggregate policer is added, and the device is updated.

Modifying QoS Aggregate Policer

STEP 1 Click **Quality of Service > Advanced Mode > Aggregate Policer**. The *Aggregate Policer Page* opens:

STEP 2 Click the **Edit** Button. The *Edit QoS Aggregate Policer Page* opens:

Edit QoS Aggregate Policer Page



The *Edit QoS Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name**— Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in bits per second.
- **Ingress Committed Burst Size (CS)** — Defines the CS in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

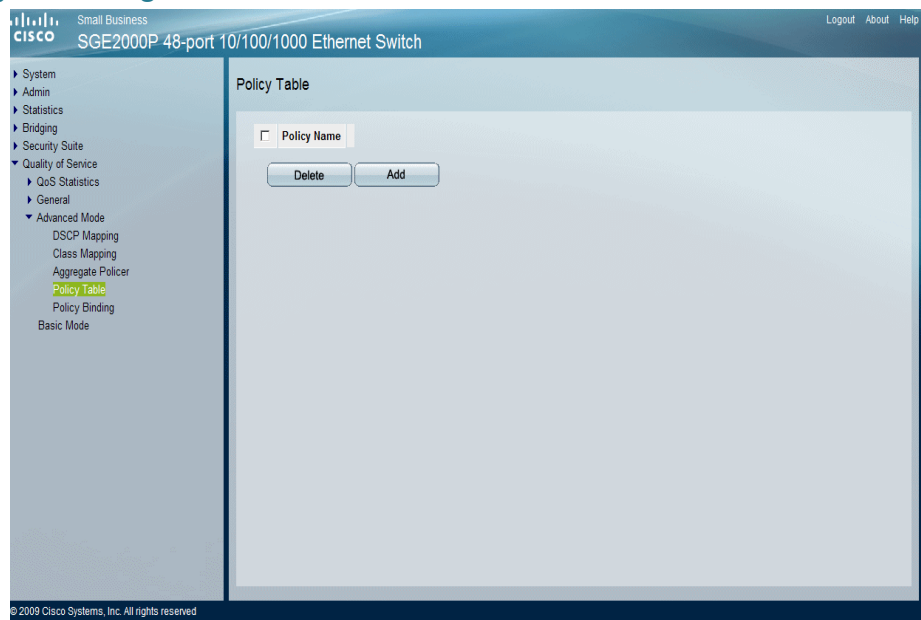
Configuring Policy Table

In the *Policy Table Page*, QoS policies are set up and assigned to interfaces.

To set up QoS policies:

- STEP 1** Click **Quality of Service > Advanced Mode > Policy Table**. The *Policy Table Page* opens:

Policy Table Page



The *Policy Table Page* contains the following field:

- **Policy Name** — Displays the user-defined policy name.

- STEP 2** Click the **Add** button. The *Add QoS Policy Profile Page* opens:

Add QoS Policy Profile Page

The *Add QoS Policy Profile Page* contains the following fields.

- **New Policy Name** — Displays the user-defined policy name.
- **Class Map** — Selects the user-defined class maps which can be associated with the policy.
- **Action** — Defines the action attached to the rule. The possible field value is:
 - **Set** — Defines the Trust configuration manually. The possible field values are:
 - *DSCP* — In the **New Value** box, the possible values are 0-63.
 - *CoS* — In the **New Value** box, the possible values are 0-7. This is applicable only for the GE device.
 - *Queue* — In the **New Value** box, the possible values are 1-4. This is applicable only for the GE device.
 - *Trust CoS-DSCP* — Determines the queue to which the packet is assigned dependent on the CoS tag and DSCP tag. This is applicable only for the GE device.
- **Police** — Enables Policer functionality.
- **Type** — Policer type for the policy. Possible values are:
 - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is

defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.

- *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbps. This field is only relevant when the Police value is Single.
- **Ingress Committed Burst Size (CS)** — Defines the CS in bytes. This field is only relevant when the Police value is Single.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Out of Profile DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
 - *None* — Forwards packets exceeding the defined CIR value.

STEP 3 Add a QoS policy profile.

STEP 4 Click **Apply**. The QoS policy profile is added, and the device is updated.

Modifying the QoS Policy Profile

STEP 1 Click **Quality of Service > Advanced Mode > QoS Policy Profile**. The *Policy Table Page* opens.

STEP 2 Click the **Edit** button. The *Edit QoS Policy Profile Page* opens:

Edit QoS Policy Profile Page

The *Edit QoS Policy Profile Page* contains the following fields.

- **Policy Name** — Displays the user-defined policy name.
- **Class Map** — Displays the user-defined name of the class map.
- **Action** — Defines the action attached to the rule. The possible field value is:
 - **Set** — Defines the Trust configuration manually. The possible field values are:
 - *DSCP* — In the **New Value** box, the possible values are 0-63.
 - *CoS* — In the **New Value** box, the possible values are 0-7.
- **Police** — Enables Policer functionality.
- **Type** — Policer type for the policy. Possible values are:
 - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
 - *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — Specifies the Aggregate Policer Name

- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbps. This field is only relevant when the Police value is Single.
- **Ingress Committed Burst Size (CS)** — Defines the CS in bytes. This field is only relevant when the Police value is Single.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Out Of Profile DSCP* —Remarks packet's DSCP values exceeding the defined CIR value.
 - *None* —Forwards packets exceeding the defined CIR value.

STEP 3 Define the relevant fields.

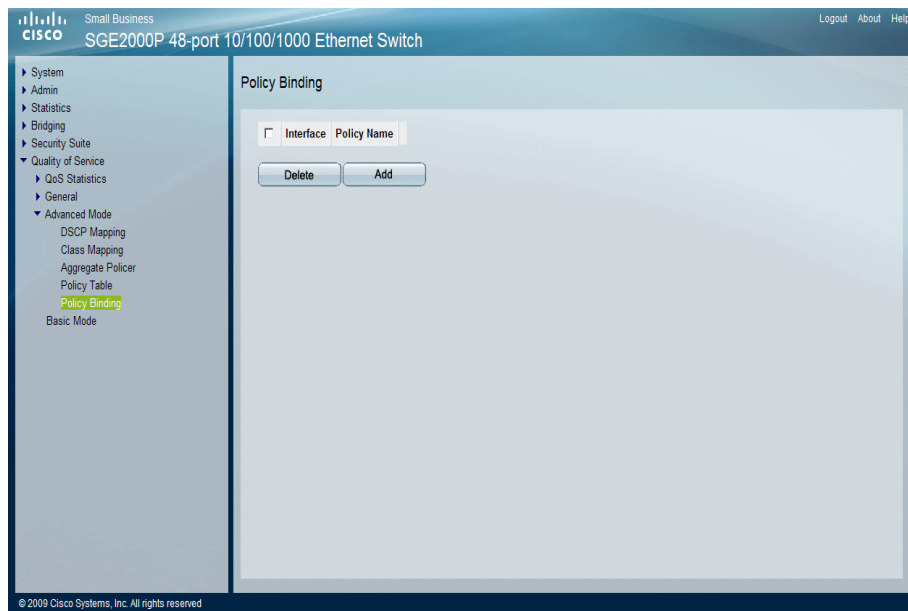
STEP 4 Click **Apply**. The device is updated.

Defining Policy Binding

In the *Policy Binding Page*, QoS policies are associated with specific interfaces.

- STEP 1** Click **Quality of Service > Advanced Mode > Policy Binding**. The *Policy Binding Page* opens:

Policy Binding Page



The *Policy Binding Page* contains the following fields:

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Displays a Policy name associated with the interface.

- STEP 2** Click the **Add** button. The *Add QoS Policy Binding Page* opens:

Add QoS Policy Binding Page

The *Add QoS Policy Binding Page* contains the following fields.

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Select a Policy to associate with the interface.

STEP 3 Define the relevant fields.

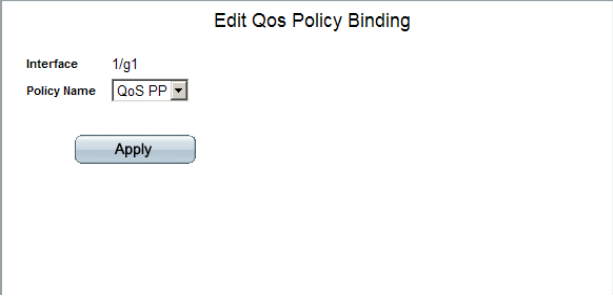
STEP 4 Click **Apply**. The QoS Policy Binding is defined, and the device is updated.

Modifying QoS Policy Binding Settings

STEP 1 Click **Quality of Service > Advanced Mode > Policy Binding**. The *Policy Binding Page* opens:

STEP 2 Click the **Edit** button. The *Edit QoS Policy Binding Page* opens:

Edit QoS Policy Binding Page



The screenshot shows a web interface titled "Edit QoS Policy Binding". It contains two input fields: "Interface" with the text "1/g1" and "Policy Name" with a dropdown menu showing "QoS PP". Below these fields is a blue "Apply" button.

The *Edit QoS Policy Binding Page* contains the following fields.

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Displays the Policy name associated with the interface.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The QoS policy binding is defined, and the device is updated.

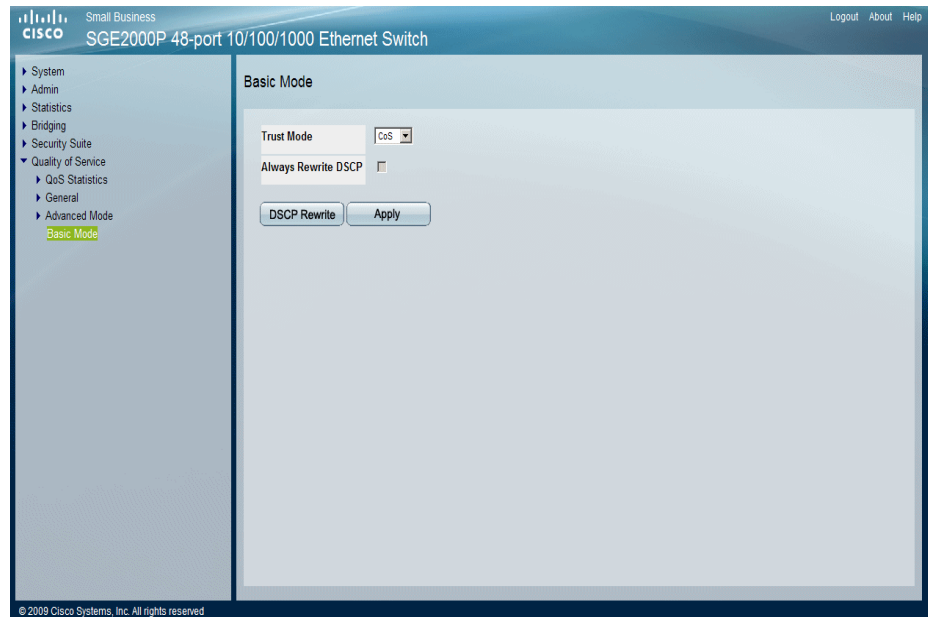
Defining QoS Basic Mode

The *Basic Mode Page* contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

STEP 1 Click **Quality of Service > Basic Mode**. The *Basic Mode Page* opens:

Basic Mode Page



The *Basic Mode Page* contains the following fields:

- **Trust Mode** — Displays the trust mode. If a packet's CoS tag and DSCP tag, are mapped to different queues, the Trust Mode determines the queue to which the packet is assigned. Possible values are:
 - *CoS* — Sets trust mode to CoS on the device. The CoS mapping determines the packet queue
 - *DSCP* — Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue.
- **Always Rewrite DSCP** — Rewrites the packet DSCP tag according to the QoS DSCP Rewriting configuration. *Always Rewrite DSCP* can only be selected if the Trust Mode is set to *DSCP*.

Rewriting DSCP Values

In the *DSCP Mapping Page*, define the *Differentiated Services Code Point* (DSCP) tag to use in place of the incoming DSCP tags.

- STEP 1** Click **Quality of Service > Advanced Mode > DSCP Mapping**. The *DSCP Mapping Page* opens:

DSCP Mapping Page

The screenshot shows the DSCP Mapping configuration page. The left sidebar contains a navigation tree with the following items: System, System Management, SNMP, Admin, Statistics, Bridging, Security Suite, Quality of Service, QoS Statistics, General, CoS, Queue, CoS to Queue, DSCP to Queue, Bandwidth, VLAN Rate Limit, Advanced Mode, **DSCP Mapping** (highlighted), Class Mapping, Aggregate Policies, Policy Table, Policy Binding, and Basic Mode. The main content area is titled 'DSCP Mapping' and contains a table with 15 rows and 6 columns. The columns are labeled 'DSCP In', 'DSCP Out', 'DSCP In', 'DSCP Out', 'DSCP In', and 'DSCP Out'. The rows are numbered 0 through 14. Each cell in the table contains a dropdown menu with a value. The values in the 'DSCP In' columns are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14. The values in the 'DSCP Out' columns are 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, and 39. The table is scrollable, and the bottom of the page shows the copyright notice '© 2009 Cisco Systems, Inc. All rights reserved.'

| DSCP In | DSCP Out | DSCP In | DSCP Out | DSCP In | DSCP Out |
|---------|----------|---------|----------|---------|----------|
| 0 | 25 | 50 | 50 | | |
| 1 | 26 | 51 | 51 | | |
| 2 | 27 | 52 | 52 | | |
| 3 | 28 | 53 | 53 | | |
| 4 | 29 | 54 | 54 | | |
| 5 | 30 | 55 | 55 | | |
| 6 | 31 | 56 | 56 | | |
| 7 | 32 | 57 | 57 | | |
| 8 | 33 | 58 | 58 | | |
| 9 | 34 | 59 | 59 | | |
| 10 | 35 | 60 | 60 | | |
| 11 | 36 | 61 | 61 | | |
| 12 | 37 | 62 | 62 | | |
| 13 | 38 | 63 | 63 | | |
| 14 | 39 | | | | |

The *DSCP Mapping Page* contains the following fields:

- **DSCP In** — Indicates the DSCP value in the incoming packet.
- **DSCP Out** — Indicates the DSCP value in the outgoing packet.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The device is updated.

Configuring SNMP

The Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

SNMP v1 and v2

SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the *Management Information Base (MIB)*. The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, *User Security Model (USM)* is defined for SNMPv3 and includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure message content. *Cipher Block-Chaining (CBC)* is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on a SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares the incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use. The device supports SNMP notification filters based on *Object IDs (OID)*. OIDs are used by the system to manage device features. SNMP v3 supports the following features:
 - Security
 - Feature Access Control
 - Traps

The device generates the following traps:

- Copy trap
- Stacking traps

The SNMP section contains the following topics:

- Configuring SNMP Security

Defining Trap Management



NOTE All private MIBs for the switches in this manual are anchored under the MIB root: enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1)

Configuring SNMP Security

The Security section contains the following topics:

- Defining the SNMP Engine ID
- Defining SNMP Views
- Defining SNMP Users
- Defining SNMP Groups

Defining SNMP Communities

Defining the SNMP Engine ID

The *Engine ID Page* provides information for defining the device engine ID. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of Enterprise number and the default MAC address. Verify that the Engine ID is unique for the administrative domain. This prevents two devices in a network from having the same Engine ID.

STEP 1 Click **System > SNMP > Security > Engine ID**. The *Engine ID Page* opens:

Engine ID Page

Small Business
SGE2000P 48-port 10/100/1000 Ethernet Switch

System
 System Management
 SNMP
 Security
 Engine ID
 Views
 Users
 Groups
 Communities
 Trap Management
 Admin
 Statistics
 Bridging
 Security Suite
 Quality of Service

Engine ID

Local Engine ID (10-64 Hex Characters)

Use Default ☐

Apply

© 2009 Cisco Systems, Inc. All rights reserved

The *Engine ID Page* contains the following fields.

- **Local Engine ID (10-64 Hex characters)** — Indicates the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings consists of two hexadecimal digits. Each byte can be separated by a period or a colon.
- **Use Default** — Uses the device generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
 - *First 4 octets* — first bit = 1, the rest is IANA Enterprise number.
 - *Fifth octet* — Set to 3 to indicate the MAC address that follows.
 - *Last 6 octets* — MAC address of the device.

The possible values are:

- *Checked* — Use the default Engine ID.
- *Unchecked* — Use a user-defined Engine ID.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

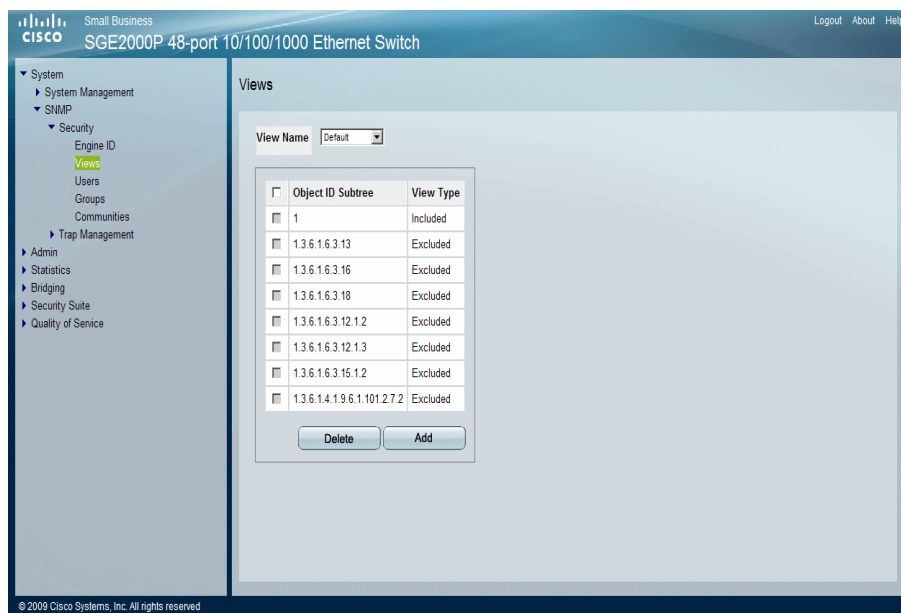
Defining SNMP Views

SNMP Views provide access or block access to device features or feature aspects. For example, a view displays that the SNMP Group A has *Read Only* (R/O) access to Multicast groups, while SNMP Group B has *Read-Write* (R/W) access to Multicast groups. Feature access is granted via the MIB name, or MIB Object ID.

To define SNMP views:

STEP 1 Click **System > SNMP > Security > Views**. The *SNMP Views Page* opens:

SNMP Views Page



The *SNMP Views Page* contains the following fields:

- **View Name** — Displays the user-defined views. The options are as follows:
 - *Default* — Displays the default SNMP view for read and read/write views.
 - *DefaultSuper* — Displays the default SNMP view for administrator views.

- **Object ID Subtree** — Indicates the device feature OID that is included or excluded in the selected SNMP view.
- **View Type** — Indicates if the defined OID branch that are included or excluded in the selected SNMP view.

STEP 2 Click the **Add** button. The *Add SNMP View Page* opens:

Add SNMP View Page

The screenshot shows the 'Add SNMP View' configuration page. It contains the following fields and controls:

- View Name:** A text input field.
- Object ID Subtree:** A section with a radio button labeled 'Select from List' (which is selected). To its right is a list box containing the following items: 'system', 'interfaces', 'ip', 'icmp', and 'tcp'. The 'system' item is currently selected. To the right of the list box are 'Up' and 'Down' buttons.
- Insert:** A radio button labeled 'Insert' followed by a text input field containing the value '1.3.6.1.2.1.1'.
- View Type:** A dropdown menu currently set to 'Included'.
- Apply:** A button at the bottom center of the form.

The *Add SNMP View Page* contains parameters for defining and configuring new SNMP view. The *Add SNMP View Page* contains the following fields:

- **View Name** — Defines the user-defined view name.
- **Object ID Subtree** — Indicates the device feature OID included or excluded in the selected SNMP view. The options to select the Object are as follows:
 - *Select from List* — Select the Subtree from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
 - *Insert* — Enables a Subtree not included to be entered.
- **View Type** — Indicates if the defined OID branch will be included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
 - *Included* — Includes the defined OID branch.
 - *Excluded* — Excludes the defined OID branch.

STEP 3 Define the relevant fields.

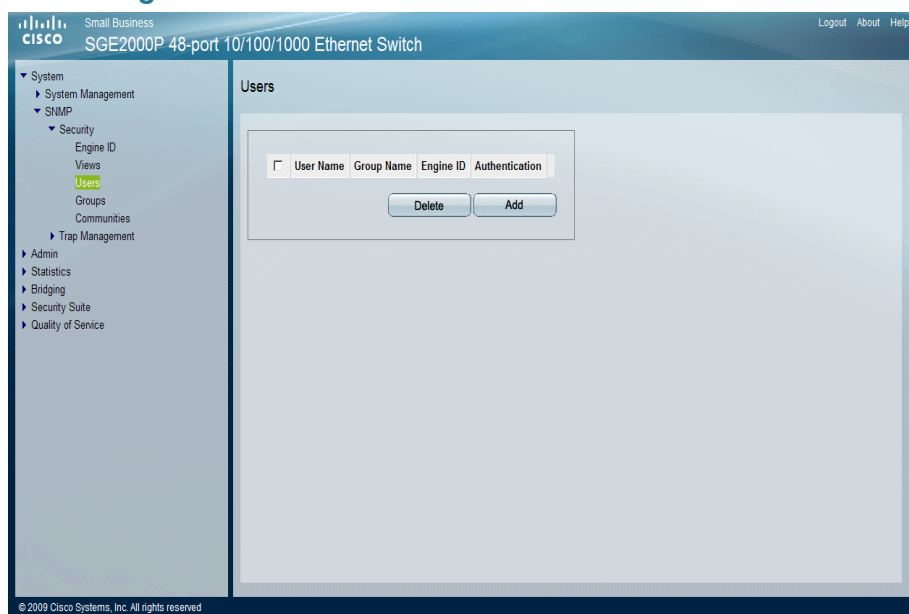
STEP 4 Click **Apply**. The SNMP views are defined, and the device is updated.

Defining SNMP Users

The *SNMP Users Page* provides information for creating SNMP users, and assigning SNMP access control privileges to SNMP users. Groups allow network managers to assign access rights to specific device features, or feature aspects.

STEP 1 Click **System > SNMP > Security > Users**. The *SNMP Users Page* opens:

SNMP Users Page



The *SNMP Users Page* contains the following fields.

- **User Name** — Displays the user-defined user name to which access control rules are applied. The field range is up to 30 characters.
- **Group Name** — User-defined SNMP group to which the SNMP user belongs. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Engine ID** — Indicates the local/remote device engine ID.
- **Authentication** — Indicates the Authentication method used.

STEP 2 Click the **Add** button. The *Add SNMP Group Membership Page* opens:

Add SNMP Group Membership Page

The screenshot shows a web-based configuration page titled "Add SNMP Group Membership". It contains several input fields and a button. The fields are: "User Name" (text input), "Engine ID" (radio buttons for "Local" and "Remote", and a text input for "EngineID not Configured"), "Group Name" (dropdown menu), "Authentication Method" (dropdown menu with "None" selected), "Password" (text input), "Authentication Key" (text input), and "Privacy Key" (text input). An "Apply" button is located at the bottom right of the form.

The *Add SNMP Group Membership Page* provides information for assigning SNMP access control privileges to SNMP groups. The *Add SNMP Group Membership Page* contains the following fields.

- **User Name** — Provides a user-defined local user list.
- **Engine ID** — Indicates either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database.
 - *Local* — Indicates that the user is connected to a local SNMP entity.
 - *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.
- **Group Name** — Contains a list of SNMP groups to which the SNMP user belongs. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Authentication Method** — Indicates the Authentication method used. The possible field values are:
 - *MD5 Key* — Users are authenticated using a valid HMAC-MD5 key.
 - *SHA Key* — Users are authenticated using a valid HMAC-SHA-96 key.
 - *MD5 Password* — Users should enter a password that is encrypted using the HMAC-MD5-96 authentication method.
 - *SHA Password* — Users should enter a password that is encrypted using the HMAC-SHA-96 authentication method.
 - *None* — No user authentication is used.

- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters. This field is available if the Authentication Method is a password.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If HMAC-MD5-96 is selected then 16 bytes are required and if HMAC-SHA-96 then 20 bytes are required. This field is available if the Authentication Method is a key.
- **Privacy Key** — Defines the *Privacy Key* (LSB). If only authentication is required, 16\20 bytes are defined. If both privacy and authentication are required, 36\40 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. This field is available if the Authentication Method is a key.

Modifying SNMP Users

The *Edit SNMP User Page* provides information for assigning SNMP access control privileges to SNMP groups.

Edit SNMP User Page

The screenshot shows the 'Edit SNMP User' configuration page. It contains the following fields and controls:

- User Name**: A dropdown menu.
- Engine ID**: A dropdown menu.
- Group Name**: A dropdown menu.
- Authentication Method**: A dropdown menu currently set to 'None'.
- Password**: A text input field.
- Authentication Key**: A text input field.
- Privacy Key**: A text input field.
- Apply**: A button at the bottom right of the form.

The *Edit SNMP User Page* contains the following fields.

- **User Name** — Displays the user-defined group to which access control rules are applied. Provides a user-defined local user list.
- **Engine ID** — Indicates the local device engine ID.
- **Group Name** — SNMP group, which can be chosen from the list, to which the SNMP user belongs. SNMP groups are defined in the SNMP Group Profile page.

- **Authentication Method**— Indicates the Authentication method used. The possible field values are:
 - *MD5 Key*— Users are authenticated using a valid HMAC-MD5 key.
 - *SHA Key*— Users are authenticated using a valid HMAC-SHA-96 key.
 - *MD5 Password*— Users should enter a password that is encrypted using the HMAC-MD5-96 authentication method.
 - *SHA Password*— Users should enter a password that is encrypted using the HMAC-SHA-96 authentication method.
 - *None*— No user authentication is used.
- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters. This field is available if the Authentication Method is a password.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. This field is available if the Authentication Method is a key.
- **Privacy Key** — Defines the *Privacy Key* (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. This field is available if the Authentication Method is a key.

STEP 3 Define the relevant fields.

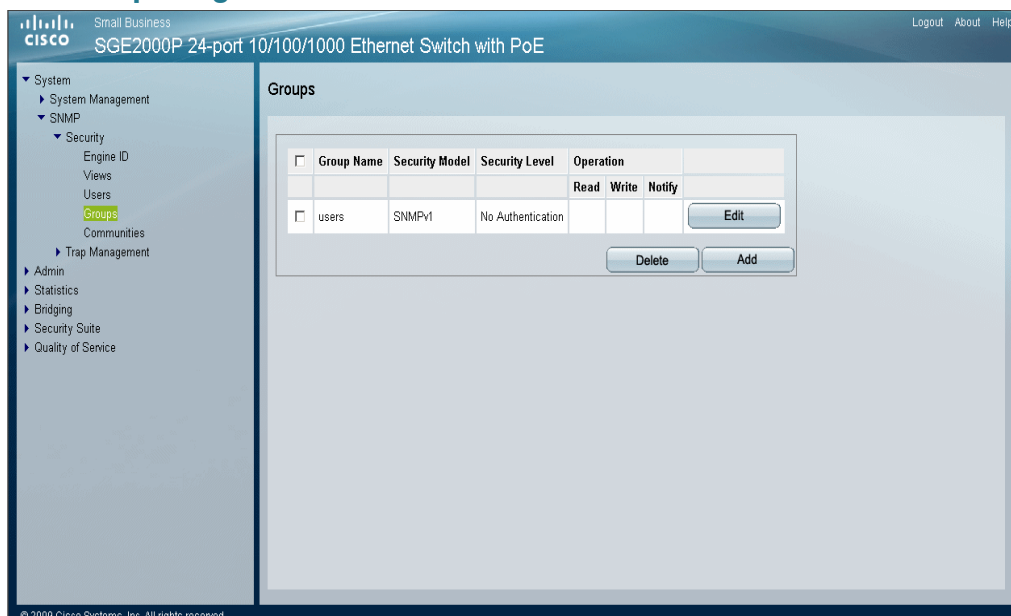
STEP 4 Click **Apply**. The SNMP User is modified, and the device is updated.

Defining SNMP Groups

The *SNMP Groups Page* provides information for creating SNMP groups and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or features aspects.

STEP 1 Click **System > SNMP > Security > Groups**. The *SNMP Groups Page* opens:

SNMP Groups Page



The *SNMP Groups Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which privileges are applied.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
 - *SNMPv1* — SNMPv1 is defined for the group.
 - *SNMPv2* — SNMPv2 is defined for the group.
 - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
 - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
 - *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
 - *Privacy* — Encrypts SNMP message.

- **Operation** — Defines the group access right, which are per view. The possible field values are:
 - *Read* — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
 - *Write* — The management access is read-write and changes can be made to the assigned SNMP view.
 - *Notify* — Sends traps for the assigned SNMP view.

STEP 2 Click the **Add** button. The *Add SNMP Group Profile Page* opens:

Add SNMP Group Profile Page

The screenshot shows a web form titled "Add SNMP Group Profile". It includes the following fields and controls:

- Group Name:** A text input field.
- Security Model:** A dropdown menu with "SNMPv1" selected.
- Security Level:** A dropdown menu with "No Authentication" selected.
- Operation:** Three checkboxes labeled "Read", "Write", and "Notify". Each checkbox has a dropdown menu next to it, all showing "Default".
- Apply:** A button at the bottom right of the form.

The *Add SNMP Group Profile Page* allows network managers to define new SNMP Group profiles. The *Add SNMP Group Profile Page* contains the following fields:

- **Group Name** — Defines the user-defined group to which privileges are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
 - *SNMPv1* — SNMPv1 is defined for the group.
 - *SNMPv2* — SNMPv2 is defined for the group.
 - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only.
 - *No Authentication* — Neither the Authentication nor the Privacy security levels are assigned to the group.

- *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
 - *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access right, which are per view. The possible field values are:
 - *Default* — Defines the default group access rights.
 - *DefaultSuper* — Defines the default group access rights for administrator.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The SNMP Community is defined, and the device is updated.

Modifying SNMP Group Profile Settings

STEP 1 Click **System > SNMP > Security > Groups**. The *SNMP Groups Page* opens:

STEP 2 Click the **Edit** Button. The *Edit SNMP Group Profile Page* opens:

Edit SNMP Group Profile Page

The screenshot shows the 'Edit SNMP Group Profile' configuration page. It includes the following fields and controls:

- Group Name:** A dropdown menu currently set to 'users'.
- Security Model:** A dropdown menu currently set to 'SNMPv1'.
- Security Level:** A dropdown menu currently set to 'No Authentication'.
- Operation:** Three checkboxes with associated dropdown menus:
 - ☒ **Read:** Dropdown set to 'Default'.
 - ☐ **Write:** Dropdown set to 'Default'.
 - ☒ **Notify:** Dropdown set to 'Default'.
- Apply:** A button at the bottom right to save the configuration.

The *Edit SNMP Group Profile Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
 - *SNMPv1* — SNMPv1 is defined for the group.
 - *SNMPv2* — SNMPv2 is defined for the group.

- *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only.
 - *No Authentication* — Neither the Authentication nor the Privacy security levels are assigned to the group.
 - *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
 - *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access rights. The options for Read, Write, and Notify operations are as follows:
 - *Default* — Defines the default group access rights.
 - *DefaultSuper* — Defines the default group access rights for administrator.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The SNMP Group Profile is modified, and the device is updated.

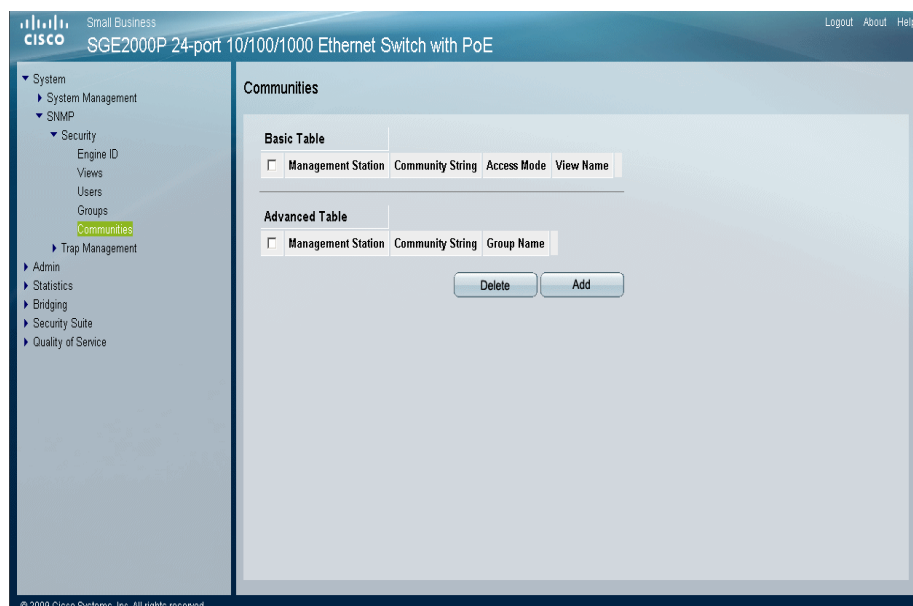
Defining SNMP Communities

The Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

To define SNMP Communities:

- STEP 1** Click **System > SNMP > Security > Communities**. The *SNMP Communities Page* opens:

SNMP Communities Page



The *SNMP Communities Page* is divided into the following tables:

- Basic Table
- Advanced Table

The SNMP Communities Basic Table area contains the following fields:

- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.
- **Access Mode** — Displays the access rights of the community.
- **View Name** — Displays the SNMP view.

The SNMP Communities Advanced Table area contains the following fields:

- **Management Station** — Displays the management station IP address for which the Advanced SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.

- **Group Name** — Displays advanced SNMP communities group name.

STEP 2 Click the **Add** button. The *Add SNMP Community Page* opens.

Add SNMP Community Page

The screenshot shows the 'Add SNMP Community' configuration page. It includes several sections: 'Supported IP Format' with radio buttons for 'Version 6' (selected) and 'Version 4'; 'IPv6 Address Type' with radio buttons for 'Link Local' (selected) and 'Global'; 'Link Local Interface' with radio buttons for 'None' (selected) and 'ISATAP'; 'SNMP Management Station' with radio buttons for a specific IP (selected) and 'All (0.0.0.0)'; and a 'Community String' text field. Below these are two tabs: 'Basic' (selected) and 'Advanced'. The 'Basic' tab contains 'Access Mode' (a dropdown menu showing 'Read Only'), a checkbox for 'View Name' (unchecked), and a 'View Name' dropdown menu showing 'Default'. The 'Advanced' tab contains a 'Group Name' dropdown menu showing 'users'. An 'Apply' button is located at the bottom right of the form.

The *Add SNMP Community Page* allows network managers to define and configure new SNMP communities. The *Add SNMP Community Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - — Indicates the device supports IPv6.
 - — Indicates the device supports IPv4.
- **IPv6 Address Type** — Indicates the supported IPv6. The possible field values are:
 - *Link Local* — Indicates IPv6 address is a Link Local.
 - *Global* — Indicates IPv6 address is global.
- **Link Local Interface** — Indicates the Link Local Interface. The possible field values are:
 - *VLAN* — Indicate the VLAN is defined as the
 - *ISATAP* — Indicates a ISATAP tunnel is a Link Local interface.
- — Defines the management station IP address for which the SNMP community is defined. **Community String** — Defines the password used to authenticate the management station to the device.

Configure either the Basic Mode or the Advanced Mode.

- **Basic** — Enables SNMP Basic mode for a selected community and contains the following fields:
 - **Access Mode** — Defines the access rights of the community. The possible field values are:
 - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
 - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
 - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
 - **View Name** — Contains a list of user-defined SNMP views.
- **Advanced** — Enables SNMP Advanced mode for a selected community and contains the following field:
 - **Group Name** — Defines advanced SNMP communities group names.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Edit SNMP Communities

STEP 1 Click **System > SNMP > Security > Communities**. The *SNMP Communities Page* opens:

STEP 2 Click the **Edit** Button. The *Edit SNMP Community Page*.

Edit SNMP Community Page

The screenshot shows the 'Edit SNMP Community' configuration window. At the top, there are two dropdown menus: 'SNMP Management' set to 'All' and 'Community String' set to '111'. Below these, there are two radio buttons: 'Basic' (selected) and 'Advanced'. The 'Basic' section includes an 'Access Mode' dropdown set to 'Read Only', a checked 'View Name' checkbox, and a 'View Name' dropdown set to 'Default'. The 'Advanced' section includes a 'Group Name' dropdown set to 'users'. An 'Apply' button is located at the bottom center of the window.

The *Edit SNMP Community Page* contains the following fields:

- **SNMP Management** — Defines the management station IP address for which the SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.

Configure either the Basic Mode or the Advanced Mode.

- **Basic** — Enables SNMP Basic mode for a selected community and contains the following fields:
 - **Access Mode** — Defines the access rights of the community. The possible field values are:
 - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
 - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
 - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
 - **View Name** — Contains a list of user-defined SNMP views.
- **Advanced** — Enables SNMP Advanced mode for a selected community and contains the following fields:
 - **Group Name** — Defines advanced SNMP communities group names.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Defining Trap Management

This section contains the following topics:

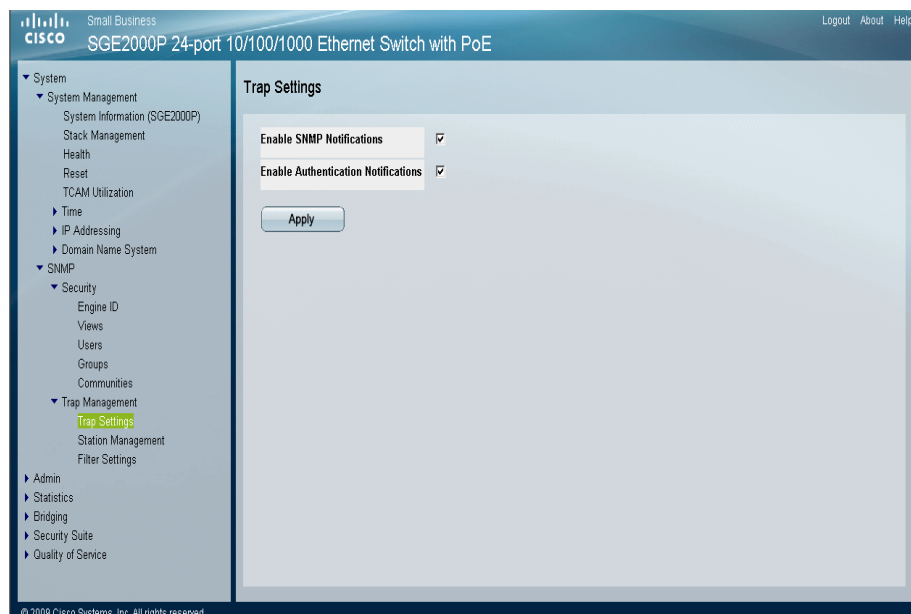
- Defining Trap Settings
- Configuring Station Management
- Defining SNMP Filter Settings

Defining Trap Settings

The *Trap Settings Page* contains parameters for defining SNMP notification parameters.

STEP 1 Click **System > SNMP > Trap Management > Trap Settings**. The *Trap Settings Page* opens:

Trap Settings Page



The *Trap Settings Page* contains the following fields:

- **Enable SNMP Notification** — Specifies whether the device can send SNMP notifications. The possible field values are:
 - *Checked* — Enables SNMP notifications.
 - *Unchecked* — Disables SNMP notifications.
- **Enable Authentication Notification** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
 - *Checked* — Enables the device to send authentication failure notifications.
 - *Unchecked* — Disables the device from sending authentication failure notifications.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The SNMP Trap settings are defined, and the device is updated.

Configuring Station Management

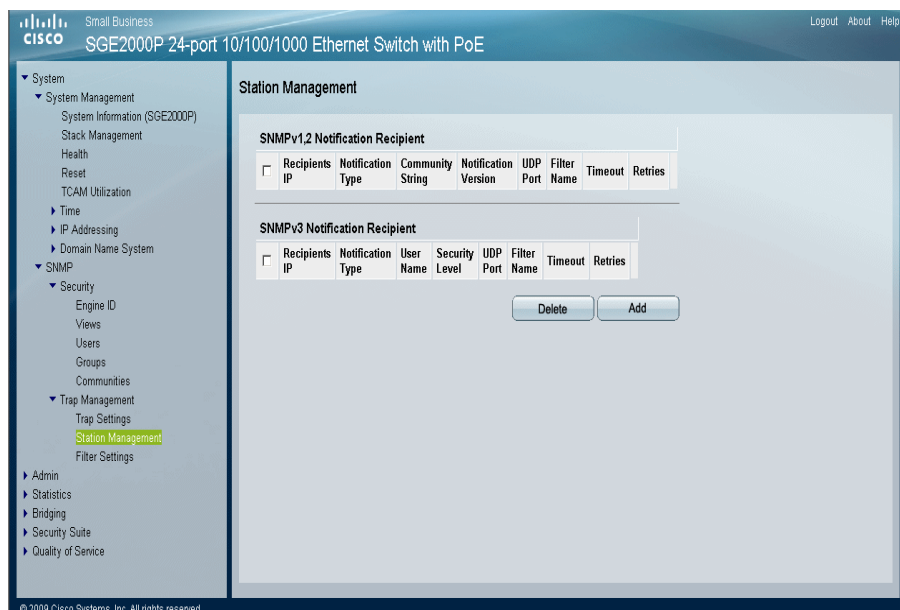
The *Station Management Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

Traps indicating status changes are issued by the switch to specified trap managers. Specify the trap managers so that key events are reported by this switch to the management station. Specify up to eight management stations that receive authentication failure messages and other trap messages from the switch.

STEP 1 Click **System > SNMP > Trap Management > Station Management**. The *Station Management Page* opens:

Station Management Page



The *Station Management Page* contains two areas, the *SNMPv1,2 Notification Recipient* and the *SNMPv3 Notification Recipient* table.

The *SNMPv1,2 Notification Recipient* table area contains the following fields:

- **Recipients IP** — Indicates the IP address to which the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
 - *Trap* — Indicates traps are sent.
 - *Inform* — Indicates informs are sent.
- **Community String** — Identifies the community string of the trap manager.
- **Notification Version** — Determines the trap type. The possible field values are:
 - *SNMP V1* — Indicates SNMP Version 1 traps are sent.
 - *SNMP V2* — Indicates SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.

- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

The *SNMPv3 Notification Recipient* table area contains the following fields:

- **Recipients IP** — Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
 - *Trap* — Indicates traps are sent.
 - *Inform* — Indicates informs are sent.
- **User Name** — Displays the SNMP user names.
- **Security Level** — Defines the means by which the packet is authenticated. The possible field values are:
 - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
 - *Authentication* — Indicates the packet is authenticated.
 - *Privacy* — Indicates the packet is both authenticated and encrypted.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Defines if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

STEP 2 Click the **Add** button. The *Add SNMP Notification Recipient Page* opens.

Add SNMP Notification Recipient Page

The screenshot shows the 'Add SNMP Notification Recipient' configuration page. It includes sections for 'Supported IP Format' (Version 6 and Version 4), 'IPv6 Address Type' (Link Local and Global), 'Link Local Interface' (None and ISATAP), 'Recipient IP Address' (text input), 'Notification Type' (Traps dropdown), 'SNMPv1,2' (Community String and Notification Version dropdown), 'SNMPv3' (User Name, Security Level dropdown), 'UDP Port' (162), 'Filter Name' (dropdown), 'Timeout' (15 seconds), and 'Retries' (3). An 'Apply' button is at the bottom right.

The *Add SNMP Notification Recipient Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

The *Add SNMP Notification Recipient Page* contains the following fields:

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - — Indicates the device supports IPv6.
 - — Indicates the device supports IPv4. *VLAN* the VLAN is defined as the Local Link Interface.
- **Recipient IP** — Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:

- *Trap* — Indicates traps are sent.
- *Inform* — Indicates informs are sent.

Either SNMPv1,2 or SNMPv3 may be used as the version of traps, with only one version enabled at a single time.

The SNMPv1,2 Notification Recipient area contains the following fields:

- **SNMPv1,2** — Enables SNMPv1,2 as the Notification version. If SNMPv1,2 is enabled, the **Community String** and **Notification Version** fields are enabled for configuration:
- **Community String** — Identifies the community string of the trap manager.
- **Notification Version** — Determines the trap type. The possible field values are:
 - *SNMP1* — Indicates SNMP Version 1 traps are sent.
 - *SNMP2* — Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

- **SNMPv3** — Enables SNMPv3 as the Notification version. If SNMPv3 is enabled, the **User Name** and **Security Level** fields are enabled for configuration:
- **User Name** — Defines the user to whom SNMP notifications are sent.
- **Security Level** — Defines the means by which the packet is authenticated. The possible field values are:
 - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
 - *Authentication* — Indicates the packet is authenticated.
 - *Privacy* — Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Defines if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The SNMP Notification Recipient settings are defined, and the device is updated.

Modifying SNMP Notifications

The *Edit SNMP Notification Recipient Page* allows system administrators to define notification settings. The *Edit SNMP Notification Recipient Page* is divided into four areas, Notification Recipient, SNMPv1,2 Notification Recipient, SNMPv3 Notification Recipient and UDP Port Notification Recipient.

STEP 1 Click **System > SNMP > Security > Trap Management > Station Management**.

STEP 2 Click the **Edit** button. The *Edit SNMP Notification Recipient Page* opens:

Edit SNMP Notification Recipient Page

The screenshot shows the 'Edit SNMP Notification Recipient' configuration page. It includes the following fields and options:

- Recipient IP Address:** A dropdown menu currently set to '10.5.80.16'.
- Notification Type:** A dropdown menu currently set to 'Traps'.
- SNMPv1,2 Section:**
 - Community String:** A text input field containing '111'.
 - Notification Version:** A dropdown menu currently set to 'SNMPv1'.
- SNMPv3 Section:**
 - User Name:** A dropdown menu.
 - Security Level:** A dropdown menu currently set to 'NoAuthentication'.
- UDP Port:** A text input field containing '162'.
- Filter Name:** A dropdown menu.
- Informs Timeout:** A text input field containing '15'.
- Informs Retries:** A text input field containing '3'.
- Apply:** A button at the bottom right of the form.

The *Edit SNMP Notification Recipient Page* contains the following fields:

- **Recipients IP**— Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
 - *Trap* — Indicates traps are sent.

- *Inform* — Indicates informs are sent.

Either SNMPv1,2 or SNMPv3 may be used as the version of traps, with only one version enabled at a single time. The SNMPv1,2 Notification Recipient area contains the following fields:

- **SNMPv1,2** — Enables SNMPv1,2 as the Notification version. If SNMPv1,2 is enabled, the **Community String** and **Notification Version** fields are enabled for configuration:
- **Community String** — (SNMP v1, 2) Identifies the community string of the trap manager.
- **Notification Version** — (SNMP v1, 2) Determines the trap type. The possible field values are:
 - *SNMP V1* — Indicates SNMP Version 1 traps are sent.
 - *SNMP V2* — Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

- **SNMPv3** — Enables SNMPv3 as the Notification version. If SNMPv3 is enabled, the **User Name** and **Security Level** fields are enabled for configuration:
- **User Name** — Defines the user to whom SNMP notifications are sent.
- **Security Level** — (SNMP v3) Defines the means by which the packet is authenticated. The possible field values are:
 - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
 - *Authentication* — Indicates the packet is authenticated.
 - *Privacy* — Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Informs Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Informs Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

STEP 3 Define the relevant fields.

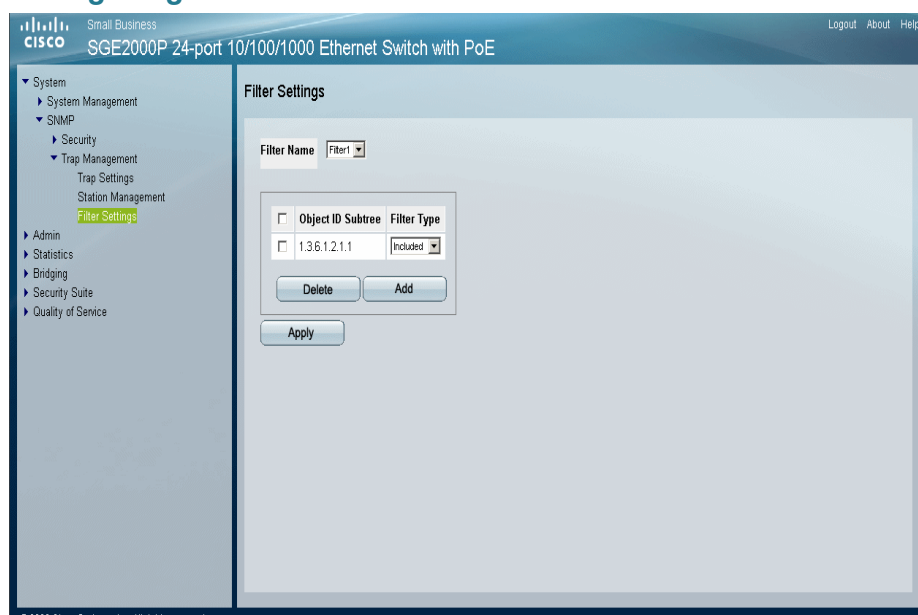
STEP 4 Click **Apply**. The SNMP Notification Receivers are defined, and the device is configured.

Defining SNMP Filter Settings

The *Filter Settings Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The Filter Settings Page also allows network managers to filter notifications.

STEP 1 Click **System > SNMP > Trap Management > Filter Settings**. The *Filter Settings Page* opens:

Filter Settings Page



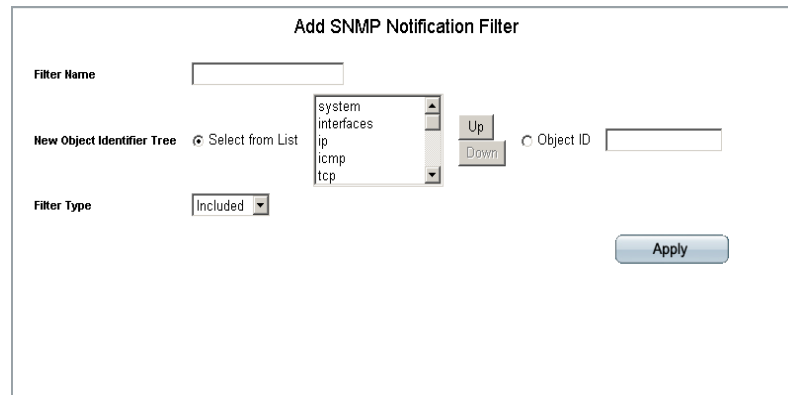
The *Filter Settings Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object ID Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients.
- **Filter Type** — Indicates whether informs or traps are sent regarding the OID to the trap recipients.

- *Excluded* — Restricts sending OID traps or informs.
- *Included* — Sends OID traps or informs.

STEP 2 Click the **Add** button. The *Add SNMP Notification Filter Page* opens:

Add SNMP Notification Filter Page



The *Add SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **New Object Identifier Tree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the *Select from List* or the *Object ID List*. There are two configuration options:
 - *Select from List* — Select the OID from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
 - *Object ID* — Enter an OID not offered in the *Select from List* option.
- **Filter Type** — Indicates whether OID-based informs or traps are sent to trap recipients.
 - *Excluded* — Restricts sending OID traps or informs.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Managing System Files

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Backup Configuration File** — Contains a backup copy of the device configuration. The Backup file is generated when the Running Configuration file or the Startup file is copied to the Backup file. The commands copied into the file replaces the existing commands saved in the Backup file. The Backup file contents can be copied to either the Running configuration or the Startup Configuration files.

Image Files — Software upgrades are used when a new version file is downloaded. This section contains information for defining File maintenance and includes both configuration file management as well as device access.

The File Management section contains the following topics:

- Firmware Upgrade
- Save Configuration
- Copy Files
- Active Image

Firmware Upgrade

Firmware files are downloaded as required for upgrading the firmware version or for backing up the system configuration. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_"). The *Firmware Upgrade Page* contains parameters for downloading system files.

STEP 1 Click **Admin > File Management > Firmware Upgrade**. The *Firmware Upgrade Page* opens:

Firmware Upgrade Page

The screenshot shows the Cisco Small Business SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE configuration page. The left sidebar contains a navigation menu with 'System', 'Admin', 'File Management', 'Logs', 'Diagnostics', 'Statistics', 'Bridging', 'Security Suite', and 'Quality of Service'. Under 'File Management', 'Firmware Upgrade' is selected. The main content area is titled 'Firmware Upgrade' and has two tabs: 'UPGRADE' and 'BACKUP'. The 'UPGRADE' tab is active, showing the following fields: 'File Type' (a dropdown menu with 'Software Image' selected), 'Supported IP Format' (radio buttons for 'Version 6' and 'Version 4'), 'IPv6 Address Type' (radio buttons for 'Link Local' and 'Global'), 'Link Local Interface' (radio buttons for 'None' and 'ISATAP'), 'TFTP Server' (a text input field), and 'Source File' (a text input field). An 'Apply' button is located at the bottom of the form.

The *Firmware Upgrade Page* contains the following fields:

- **U** — Specifies that firmware is downloaded for a firmware upgrade.
- **B** — Indicates the file name on TFTP server where the uploaded image is saved.
- **File Type** — Specifies the file type of the downloaded file. The possible field values are:
 - *Software Image* — Downloads the Image file.
 - *Boot Code* — Downloads the Boot file.

- **Supported IP Format** — Indicates the supported IP version. The possible values are:
 - — Indicates the device supports IPv6.
 - — Indicates the device supports IPv4.
- **IPv6 Address Type** — Displays the IPv6 Type. The possible field values are:
 - *Link local* — Indicates the IPv6 address is link-local, that uniquely identifies hosts on a single network link. A Link-local address has a prefix of 'FE80'. The link-local addresses are not routable and can be used for communication on the same network only.
 - *Global* — Indicates the IPv6 address is a global Unicast IPV6 type which is visible and reachable from different subnets.
- **VLAN** the VLAN is defined as the Link Local Interface.
- **TFTP Server** — Specifies the TFTP Server IP Address from which files are downloaded.
- **Source File** — Specifies the file to be downloaded. This field is applicable for upgrades only.
- **Destination File** — Specifies the name of the file after it is downloaded (Save As).
- **Download to Master Only** — Downloads the file to the Stacking Master only.
- **Download to all Units** — Downloads the file to all stacking members.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

Save Configuration

The configuration files control the operation of the switch, and contain the functional settings at the device and the port level. Configuration files are one of the following types:

- **Factory Default** — Contains preset default parameter definitions which are downloaded with a new or upgraded version.
- **Running Configuration** — Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device

was started or rebooted. When the device shuts down or reboots the next time, this configuration becomes the Starting Configuration.

- **Starting configuration** — Contains the parameter definitions which were valid in the Running Configuration when the system last rebooted or shut down.
- **Backup configuration** — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”). In the *Save Configuration Page*, define the parameters of the system configuration files.

STEP 1 Click **Admin > File Management > Save Configuration**. The *Save Configuration Page* opens:

Save Configuration Page

The *Save Configuration Page* contains the following fields:

- **via TFTP** — Download and upload files using TFTP.
- **via HTTP** — Download and upload files using HTTP.

Via TFTP

- — Specifies that the configuration file is associated with a upgrade.
- — Specifies that the configuration file contains the system backup configuration.

Via HTTP

- **Source File** — Name of the configuration file.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

Copy Files

All software images on the stack must be identical to ensure proper operation of the stack. There are two different ways to update images across the stack:

- Image can be updated prior to connecting a unit to the stack. (This is the recommended method.)
- Upgrade master and copy master image to units across the stack.

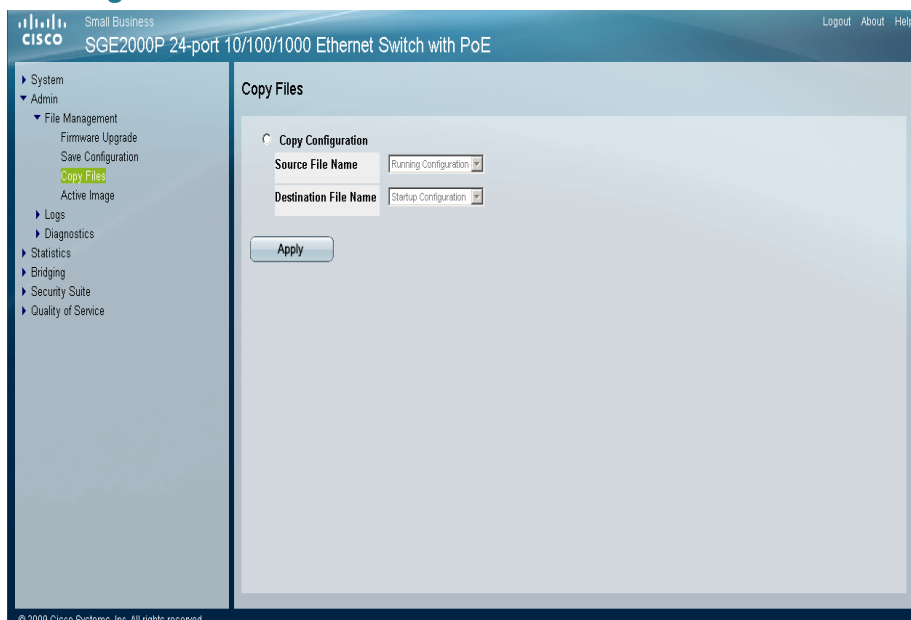
These steps can be done from the Menu-Based CLI or from the web interface.

- Copy image from TFTP to master
- Change active image on master
- Reboot master
- Copy from master to rest of units
- Change active of rest of units
- Reload only rest of units and not master.

In the *Copy Files Page*, network administrators can copy configuration files from one device to another.

STEP 1 Click **Admin > File Management > Copy Files**. The *Copy Files Page* opens:

Copy Files Page



The *Copy Files Page* contains the following fields:

- **Copy Master Firmware** — Indicates the Stacking Master image or boot file to copy. The possible field values are:
 - *Source* — Copies the current Stacking Master's firmware.
 - *Destination Unit* — Defines the stacking member to which the firmware is downloaded.
- **Copy Configuration** — Indicates the device configuration file to copy and the intended usage of the copied file (Running, Startup, or Backup).
 - *Source File Name* — Indicates the type of configuration file to copy from the device.
 - *Destination File Name* — Indicates the file to be copied to the destination device.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

Active Image

The *Active Image Page* allows network managers to select the Image files. For stackable device, active image is indicated/selected per each stack unit. Images are activated only after the device is reset.

STEP 1 Click **Admin > File Management > Active Image**. The *Active Image Page* opens:

Active Image Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
File Management
Firmware Upgrade
Save Configuration
Copy Files
Active Image
Logs
Diagnostics
Statistics
Bridging
Security Suite
Quality of Service

Active Image

| Unit No. | Active Image | After Reset |
|----------|--------------|-------------|
| 2 | Image 1 | Image 1 |

Apply

© 2009 Cisco Systems, Inc. All rights reserved.

The *Active Image Page* contains the following fields:

- **Unit No.** — Indicates the unit number for which the Image file is selected.
- **Active Image** — Indicates the Image file which is currently active on the device.
- **After Reset** — The Image file which is active after the device is reset. The possible field values are:
 - *Image 1* — Activates Image file 1 after the device is reset.
 - *Image 2* — Activates Image file 2 after the device is reset.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

Managing Power-over-Ethernet Devices

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources.

Power-over-Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- Audio and Video Remote Monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports. Guard Band protects the device from exceeding the maximum power level. For example, if 400W is maximum power level, and the Guard Band is 20W, if the total system power consumption exceeds 380W no additional PoE components can be added. The accumulated PoE components power consumption is rounded down for display purposes, therefore remove value after decimal point.

This section contains the following topic:

- Defining PoE Settings

Defining PoE Settings

The *PoE Settings Page* contains system PoE information for enabling PoE on the device and monitoring the current power usage.

To configure PoE Settings:

STEP 1 Click **Bridging > Port Management > PoE Settings**. The *PoE Settings Page* opens:

PoE Settings Page



The *PoE Settings Page* displays the currently configured PoE ports and contains the following information:

- **Port** — Displays the selected port number.
- **Admin Status** — Indicates whether PoE is enabled or disabled on the port. The possible values are:
 - *Enable* — Enables PoE on the port. This is the default setting.
 - *Disable* — Disables PoE on the port.
- **Priority** — Indicates the PoE port priority. The possible values are: *Critical*, *High* and *Low*. The default is *Low*.
- **Power Allocation (mW)** — Indicates the power in milliwatts allocated to the port. The range is 3,400 -15,400.
- **Power Consumption (mW)** — Indicates the amount of power in milliwatts assigned to the powered device connected to the selected interface.

STEP 2 Click the **Edit** button. The *Edit PoE Settings Page* opens:

Edit PoE Settings Page

Edit PoE Settings

| | |
|---------------------------|-------------------------------------|
| Port | 2/g1 |
| Enable PoE | <input checked="" type="checkbox"/> |
| Power Priority Level | Low |
| Power Allocation | 15400 |
| Power Consumption | 0 |
| Overload Counter | 0 |
| Short Counter | 0 |
| Denied Counter | 0 |
| Absent Counter | 0 |
| Invalid Signature Counter | 0 |

Apply

The *Edit PoE Settings Page* contains the following fields:

- **Port** — Indicates the specific interface for which PoE parameters are defined, and assigned to the powered interface connected to the selected port.
- **Enable PoE** — Enables or disables PoE on the port. The possible values are:
 - *Checked* — Enables PoE on the port. This is the default setting.
 - *Unchecked* — Disables PoE on the port.
- **Power Priority Level** — Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power. The possible field values are:
 - *Low* — Defines the PoE priority level as low.
 - *High* — Defines the PoE priority level as high.
 - *Critical* — Defines the PoE priority level as Critical. This is the highest PoE priority level.
- **Power Allocation** — Indicates the power in milliwatts allocated to the port. The range is 0 -15,400.

- **Power Consumption** — Indicates the amount of power in milliwatts assigned to the powered device connected to the selected interface.
- **Overload Counter** — Indicates the total power overload occurrences.
- **Short Counter** — Indicates the total power shortage occurrences.
- **Denied Counter** — Indicates times the powered device was denied power.
- **Absent Counter** — Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.
- **Invalid Signature Counter** — Indicates the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signature are generated during powered device detection, classification, or maintenance.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The PoE Settings are defined, and the device is updated.

Managing Device Diagnostics

This section contains information for configuring port mirroring, running cable tests, and viewing device operational information, and includes the following topics:

- Viewing Integrated Cable Tests
- Performing Optical Tests
- Configuring Port Mirroring
- Viewing CPU Utilization

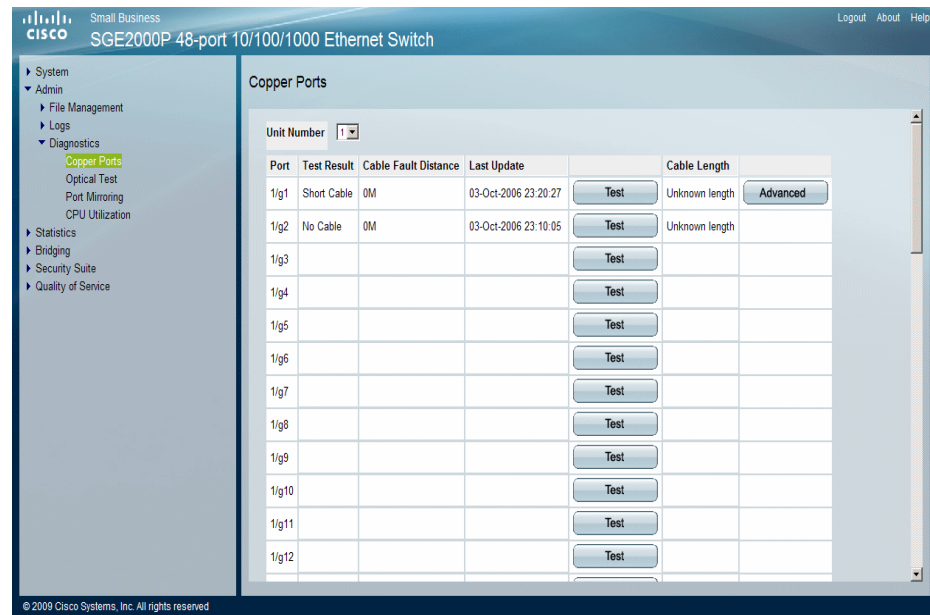
Viewing Integrated Cable Tests

The *Copper Ports Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error that occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 100 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To test cables:

STEP 1 Click **Admin > Diagnostics > Copper Ports**. The *Copper Ports Page* opens:

Copper Ports Page

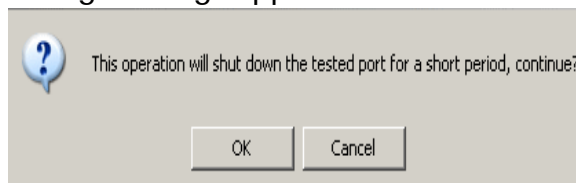


The *Copper Ports Page* contains the following fields:

- **Unit Number** — Indicates the unit number on which the tests are performed.
- **Port** — Displays the port list.
- **Test Result** — Displays the cable test results. Possible values are:
 - *No Cable* — Indicates that a cable is not connected to the port.
 - *Open Cable* — Indicates that a cable is connected on only one side.
 - *Short Cable* — Indicates that a short has occurred in the cable.
 - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred. **Last Update** — Indicates the last time the cable tests were updated. **Cable Length** — Indicates the cable length. This test can only be performed when the port is up and operating at 1 Gbps.

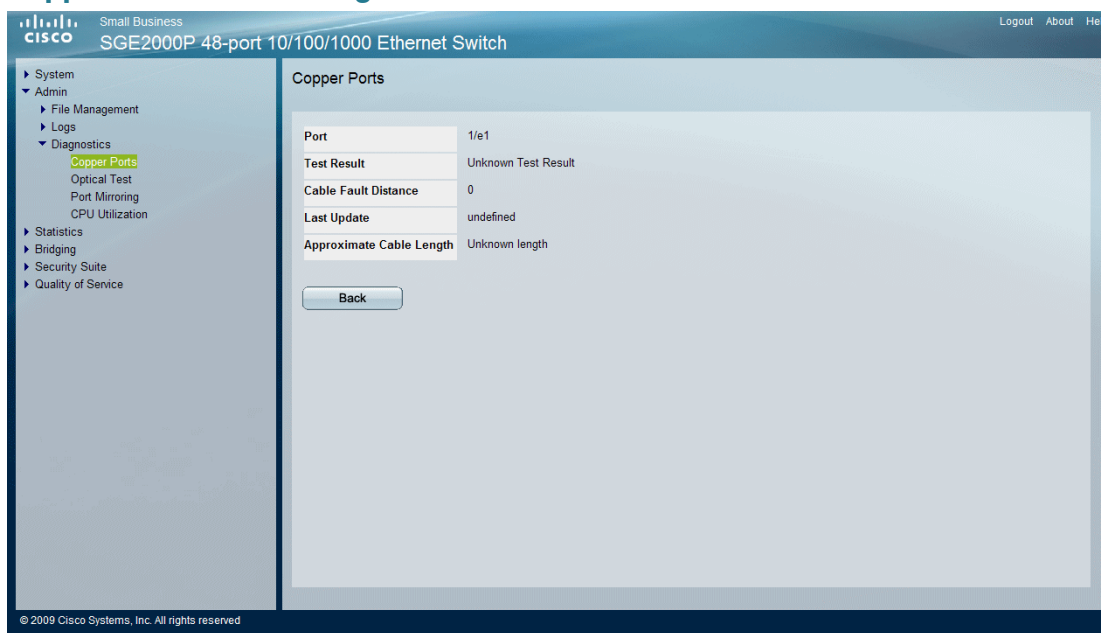
STEP 2 Click the **Test** button to run the cable test. The results of the test appear.

STEP 3 The following message appears:



STEP 4 Click OK, The Copper Ports Page opens:

Copper Ports Results Page



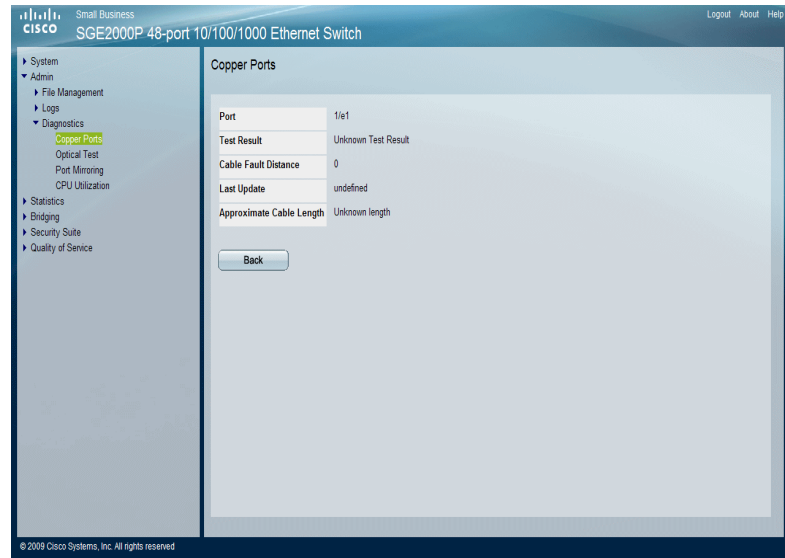
The *Copper Ports Results Page* contains the following fields:

- **Port** — Specifies port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
 - *OK* — Indicates that a cable passed the test.
 - *No Cable* — Indicates that a cable is not connected to the port.
 - *Open Cable* — Indicates that a cable is connected on only one side.
 - *Short Cable* — Indicates that a short has occurred in the cable.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.
- **Last Update** — Indicates the last time the port was tested.

- **Approximate Cable Length** — Indicates the estimated cable length. This test can only be performed when the port is up and operating at 1 Gbps.

For testing on GE ports, an **Advanced** button opens the *Copper Cable Extended Feature Screen*.

Advanced Cable Test Screen - GE Ports



The *Copper Cable Extended Feature Screen* contains the following fields.

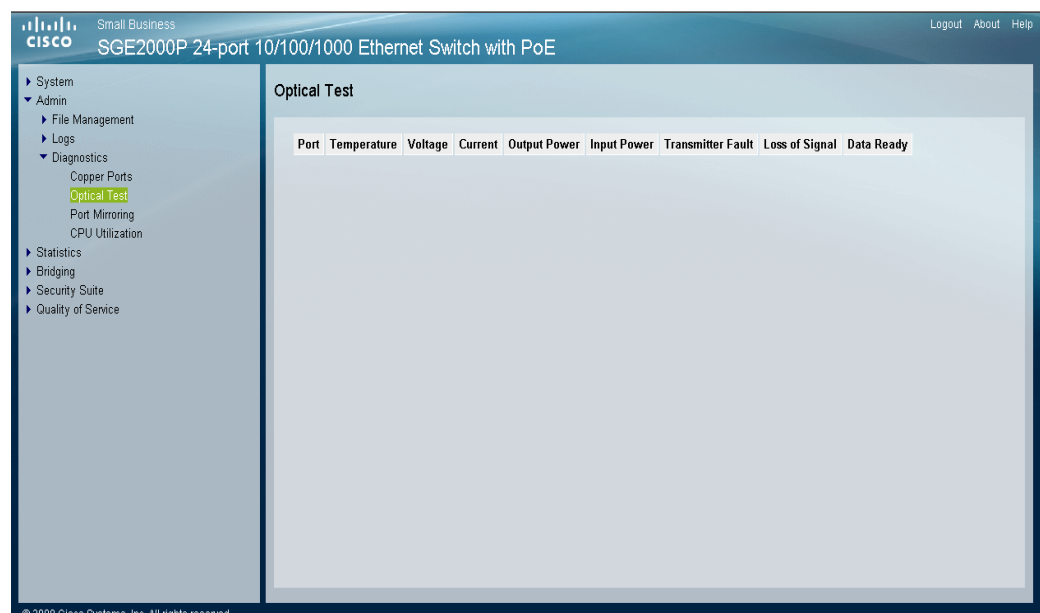
- **Cable Status** — Displays the cable status.
- **Speed** — Indicates the speed at which the cable is transmitting packets.
- **Link Status** — Displays the current link status.
- **Pair** — The pair of cables under test.
- **Distance to Fault** — Indicates the distance between the port and where the cable error occurred.
- **Status** — Displays the cable status.
- **Cable length** — Displays the cable length.
- **Channel** — Displays the cable's channel.
- **Polarity** — Automatic polarity detection and correction permits on all RJ-45 ports for automatic adjustment of wiring errors.
- **Pair Skew** — Reaction or transmission time in nanoseconds for the selected cable pair and given cable length.

STEP 5 Click **Done** to close the window.

Performing Optical Tests

The *Optical Test Page* allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present.

Optical Test Page



The *Optical Test Page* contains the following fields:

- **Port** — Displays the port number on which the cable is tested.
- **Temperature** — Displays the temperature (C) at which the cable is operating.
- **Voltage** — Displays the voltage at which the cable is operating.
- **Current** — Displays the current at which the cable is operating.
- **Output Power** — Indicates the rate at which the output power is transmitted.
- **Input Power** — Indicates the rate at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.

- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the data status.

Configuring Port Mirroring

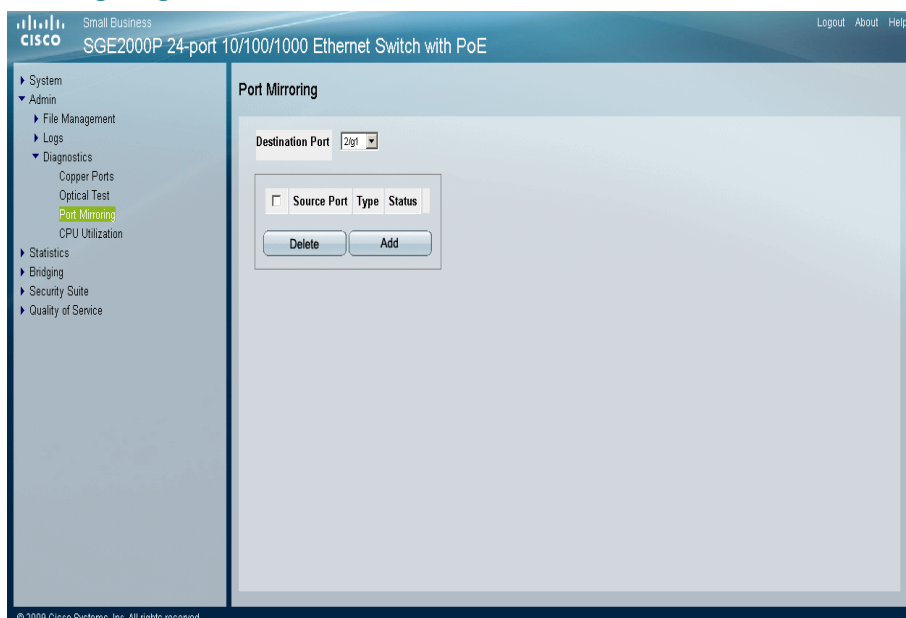
Port Mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as diagnostic tool and/or a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators configure port mirroring by selecting a specific port to copy all packets, and different ports from which the packets are copied.

To enable port mirroring:

- STEP 1** Click **Admin > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens:

Port Mirroring Page



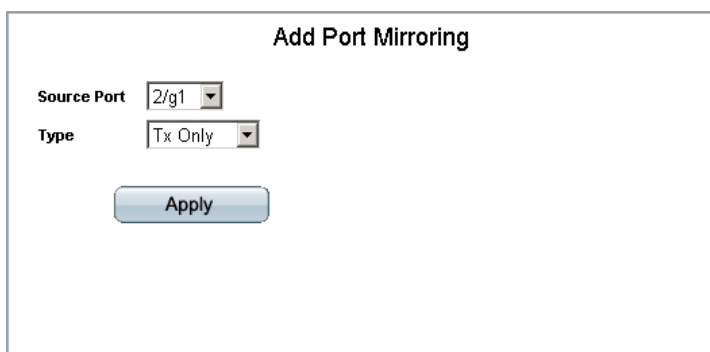
The *Port Mirroring Page* contains the following fields:

- **Destination Port** — Defines the port to which the source port's traffic is mirrored.
- **Source Port** — Defines the port from which traffic is to be analyzed.

- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
 - *RxOnly* — Defines the port mirroring for receive traffic only on the selected port.
 - *TxOnly* — Defines the port mirroring on transmitting ports. This is the default value.
 - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.
- **Status** — Indicates if the port is currently monitored. The possible field values are:
 - *Active* — Indicates the port is currently monitored.
 - *NotReady* — Indicates the port is not currently monitored.

STEP 2 Click the **Add** button. The *Add Port Mirroring Page* opens:

Add Port Mirroring Page



The screenshot shows a web interface titled "Add Port Mirroring". It contains two dropdown menus: "Source Port" with the value "2/g1" selected, and "Type" with the value "Tx Only" selected. Below these fields is a blue "Apply" button.

The *Add Port Mirroring Page* contains the following fields:

- **Source Port** — Defines the port from which traffic is to be analyzed.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
 - *RxOnly* — Defines the port mirroring on receiving ports. This is the default value.
 - *TxOnly* — Defines the port mirroring on transmitting ports.
 - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.

STEP 3 Define the relevant fields.

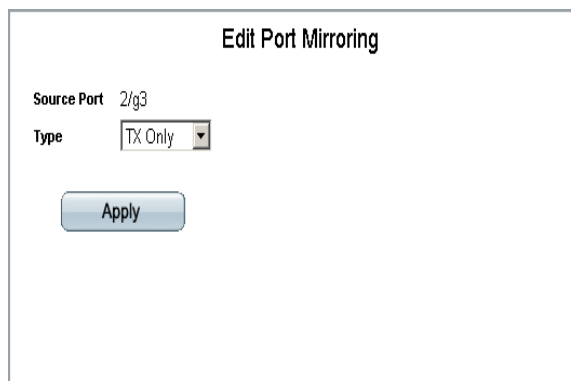
STEP 4 Click **Apply**. Port mirroring is added, and the device is updated.

Modifying Port Mirroring

STEP 1 Click **Admin > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens:

STEP 2 Click the **Edit** Button. The *Edit Port Mirroring Page* opens:

Edit Port Mirroring Page



The screenshot shows a web form titled "Edit Port Mirroring". It contains two input fields: "Source Port" with the text "2/g3" and "Type" with a dropdown menu currently set to "TX Only". Below these fields is a blue "Apply" button.

The *Edit Port Mirroring Page* contains the following fields:

- **Source Port** — Indicates the port from which traffic is to be analyzed.
- **Type** — Defines the port mode configuration for port mirroring. The possible field values are:
 - *RxOnly* — Defines the port mirroring on receiving ports. This is the default value.
 - *TxOnly* — Defines the port mirroring on transmitting ports.
 - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.

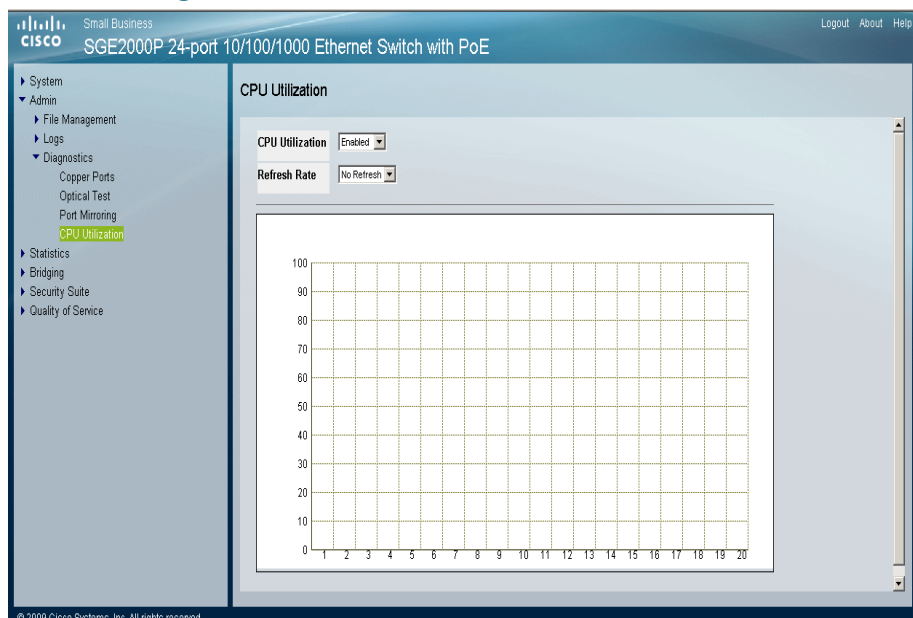
STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The Port mirroring is modified, and the device is updated.

Viewing CPU Utilization

The **CPU Utilization Page** contains information about the system's CPU utilization.

CPU Utilization Page



The **CPU Utilization Page** contains the following fields:

- **CPU Utilization** — Displays CPU resource utilization information. The possible field values are:
 - *Enabled* — Enables viewing CPU utilization information. This is the default value.
 - *Disabled* — Disables viewing the CPU utilization information.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the CPU utilization statistics are not refreshed.
 - *15 Sec* — Indicates that the CPU utilization statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the CPU utilization statistics are refreshed every 30 seconds.

- **60 Sec** — Indicates that the CPU utilization statistics are refreshed every 60 seconds.
- **Usage Percentages** — Graph's y-axis indicates the percentage of the CPU's resources consumed by the device.
- **Time** — Graph's x-axis indicates the time, in 15,30,60 second intervals, that usage samples are taken.

Managing System Logs

The System Logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors or informational messages.

Event messages have a unique format, as per the SYSLOG protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event logging.

This section contains the following :

- Enabling System Logs
- Viewing the Device Memory Logs
- Viewing the Flash Logs
- Viewing Remote Logs

Enabling System Logs

In the *Log Settings Page*, define the levels of event severity that are recorded to the system event logs.

The event severity levels are listed on this page in descending order from the highest severity to the lowest. When a severity level is selected to appear in a log, all higher severity events will automatically be selected to appear in the log. Conversely, when a security level is not selected, no lower severity events will appear in the log.

For example, if Warning is selected, all severity levels higher and including Warning will appear in the log. Additionally, no events with a lower severity level than Warning will be listed.

To define Log Global Parameters:

STEP 1 Click **Admin > Logs > Logs Settings**. The *Log Settings Page* opens.

Log Settings Page

| Severity | Console | Memory Logs | Log Flash |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Emergency | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Alert | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Critical | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Error | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Warning | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Notice | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Informational | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Debug | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The *Log Settings Page* contains the following fields:

- **Enable Logging** — Indicates if message logging is enabled globally in the device.
- **Severity** — The following are the available severity levels:
 - *Emergency* — The system is not functioning.
 - *Alert* — The system needs immediate attention.
 - *Critical* — The system is in a critical state.
 - *Error* — A system error has occurred.
 - *Warning* — A system warning has occurred.
 - *Notice* — The system is functioning properly, but system notice has occurred.
 - *Informational* — Provides device information.
 - *Debug* — Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

- **Memory Logs** — The selected Severity types will appear in chronological order in all system logs that are saved in RAM (Cache). After restart, these logs are deleted.
- **Log Flash** — The selected Severity types will be sent to the Logging file kept in FLASH memory. After restart, this log is not deleted.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. The device is updated.

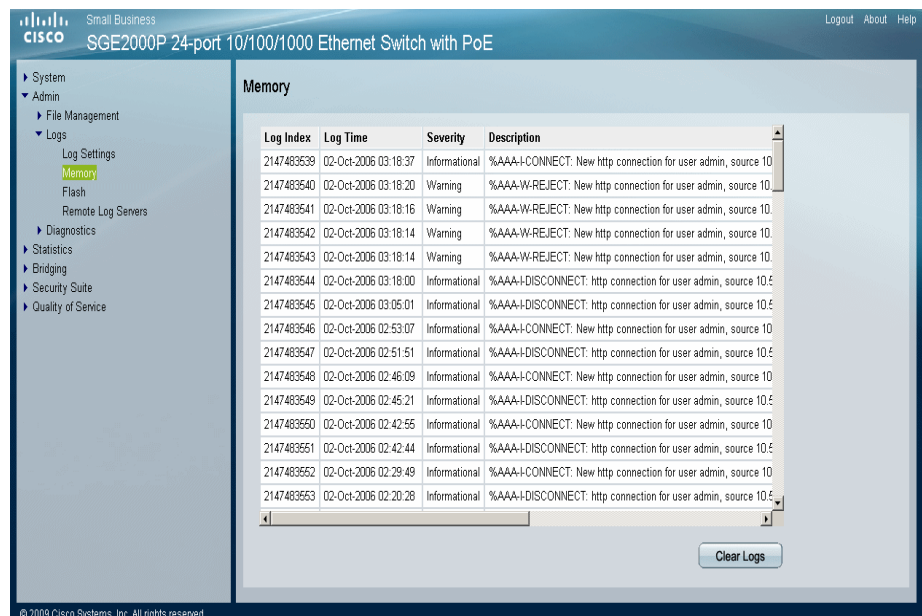
Viewing the Device Memory Logs

The *Memory Page* contains all system log entries in chronological order that are saved in RAM (Cache). After restart, these log entries are deleted.

To open the *Memory Page*:

STEP 1 Click **Admin > Logs > Memory**. The *Memory Page* opens.

Memory Page



The *Memory Page* contains the following fields:

- **Log Index** — Displays the log entry number.

- **Log Time** — Displays the time at which the log entry was generated.
- **Severity** — Displays the event severity.
- **Description** — Displays the log message text.

Clearing Message Logs

Message Logs can be cleared from the *Memory Page*. To clear the *Memory Page*:

-
- STEP 1** Click **Admin > Logs > Memory**. The *Memory Page* opens.
- STEP 2** Click the **Clear Logs** button. The message logs are cleared.
-

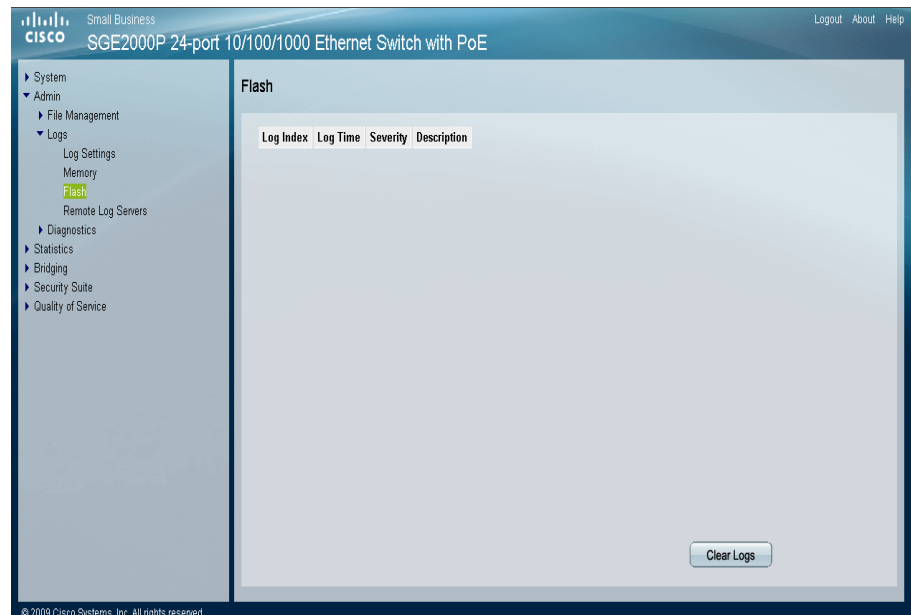
Viewing the Flash Logs

The *Flash Page* contains information about log entries saved to the Log File in FLASH, including the time the log was generated, the event severity, and a description of the log message. The Message Log is available after reboot.

To view the Flash Logs:

STEP 1 Click **Admin > Logs > Flash**. The *Flash Page* opens:

Flash Page



The *Flash Page* contains the following fields:

- **Log Index** — Displays the log entry number.
- **Log Time** — Displays the time at which the log entry was generated.
- **Severity** — Displays the event severity.
- **Description** — Displays the log message text.

Clearing Flash Logs

Flash Logs can be cleared from the *Flash Page*. To clear the *Flash Page*:

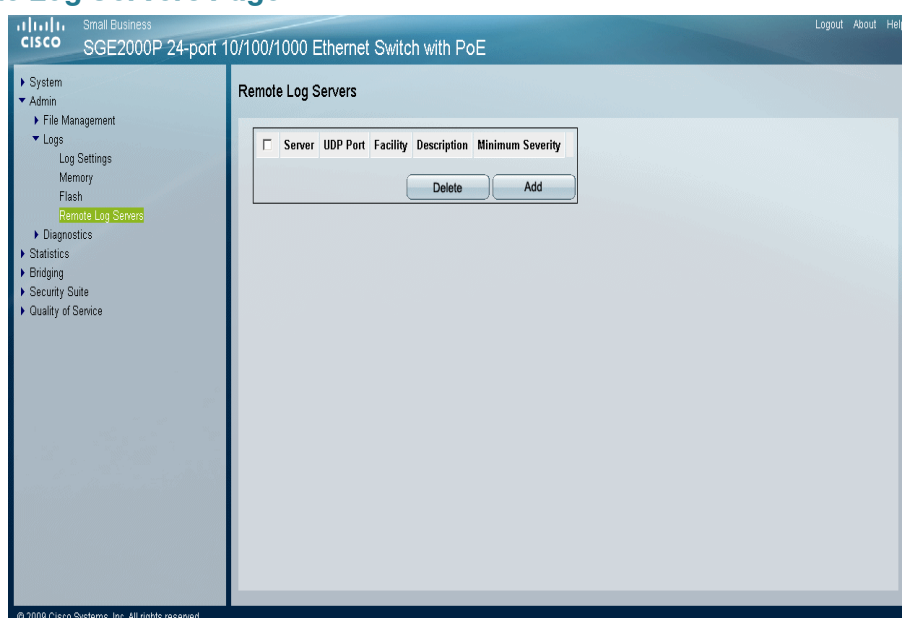
STEP 2 Click **Clear Logs**. The message logs are cleared.

Viewing Remote Logs

The *Remote Log Servers Page* contains information for viewing and configuring the Remote Log Servers. New log servers and the minimum severity level of events sent to them may be added.

STEP 1 Click **Admin > Logs > Remote Log Servers**. The *Remote Log Servers Page* opens:

Remote Log Servers Page



The *Remote Log Servers Page* contains the following fields:

- **Server** — Specifies the server IP address to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.
- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity level for logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- *Notice* — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

STEP 2 Click the **Add** button. The *Add Syslog Server Page* opens:

Add Syslog Server Page

The *Add Syslog Server Page* contains fields for defining new Remote Log Servers.

The *Add Syslog Server Page* contains the following fields:

- **Supported IP Format** — Provides the supported IP format: Version 6 or Version 4.
- **IPv6 Address type** — Indicates the IPv6 Type. The possible field values are:
 - *Link Local* — Indicates the IPv6 address is link-local.
 - *Global* — Indicates the IPv6 address is global Unicast.
- **Link Local Interface** — Indicates the Link Local Interface. The possible field values are:
 - — Indicates Link Local interface.
 - *ISATAP* — Indicates a ISATAP tunnel is a Link Local interface.
- **Log Server IP Address** — Specifies the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.

- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity level of logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

STEP 3 Define the relevant fields.

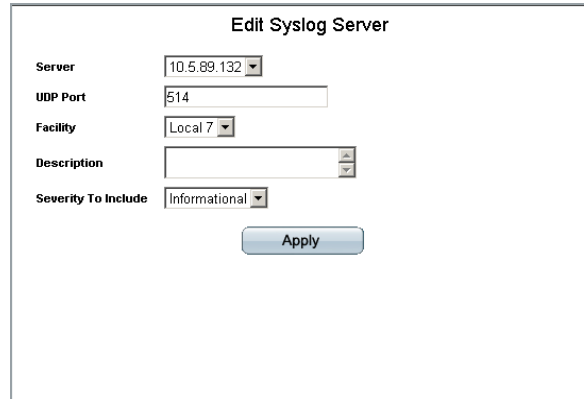
STEP 4 Click **Apply**. The *Add Syslog Server Page* closes, the syslog server is added, and the device is updated.

Modifying Syslog Server Settings

STEP 1 Click **Admin > Logs > Remote Log Servers**. The *Remote Log Servers Page* opens:

STEP 2 Click the **Edit** button. The *Edit Syslog Server Page* opens:

Edit Syslog Server Page

The screenshot shows a web form titled "Edit Syslog Server". It contains five fields: "Server" with a dropdown menu showing "10.5.89.132", "UDP Port" with a text input field containing "514", "Facility" with a dropdown menu showing "Local 7", "Description" with a text input field, and "Severity To Include" with a dropdown menu showing "Informational". Below these fields is an "Apply" button.

The *Edit Syslog Server Page* contains fields for modifying Remote Log Server settings.

The *Edit Syslog Server Page* contains the following fields:

- **Server** — Specifies the name of the Remote Log Server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.
- **Description** — Provides a user-defined server description.
- **Severity to Include** — Indicates the minimum severity level for logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.

- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Viewing Statistics

This section describes device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics. This section contains the following topics:

- Viewing Ethernet Statistics
- Managing RMON Statistics
- Managing QoS Statistics

Viewing Ethernet Statistics

The Ethernet section contains the following :

- Defining Ethernet Interface
- Viewing Etherlike Statistics
- Viewing GVRP Statistics

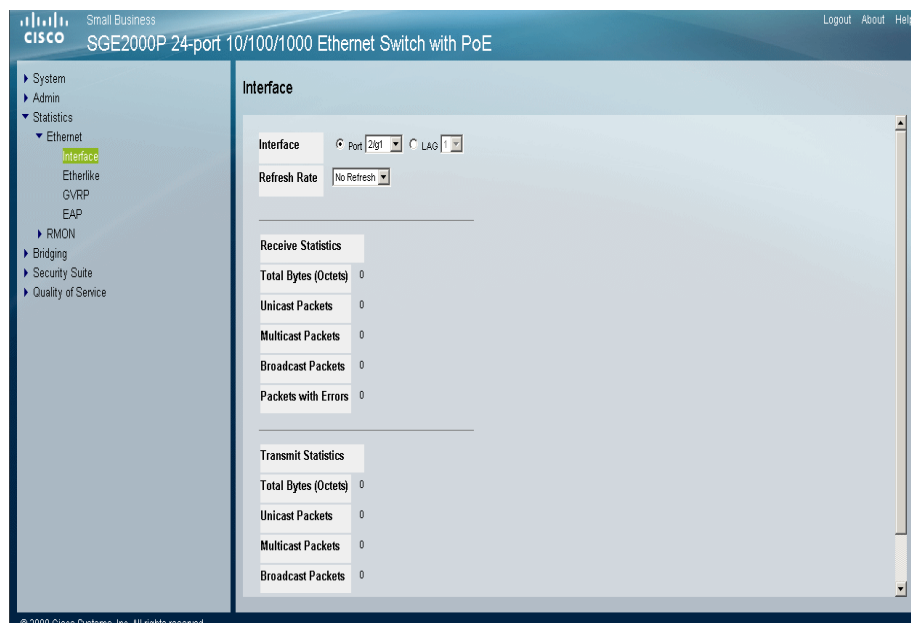
Viewing EAP Statistics

Defining Ethernet Interface

The *Ethernet Interface Page* contains statistics for both received and transmitted packets. The *Ethernet Interface Page* is divided into three areas, General Information, Receive Statistics and Transmit Statistics.

STEP 1 Click **Statistics > Ethernet > Interface**. The *Ethernet Interface Page* opens:

Ethernet Interface Page



The *Ethernet Interface Page* contains the following fields:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which Ethernet statistics are displayed.
 - *LAG* — Defines the specific LAG for which Ethernet statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the Ethernet statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the Ethernet statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the Ethernet statistics are refreshed every 60 seconds.

The Receive Statistics area contains the following fields:

- **Total Bytes (octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Unicast Packets** — Displays the number of good Unicast packets received on the interface since the page was last refreshed.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **Broadcast Packets** — Displays the number of good broadcast packets received on the interface since the page was last refreshed.
- **Packets with Errors** — Displays the number of packets with errors.

The Transmit Statistics area contains the following fields:

- **Total Bytes (octets)** — Displays the number of octets transmitted on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Unicast Packets** — Displays the number of good Unicast packets transmitted on the interface since the page was last refreshed.
- **Multicast Packets** — Displays the number of good Multicast packets transmitted on the interface since the page was last refreshed.
- **Broadcast Packets** — Displays the number of good broadcast packets transmitted on the interface since the page was last refreshed.

Resetting Interface Statistics Counters

To reset the statistics counters:

- STEP 2** Click the **Clear Counters** button. The interface statistics counters are cleared.
-

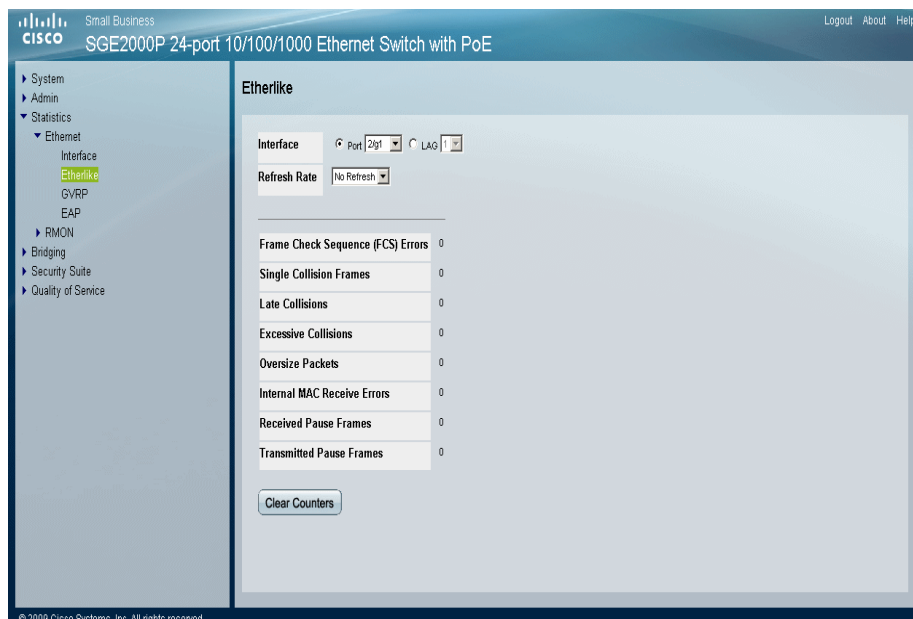
Viewing Etherlike Statistics

The *Etherlike Page* contains interface statistics.

To view Etherlike Statistics:

STEP 1 Click **Statistics > Ethernet > Etherlike**. The *Etherlike Page* opens:

Etherlike Page



The *Etherlike Page* contains Ethernet-like interface statistics. The *Etherlike Page* contains the following fields:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
 - *Port* — Defines the specific port for which Etherlike statistics are displayed.
 - *LAG* — Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the Etherlike statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the Etherlike statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the Etherlike statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the Etherlike statistics are refreshed every 60 seconds.

- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.
- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Internal MAC Receive Errors** — Displays the number of internal MAC received errors on the selected interface
- **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
- **Transmitted Pause Frames** — Displays the number of paused frames transmitted from the selected interface.

Resetting Etherlike Statistics Counters

- STEP 2** Click the **Clear Counters** button. The interface statistics counters are cleared.
-

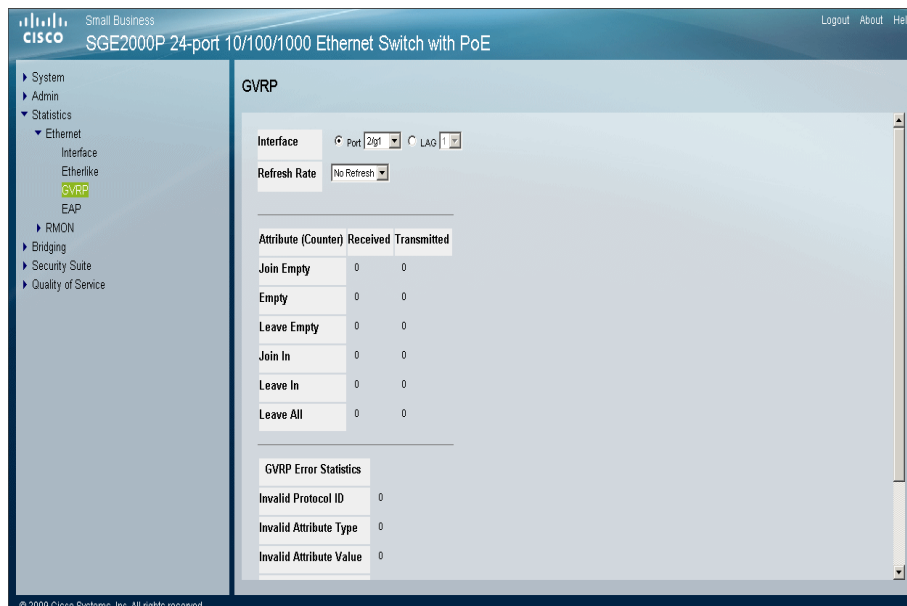
Viewing GVRP Statistics

The *GVRP Page* contains statistics for GVRP communication on the device.

To view GVRP statistics:

STEP 1 Click **Statistics > Ethernet > GVRP**. The *GVRP Page* opens:

GVRP Page



The *GVRP Page* is divided into two areas, GVRP Statistics Table and GVRP Error Statistics Table.

The following fields are relevant for both tables:

- **Interface** — Specifies the interface type for which the statistics are displayed.
 - *Port*— Indicates if port statistics are displayed.
 - *LAG*— Indicates if LAG statistics are displayed.
- **Refresh Rate** — Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the GVRP statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the GVRP statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the GVRP statistics are refreshed every 60 seconds.

The GVRP Received Transmitted Table contains the following fields:

- **Join Empty** — Displays the device GVRP Join Empty statistics.

- **Empty** — Displays the device GVRP Empty statistics.
- **Leave Empty** — Displays the device GVRP Leave Empty statistics.
- **Join In** — Displays the device GVRP Join In statistics.
- **Leave In** — Displays the device GVRP Leave in statistics.
- **Leave All** — Displays the device GVRP Leave all statistics.

The GVRP Error Statistics Table contains the following fields:

- **Invalid Protocol ID** — Displays the device GVRP Invalid Protocol ID statistics.
- **Invalid Attribute Type** — Displays the device GVRP Invalid Attribute ID statistics.
- **Invalid Attribute Value** — Displays the device GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length** — Displays the device GVRP Invalid Attribute Length statistics.
- **Invalid Event** — Displays the device GVRP Invalid Events statistics.

Resetting GVRP Statistics Counters

- STEP 2** Click **Clear Counters**. The GVRP statistics counters are cleared.
-

Viewing EAP Statistics

The *EAP Page* contains information about EAP packets received on a specific port.

To view the EAP Statistics:

STEP 1 Click **Statistics > Ethernet > EAP**. The *EAP Page* opens:

EAP Page

Small Business
Cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
 Ethernet
 Interface
 Etherlike
 GVRP
 EAP
 RMON
 Bridging
 Security Suite
 Quality of Service

EAP

Port: 2/21
Refresh Rate: No Refresh

| | |
|-----------------------------|-------------------|
| Frames Receive | 0 |
| Frames Transmit | 0 |
| Start Frames Receive | 0 |
| Log off Frames Receive | 0 |
| Respond ID Frames Receive | 0 |
| Respond Frames Receive | 0 |
| Request ID Frames Transmit | 0 |
| Request Frames Transmit | 0 |
| Invalid Frames Receive | 0 |
| Length Error Frames Receive | 0 |
| Last Frame Version | 0 |
| Last Frame Source | 00:00:00:00:00:00 |

© 2009 Cisco Systems, Inc. All rights reserved

The EAP Page contains the following fields:

- **Unit Number** — Indicates the stacking member for which the EAP statistics are displayed.
- **Port** — Indicates the port which is polled for statistics.
- **Refresh Rate** — Defines the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the EAP statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
- **Frames Receive** — Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** — Indicates the number of EAPOL frames transmitted via the port.

- **Start Frames Receive** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Request ID Frames Transmit** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Receive** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.

Last Frame Source — Indicates the source MAC address attached to the most recently received EAPOL frame.

Managing RMON Statistics

The RMON section contains the following :

- Viewing RMON Statistics
- Configuring RMON History
- To return to the RMON History Control Page, click the Interface Table button.

Viewing the RMON Events Logs

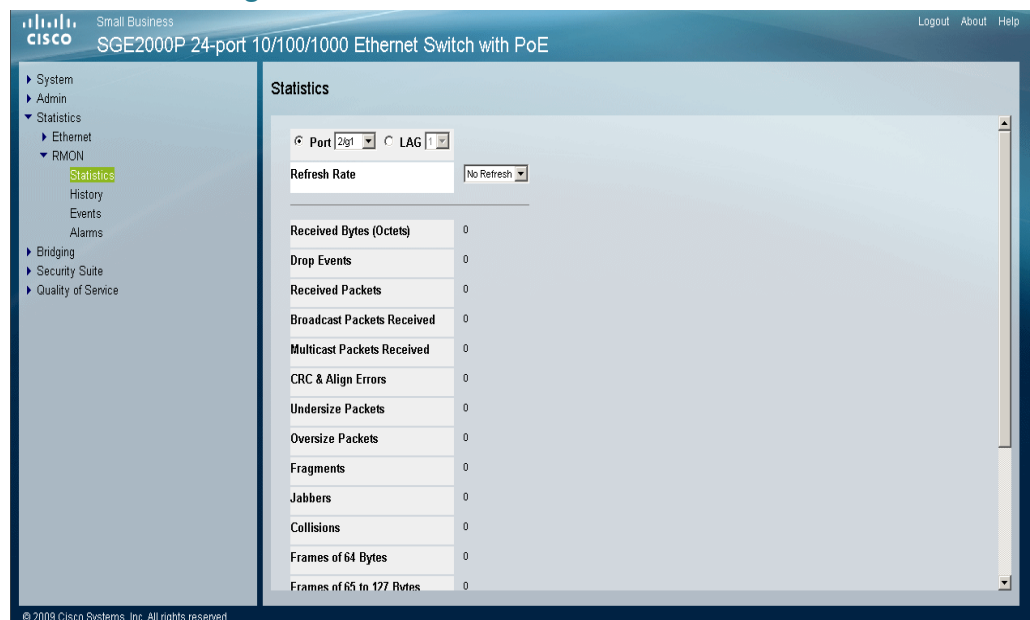
Viewing RMON Statistics

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device.

To view the RMON statistics:

STEP 1 Click **Statistics > RMON > Statistics**. The *RMON Statistics Page* opens:

RMON Statistics Page



The *RMON Statistics Page* contains the following fields:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
 - *Ports of Unit*— Defines the specific port for which RMON statistics are displayed.
 - *LAG* — Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
 - *15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.

- *30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Dropped Events** — Displays the number packets that were dropped.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the page was last refreshed.
- **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the page was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the page was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the page was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the page was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the page was last refreshed.
- **Frames of xx Bytes** — Number of frames containing the specified number of bytes that were received on the interface since the page was last refreshed.

STEP 2 Select an interface in the *Interface* field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

STEP 3 Click the **Reset Counters** button. The RMON statistics counters are cleared.

Configuring RMON History

This section contains the following topics:

- Defining RMON History Control
- Viewing the RMON History Table

Defining RMON History Control

The *RMON History Control Page* contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

To view RMON history information:

- STEP 1** 1. Click **Statistics > RMON > History**. The *RMON History Control Page* opens.

RMON History Control Page

| History Entry No. | Source Interface | Sampling Interval | Sampling Requested | Current Number of Samples | Owner |
|-------------------|------------------|-------------------|--------------------|---------------------------|-------|
| 1 | 2/g1 | 1800 | 50 | 50 | |

The *RMON History Control Page* contains the following fields:

- **History Entry No.** — Number automatically assigned to the table entry number.
- **Source Interface** — Displays the interface (port or LAG) from which the history samples were taken. The possible field values are:
 - *Ports* — Specifies the port from which the RMON information was taken.
 - *LAGs* — Specifies the LAG from which the RMON information was taken.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- **Sampling Requested** — Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples** — Displays the current number of samples taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.

- STEP 2** Click the **Add** button. The *Add RMON History Page* opens:

Add RMON History Page

Add RMON History

New History Entry 2

Source Interface ☒ Port 2/g1 ☐ LAG 1

Owner

Max No. of Samples to Keep 50

Sampling Interval 1800 (Sec)

Apply

The *Add RMON History Page* contains the following fields:

- **New History Entry** — Number automatically assigned to the table entry number.
- **Source Interface** — Select the interface (port or LAG) from which the history samples will be taken. The possible field values are:
 - *Port* — Specifies the port from which the RMON information is taken.
 - *LAG* — Specifies the LAG from which the RMON information is taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Max No. of Samples to Keep** — Indicates the number of samples to save.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

STEP 3 Define the relevant fields.

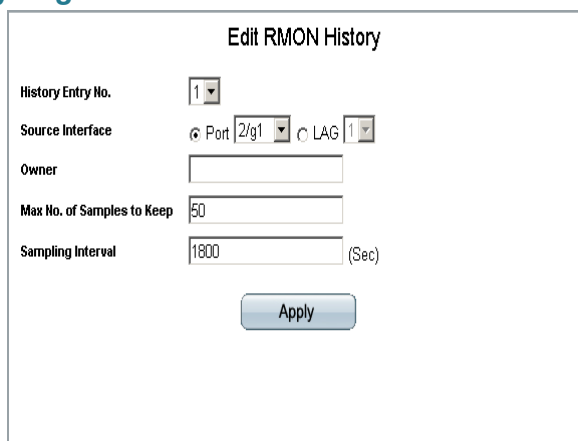
STEP 4 Click **Apply**. The entry is added to the *RMON History Control Page*, and the device is updated.

Modifying RMON History Settings

STEP 1 Click **Statistics > RMON > History**. The *RMON History Control Page* opens.

STEP 2 Click the **Edit** button. The *Edit RMON History Page* opens:

Edit RMON History Page



The screenshot shows a web-based configuration page titled "Edit RMON History". It contains several input fields: "History Entry No." with a dropdown menu showing "1"; "Source Interface" with radio buttons for "Port" (selected) and "LAG", and corresponding dropdown menus for "2/g1" and "1"; "Owner" with a text input field; "Max No. of Samples to Keep" with a text input field showing "50"; and "Sampling Interval" with a text input field showing "1800" and a unit label "(Sec)". An "Apply" button is located at the bottom right of the form.

The *Edit RMON History Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Source Interface** — Displays the interface (port or LAG) from which the history samples are taken. The possible field values are:
 - *Port* — Specifies the port from which the RMON information is taken.
 - *LAG* — Specifies the LAG from which the RMON information is taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Max No. of Samples to Keep** — Indicates the number of samples to save.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The history control settings are modified, and the device is updated.

Viewing the RMON History Table

The *RMON History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To view the RMON History Table:

STEP 1 Click **Statistics > RMON > History**. The *RMON History Control Page* opens:

STEP 2 Click the **History Table** button. The *RMON History Table Page* opens:

RMON History Table Page

Small Business
Cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

System
Admin
Statistics
Ethernet
RMON
History
Events
Alarms
Bridging
Security Suite
Quality of Service

History

History Entry No. 1
Owner

| Sample No. | Drop Events | Received Bytes (Octets) | Received Packets | Broadcast Packets | Multicast Packets | CRC Align Errors | Undersize Packets | Oversize Packets | Fragments | Jabbers | Collisions | Utilization |
|------------|-------------|-------------------------|------------------|-------------------|-------------------|------------------|-------------------|------------------|-----------|---------|------------|-------------|
|------------|-------------|-------------------------|------------------|-------------------|-------------------|------------------|-------------------|------------------|-----------|---------|------------|-------------|

Interface Table

© 2009 Cisco Systems, Inc. All rights reserved.

The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Drop Events** — Indicates the number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number dropped packets, but rather the number of times dropped packets were detected.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

- **Received Packets** — Displays the number of packets received on the interface since the page was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the page was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the page was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the page was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the page was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the page was last refreshed.
- **Utilization** — Displays the percentage of the interface utilized.

STEP 3 To return to the *RMON History Control Page*, click the **Interface Table** button.

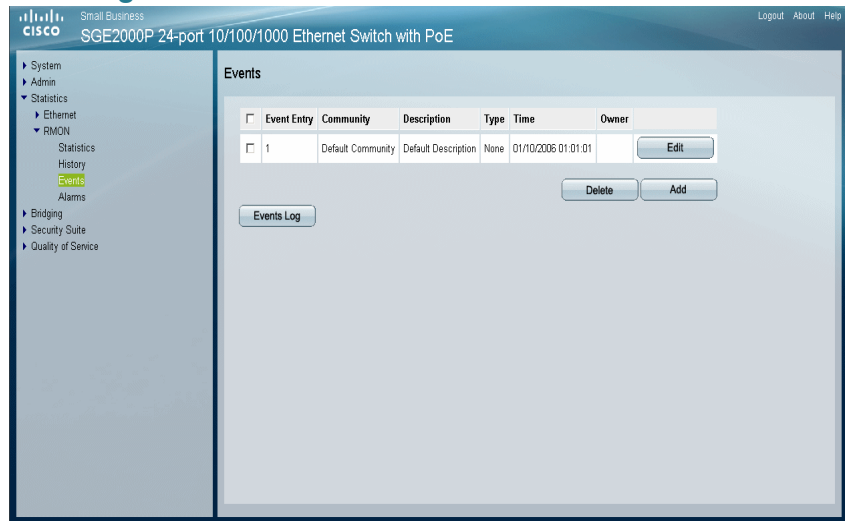
Defining RMON Events Control

The *RMON Events Page* contains fields for defining RMON events.

To view RMON events:

STEP 1 Click **Statistics > RMON > Events**. The *RMON Events Page* opens:

RMON Events Page



The *RMON Events Page* contains the following fields:

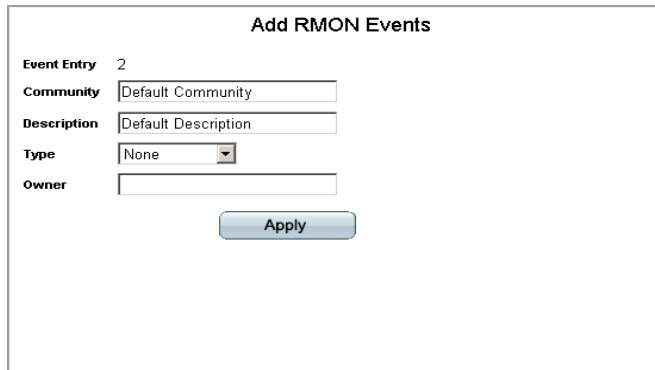
- **Event Entry** — Displays the event index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays the event description.
- **Type** — Describes the event type. Possible values are:
 - *None* — No action occurs.
 - *Log* — The device adds a log entry.
 - *Trap* — The device sends a trap.
 - *Log and Trap* — The device adds a log entry and sends a trap.
- **Time** — Displays the date and time that the event occurred.
- **Owner** — Displays the device or user that defined the event.

The **Add** button adds the configured RMON event to the Event Table.

The **Delete** button deletes the selected RMON event.

STEP 2 Click the **Add** button. The *Add RMON Events Page* opens:

Add RMON Events Page



The *Add RMON Events Page* contains the following fields:

- **Event Entry** — Indicates the event entry index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays a user-defined event description.
- **Type** — Describes the event type. Possible values are:
 - *None* — No action occurs.
 - *Log* — The device adds a log entry.
 - *Trap* — The device sends a trap.
 - *Log and Trap* — The device adds a log entry and sends a trap.
- **Owner** — Displays the device or user that defined the event.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The RMON event is added, and the device is updated.

Modifying RMON Event Log Settings

STEP 1 Click **Statistics > RMON > Events**. The *RMON Events Page* opens:

STEP 2 Click **Edit**. The *Edit RMON Events Page* opens:

Edit RMON Events Page



The screenshot shows a web form titled "Edit RMON Events". It contains the following fields:

- Event Entry No.**: A dropdown menu with the value "1" selected.
- Community**: A text input field containing "Default Community".
- Description**: A text input field containing "Default Description".
- Type**: A dropdown menu with the value "None" selected.
- Owner**: An empty text input field.
- Apply**: A button located at the bottom right of the form.

The *Edit RMON Events Page* contains the following fields:

- **Entry Event No.** — Displays the event entry index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
 - *None* — No action occurs.
 - *Log* — The device adds a log entry.
 - *Trap* — The device sends a trap.
 - *Log and Trap* — The device adds a log entry and sends a trap.
- **Owner** — Displays the device or user that defined the event.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The event control settings are modified, and the device is updated.

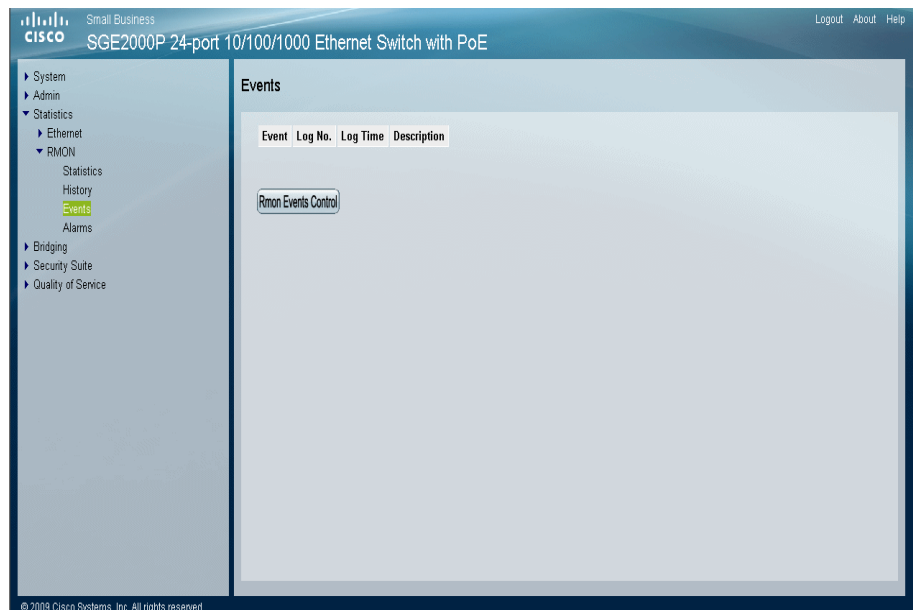
Viewing the RMON Events Logs

The *RMON Events Log Page* contains a list of RMON events.

STEP 1 Click **Statistics > RMON > Events**. The *RMON Events Page* opens:

STEP 2 Click the **Events Log** button. The *RMON Events Log Page* opens:

RMON Events Log Page



The *RMON Events Log Page* contains the following fields:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.**— Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

To return to the *RMON Events Page*, click the **RMON Events Control** button.

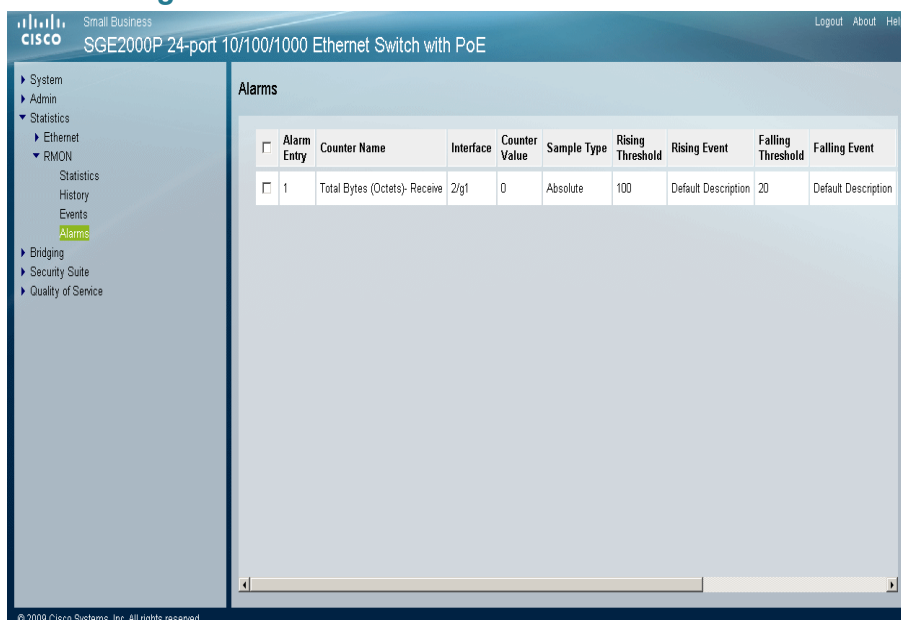
Defining RMON Alarms

The *RMON Alarms Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To set RMON alarms:

STEP 1 Click **Statistics > RMON > Alarms**. The *RMON Alarms Page* opens:

RMON Alarms Page



The *RMON Alarms Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Counter Name** — Displays the selected MIB variable.
- **Interface** — Displays the interface (port or LAG) for which RMON statistics are displayed. The possible field values are:
 - *Port* — Displays the RMON statistics for the selected port.
 - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Value** — Displays the current counter value for the particular alarm.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
 - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
 - *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.

- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the RMON Events page.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
 - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
 - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
 - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval (Sec)** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

STEP 2 Click the **Add** button. The Add RMON Alarm Page opens:

Add RMON Alarm Page

The screenshot shows the 'Add RMON Alarm' configuration page. It contains the following fields and options:

- Alarm Entry:** 1
- Interface:** Port 2/g1 (selected), LAG 1 (available)
- Counter Name:** Total Bytes (Octets) Receive (selected)
- Sample Type:** Absolute (selected)
- Rising Threshold:** 100
- Rising Event:** 1 - Default Description (selected)
- Falling Threshold:** 20
- Falling Event:** 1 - Default Description (selected)
- Startup Alarm:** Rising and Falling (selected)
- Interval:** 100
- Owner:** (empty text field)
- Apply:** (button)

The *Add RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Interface** — Displays the interface (port or LAG) for which RMON statistics are displayed. The possible field values are:
 - *Port* — Displays the RMON statistics for the selected port.
 - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Name** — Displays the selected MIB variable.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
 - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the *RMON Events Page*.

- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
 - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
 - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
 - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The RMON alarm is added, and the device is updated.

Modifying RMON Alarm Settings

STEP 1 Click **Statistics > RMON > Alarms**. The *RMON Alarms Page* opens:

STEP 2 Click the **Edit** Button. The *Edit RMON Alarm Page* opens:

Edit RMON Alarm Page

Edit RMON Alarm

Alarm Entry: 1

Interface: ☒ Port 2/g1 ☐ LAG 1

Counter Name: Total Bytes (Octets)- Receive

Counter Value: 0

Sample Type: Absolute

Rising Threshold: 100

Rising Event: 1 - Default Description

Falling Threshold: 20

Falling Event: 1 - Default Description

Startup Alarm: Rising and Falling

Interval (Sec): 100

Owner:

Apply

The *Edit RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Interface** — Displays the interface (port or LAG) for which RMON statistics are displayed. The possible field values are:
 - *Port* — Displays the RMON statistics for the selected port.
 - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Name** — Displays the selected MIB variable.
- **Counter Value** — Displays the current counter value for the particular alarm.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
 - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the *RMON Events Page*.

- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
 - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
 - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
 - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The RMON alarms are modified, and the device is updated.

Managing QoS Statistics

The QoS Statistics section contains the following :

- Viewing Policer Statistics
- Viewing Aggregated Policer Statistics
- Viewing Queues Statistics

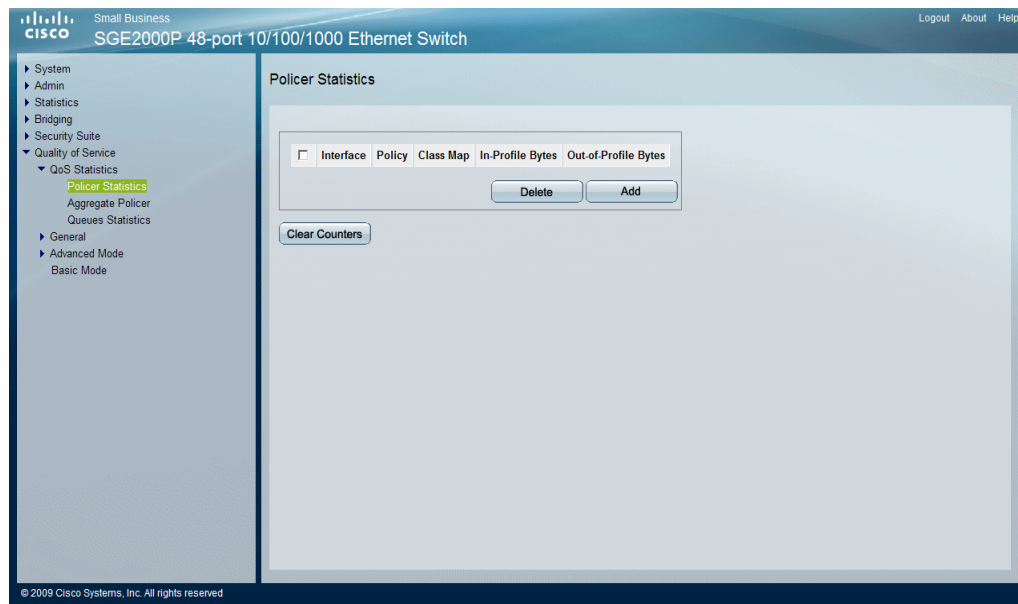
Viewing Policer Statistics

The *Policer Statistics Page* indicates the amount of in-profile and out-of-profile packets that are received on an interface.

To view policer statistics:

- STEP 1** Click **Quality of Service > QoS Statistics > Aggregated Policer Statistics**. The *Policer Statistics Page* opens:

Policer Statistics Page



The *Policer Statistics Page* contains the following fields:

- **Interface** — Displays the interface (port or LAG) for which Policer statistics are displayed. The possible field values are:
 - *Ports* — Displays the Policer statistics for the selected port.
 - *LAGs* — Displays the Policer statistics for the selected LAG.
- **Policy** — Displays the policy for which the statistics are displayed.
- **Class Map** — Displays the class map for which the statistics are displayed.
- **In-Profile Bytes** — Displays the total number in-profile bytes received on the interface.
- **Out-of-Profile Bytes** — Displays the total number out-profile bytes received on the interface.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The Police Statistics accumulation configuration is modified, and the device is updated.
-

Viewing Aggregated Policer Statistics

To view Aggregated Policer Statistics: To view Aggregated Policer Statistics

- STEP 1** Click **Quality of Service > QoS Statistics >Aggregate Polcier**. The *Aggregate Policer Page* opens:

The window contains the following fields:

- **Aggregate Policer** — Indicates the port or LAG on which the packets were received.
- **In-profile bytes** — Displays the total number of in-profile packets that were received.
- **Out-of-profile bytes** — Displays the total number of out-of-profile packets that were received.

Resetting Aggregate Policer Statistics Counters

- STEP 1** Click **Quality of Service > QoS Statistics >Aggregated Policer**. The *The window contains the following fields:* opens:
- STEP 2** Click **Clear Counters**. The Aggregate Policer statistics counters are cleared.

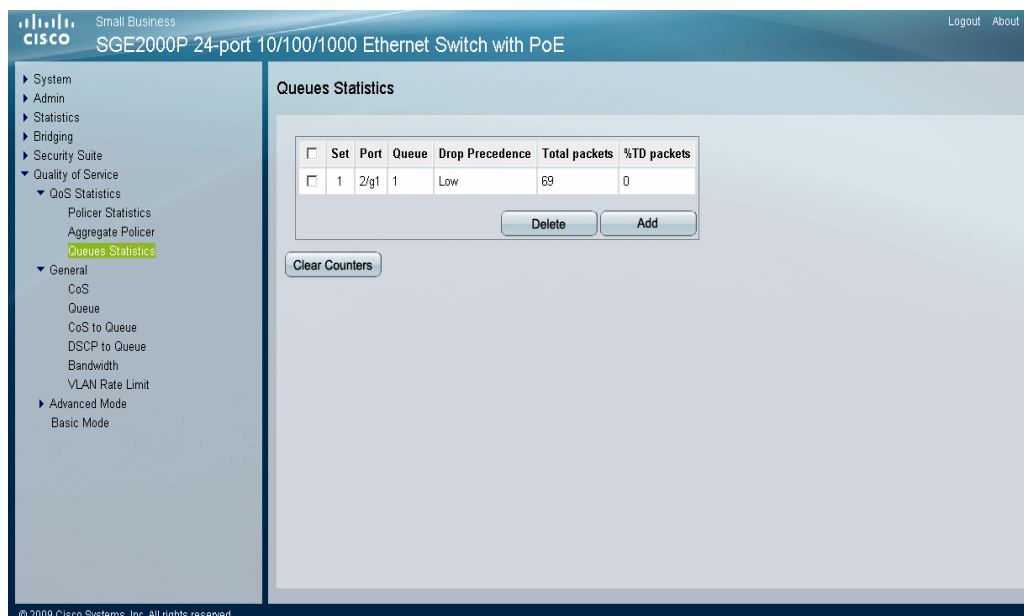
Viewing Queues Statistics

The *Queues Statistics Page* contains parameters for viewing queue statistics including statistics forwarded and dropped packets based on interface, queue, and drop precedence. The *Queues Statistics Page* is applicable to GE devices only.

To view Queues Statistics:

STEP 1 Click **Quality of Service > QoS Statistics > Queues Statistics**. The *Queues Statistics Page* opens:

Queues Statistics Page



The *Queues Statistics Page* contains the following fields:

- **Set** — Displays the counter set. The possible field values are:
 - Set 1 — Displays the statistics for Set 1. Set 1 contains all interfaces and all queues with a high DP.
 - Set 2 — Displays the statistics for Set 2. Set 2 contains all interfaces and all queues with a low DP.
- **Port** — Displays the port for which the queue statistics are displayed.
- **Queue** — Displays the queue from which packets were forwarded or tail dropped.
- **Drop Precedence** — Displays the drop precedence assigned to the packets forwarded or tail dropped for which statistics are displayed.
- **Total packets** — Displays the total number of packets forwarded or tail dropped.
- **%TD packets** — Displays the percentage of packets that were tail dropped.

STEP 2 Click the **Add** button. The *Add Queues Statistics Page* opens:

Add Queues Statistics Page

The screenshot shows a web form titled "Add Queues Statistics". It contains the following fields and controls:

- Select Counter Set**: A dropdown menu with "Set 1" selected.
- Interface**: A group of controls including three radio buttons ("Unit No.", "Port", "All Ports") and two dropdown menus. "Unit No." is selected, showing "1" in its dropdown. "Port" is also selected, showing "1/g1" in its dropdown.
- Queue**: A dropdown menu with "1" selected.
- Drop Precedence**: A dropdown menu with "Low" selected.
- Apply**: A button located at the bottom right of the form.

The *Add Queues Statistics Page* contains the following fields:

- **Select Counter Set** — Selects the counter set.
- **Interface** — Defines the ports for which statistics are displayed. The possible field values are:
 - *Unit No.* — Selects the unit number.
 - *Port* — Selects the port on the selected unit number for which statistics are displayed.
 - *All Ports* — Specifies that statistics are displayed for all ports.
- **Queue** — Selects the queue for which statistics are displayed.
- **Drop Precedence** — Selects the drop precedence assigned to the packets forwarded or tail dropped for which statistics are displayed.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The Queue Statistics counter is added, and the device is updated.

Resetting Queues Statistics Counters

STEP 1 Click **Quality of Service > QoS Statistics > Queues Statistics**. The *Queues Statistics Page* opens:

Click **Clear Counters**. The Queues statistics counters are cleared.

Aggregating Ports

Link Aggregated Groups (LAGs) optimize port usage by linking a group of ports together to form a single aggregated group. Link aggregated groups multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

The device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAGs negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them. Ensure the following:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to 64 LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.
- Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

This section contains information for configuring ports and contains the following topics:

- Defining LAG Management
- Defining LAG Settings

- Configuring LACP

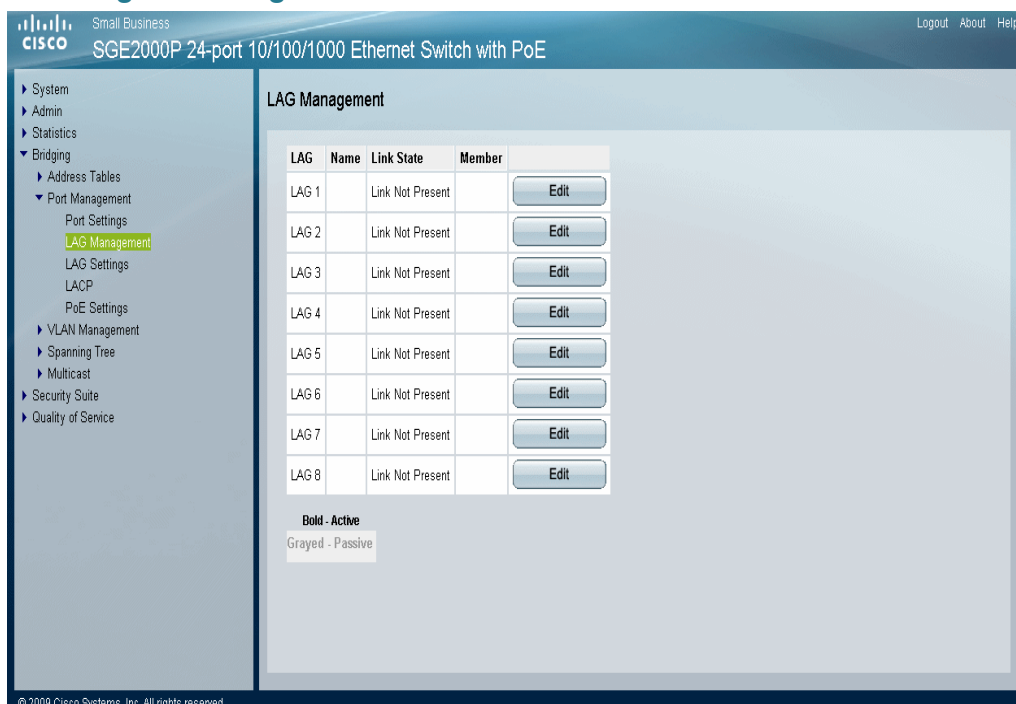
Defining LAG Management

Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

To define LAG management:

- STEP 1** Click **Bridging > Port Management > LAG Management**. The *LAG Management Page* opens:

LAG Management Page



The *LAG Management Page* contains the following fields.

- **LAG** — Displays the LAG number.
- **Name** — Displays the LAG name.
- **Link State** — Displays the link operational status.
- **Member** — Displays the ports configured to the LAG.

STEP 2 Define the relevant fields.

STEP 3 Click **Apply**. LAG Management is defined, and the device is updated.

Modifying LAG Membership

STEP 1 Click **Bridging > Port Management > LAG Management**. The *LAG Management Page* opens:

STEP 2 Click the **Edit** button. The *Edit LAG Membership Page* opens:

Edit LAG Membership Page

The screenshot shows the 'Edit LAG Membership' configuration page. At the top, the title 'Edit LAG Membership' is centered. Below the title, there are three configuration fields: 'LAG' with a dropdown menu currently set to '1', 'LAG Name' with an empty text input box, and 'LACP' with an unchecked checkbox. A horizontal line separates these fields from the membership configuration section below. This section contains two main areas: 'Port List' on the left, which is a scrollable list of network interfaces (2/g1 through 2/g8), and 'LAG Members' on the right, which is an empty box for the selected members. Between these two areas are two small buttons, '>>' and '<<', for moving ports between the lists. At the bottom center of the page is a large 'Apply' button.

The *Edit LAG Membership Page* contains the following fields.

- **LAG** — Displays the LAG number.
- **LAG Name** — Displays the LAG name.
- **LACP** — Indicates that LACP is enable on the LAG.
- **Unit Number** — Displays the stacking member for which LAG information is defined.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The LAG membership is defined, and the device is updated.

Defining LAG Settings

Link Aggregated Groups optimize port usage by linking a group of ports together to form a single aggregated group. Link aggregated groups multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

The *LAG Settings Page* contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and eight LAGs per system.

The *LAG Settings Page* varies, depending on whether the device is in Layer 2 or Layer 3 mode (definable on the device through the CLI interface).

Layer 2 devices support Private VLAN Edge, which can be enabled for specific LAGs on the *Edit LAG Settings Page*.

STEP 1 Click **Bridging > Port Management > LAG Settings**. The *LAG Settings Page* opens:

LAG Settings Page

Small Business
cisco SGE2000P 24-port 10/100/1000 Ethernet Switch with PoE

Logout About Help

System
Admin
Statistics
Bridging
Address Tables
Port Management
Port Settings
LAG Management
LAG Settings
LACP
PoE Settings
VLAN Management
Spanning Tree
Multicast
Security Suite
Quality of Service

LAG Settings

Copy from Entry Number to Entry Number(s) (Example: 1,3,5-10)

| # | LAG | Description | Type | Status | Speed | Auto Negotiation | Flow Control | PVE | |
|---|-------|-------------|------|--------|-------|------------------|--------------|-----|------|
| 1 | LAG 1 | | | | | | | | Edit |
| 2 | LAG 2 | | | | | | | | Edit |
| 3 | LAG 3 | | | | | | | | Edit |
| 4 | LAG 4 | | | | | | | | Edit |
| 5 | LAG 5 | | | | | | | | Edit |
| 6 | LAG 6 | | | | | | | | Edit |
| 7 | LAG 7 | | | | | | | | Edit |
| 8 | LAG 8 | | | | | | | | Edit |

Apply

© 2009 Cisco Systems, Inc. All rights reserved

The *LAG Settings Page* contains the following fields:

- **Copy From Entry Number** — Copies the LAG configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied LAG configuration to the specified table entry.
- **LAG** — Displays the LAG ID number.
- **Description** — Displays the user-defined port name.
- **Type** — Displays the port types that comprise the LAG.
- **Status** — Indicates if the LAG is currently operating.
- **Speed** — Displays the configured speed at which the LAG is operating.
- **Auto Negotiation** — Displays the current Auto Negotiation setting. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, and flow control abilities to its partner.
- **Flow Control** — Displays the current Flow Control setting. Flow control may be *enabled*, *disabled*, or be in *auto negotiation* mode. *Flow control* operates when the ports are in full duplex mode.
- **PVE** — Indicates that this LAG's ports are protected by an uplink, so that the forwarding decisions are overwritten by those of the ports that protect them. PVE is supported in Layer 2 mode.

STEP 2 Click the **Edit** button. The *Edit LAG Page* opens:

Edit LAG Page

Edit LAG

LAG: 1

Description:

LAG Type:

Admin Status: Up

Current LAG Status: Active

Reactivate Suspended LAG: ☐

Operational Status: Active

Admin Auto Negotiation: Enable

Current Auto Negotiation:

Admin Advertisement: ☒ Max Capability ☐ 10 Full ☐ 100 Full ☐ 1000 Full

Current Advertisement: Unknown

Neighbor Advertisement: Unknown

Admin Speed: 10M

Current LAG Speed:

Admin Flow Control: Disable

Current Flow Control:

PVE: None

Apply

The *Edit LAG Page* contains the following fields:

- **LAG** — Displays the LAG ID number.
- **Description** — Displays the user-defined port name.
- **LAG Type** — Indicates the port types that comprise the LAG.
- **Admin Status** — Enables or disables traffic forwarding through the selected LAG.
- **Current LAG Status** — Indicates if the LAG is currently operating.
- **Reactivate Suspended LAG** — Reactivates a port if the LAG has been disabled through the locked port security option or through Access Control List configurations.
- **Operational Status** — Indicates whether the LAG is currently operational or non-operational.
- **Admin Auto Negotiation** — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to

advertise its transmission rate, and flow control (the flow control default is disabled) abilities to its partner.

- **Current Auto Negotiation** — Displays the current Auto Negotiation setting.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the LAG. The possible field values are:
 - *Max Capability* — Indicates that all LAG speeds and Duplex mode settings can be accepted.
 - *10 Full* — Indicates that the LAG is advertising a 10 Mbps speed and full Duplex mode setting.
 - *100 Full* — Indicates that the LAG is advertising a 100 Mbps speed and full Duplex mode setting.
 - *1000 Full* — Indicates that the LAG is advertising a 1000 Mbps speed and full Duplex mode setting.
- **Current Advertisement** — Indicates the admin advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — The neighbor LAG (the LAG to which the selected interface is connected) advertises its capabilities to the LAG to start the negotiation process. The possible values are those specified in the *Admin Advertisement* field.
- **Admin Speed** — The configured speed at which the LAG is operating.
- **Current LAG Speed** — The current speed at which the LAG is operating.
- **Admin Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the LAG.
- **Current Flow Control** — The user-designated Flow Control setting.
- **PVE** — Indicates if this LAG's ports are protected by an uplink, so that the forwarding decisions are overwritten by those of the ports that protect them. PVE is supported in Layer 2 mode.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.

Configuring LACP

Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

Aggregated Links can be manually setup or automatically established by enabling *Link Aggregation Control Protocol (LACP)* on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

To define LACP:

STEP 1 Click **Bridging > Port Management > LACP**. The *LACP Page* opens:

LACP Page

The screenshot shows the LACP configuration page. On the left is a navigation menu with options like System, Admin, Statistics, Bridging, Address Tables, Port Management, Port Settings, LAG Management, LAG Settings, LACP, PoE Settings, VLAN Management, Spanning Tree, Multicast, Routing, Security Suite, and Quality of Service. The LACP section is highlighted. The main content area has a title 'LACP' and a 'LACP System Priority' field set to 1. Below that is a 'Unit Number' dropdown set to 1. A table lists 10 ports (1/e1 to 1/e10) with 'Port Priority' 1 and 'LACP Timeout' Long. Each row has an 'Edit' button.

| Port | Port Priority | LACP Timeout | |
|-------|---------------|--------------|------|
| 1/e1 | 1 | Long | Edit |
| 1/e2 | 1 | Long | Edit |
| 1/e3 | 1 | Long | Edit |
| 1/e4 | 1 | Long | Edit |
| 1/e5 | 1 | Long | Edit |
| 1/e6 | 1 | Long | Edit |
| 1/e7 | 1 | Long | Edit |
| 1/e8 | 1 | Long | Edit |
| 1/e9 | 1 | Long | Edit |
| 1/e10 | 1 | Long | Edit |

The *LACP Page* contains fields for configuring LACP LAGs.

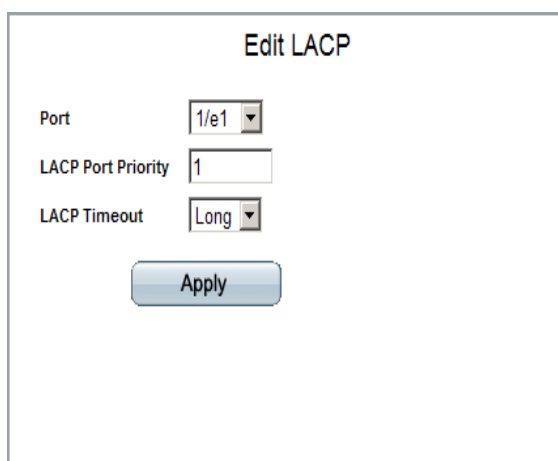
- **LACP System Priority** — Indicates the global LACP priority value. The possible range is 1- 65535. The default value is 1.
- **Unit Number** — Displays the stacking member for which LACP information is defined.
- **Port** — Defines the port number to which timeout and priority values are assigned.

- **Port Priority** — Defines the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Administrative LACP timeout. The possible field values are:
 - *Short* — Defines a short timeout value.
 - *Long* — Defines a long timeout value. This is the default value.

Modify LACP Parameter Settings

STEP 2 Click the **Edit** button. The *Edit LACP Page* opens:

Edit LACP Page

The screenshot shows a web interface titled "Edit LACP". It contains three configuration fields: "Port" with a dropdown menu showing "1/e1", "LACP Port Priority" with a text input field containing the number "1", and "LACP Timeout" with a dropdown menu showing "Long". Below these fields is a blue "Apply" button.

The *Edit LACP Page* contains the following fields:

- **Port** — Defines the port number to which timeout and priority values are assigned.
- **LACP Port Priority** — Defines the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Administrative LACP timeout. The possible field values are:
 - *Short* — Defines a short timeout value.

STEP 3 Define the relevant fields.

STEP 4 Click **Apply**. The device is updated.