LINKSYS®

A Division of Cisco Systems, Inc.

# SFE1000P 8-port 10/100 Ethernet Switch with PoE Reference Guide

March 2008

SFE1000P 8-port 10/100 Ethernet Switch with PoE Reference Guide

Specifications are subject to change without notice.

## Document Revision History

| Revision | Date | Description |
|---|---|---|
| 1.0 | March 2008 | Initial release |

# Preface

## Audience

This publication is designed for people who have some experience installing networking equipment such as routers, hubs, servers, and switches. We assume the person installing and troubleshooting the SFE1000P is familiar with electronic circuitry and wiring practices and has experience as an electronic or electromechanical technician.

## Purpose

This guide documents the features of the Linksys Business Series SFE1000P Gigabit Ethernet Switch (SFE1000P). It describes the selections available on the administration screens of the SFE1000P, and provides configuration information.

## Organization

This guide is organized into the following chapters:

- Chapter 2, "Getting Started,"is an introduction to the user interface.
- Chapter 3, "Managing Device Information,"defines both basic and advanced system information.
- Chapter 4, "Managing Power-over-Ethernet Devices,"describes configuring PoE settings.
- Chapter 5, "Configuring Device Security,"describes password management, defining authentication, access method, traffic control, 802.1x protocols, access control, and Denial of service prevention.
- Chapter 6, "Configuring Device Interfaces,"describes defining port settings, LAG management, LAG settings, and configuring LACP.
- Chapter 7, "Configuring VLANs," defines VLAN properties, VLAN memberships, interface settings, and GVRP settings.
- Chapter 8, "Configuring IP Information," provides information for defining device IP addresses.
- Chapter 9, "Defining Address Tables," contains information for defining both static and dynamic Forwarding Database entries.
- Chapter 10, "Configuring Multicast Forwarding," contains information on configuring IGMP snooping, defining multicast bridging groups, and multicast forwarding.
- Chapter 11, "Configuring Spanning Tree," contains information on configuring Spanning Tree Protocol with classic STP, Rapid STP, and Multiple STP.
- Chapter 12, "Configuring SNMP," describes SNMP security and define trap management.

- Chapter 13, "Configuring Quality of Service," shows how to define Quality of Service general settings, advanced mode settings, and basic mode settings. It also describes configuring policy tables.
- Chapter 14, "Managing System Files," describes working with file management, logs, and diagnostics.
- Chapter 15, "Managing System Logs," shows how to enable system logs, view device memory logs, flash logs, and remote logs.
- Chapter 16, "Configuring System Time," provides information for configuring the system time, and includes defining system time, SNTP settings, and SNTP authentication.
- Chapter 17, "Viewing Statistics," describes viewing and managing device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics.
- Chapter 18, "Managing Device Diagnostics," contains information for configuring port mirroring, running cable tests, and viewing device operational information.

# Getting Started

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

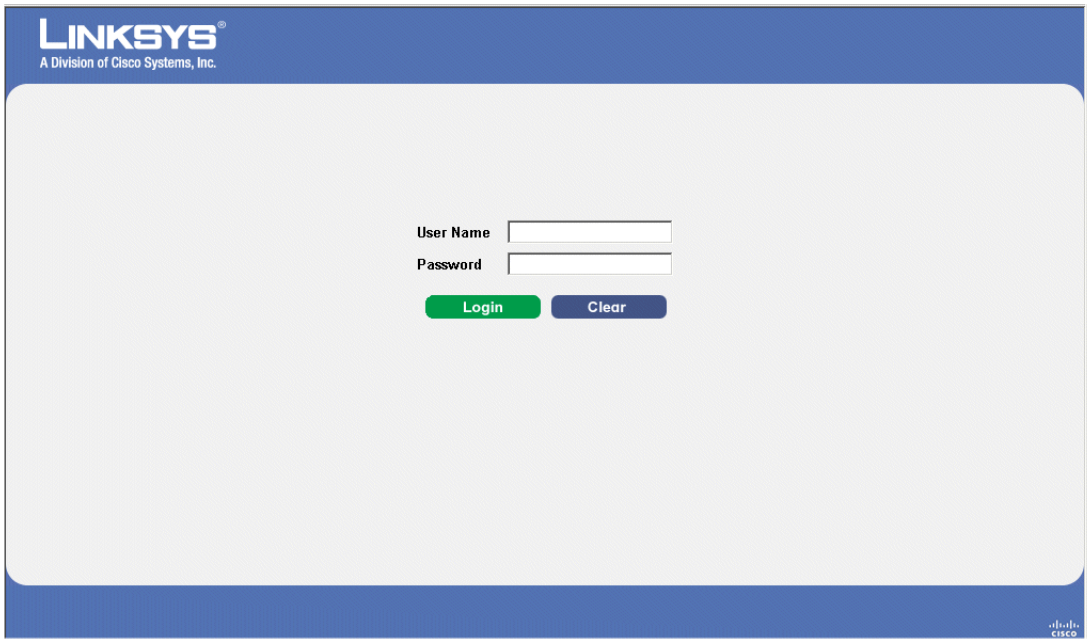
- Starting the Application
- Understanding the Interface
- Using the Linksys Management Buttons
- Using Screen and Table Options
- Resetting the Device
- Logging Off The Device

## Starting the Application

This section contains information for starting the Linksys User Interface.

**NOTE:** By default, the IP address of the device is assigned dynamically. The IP address can be changed

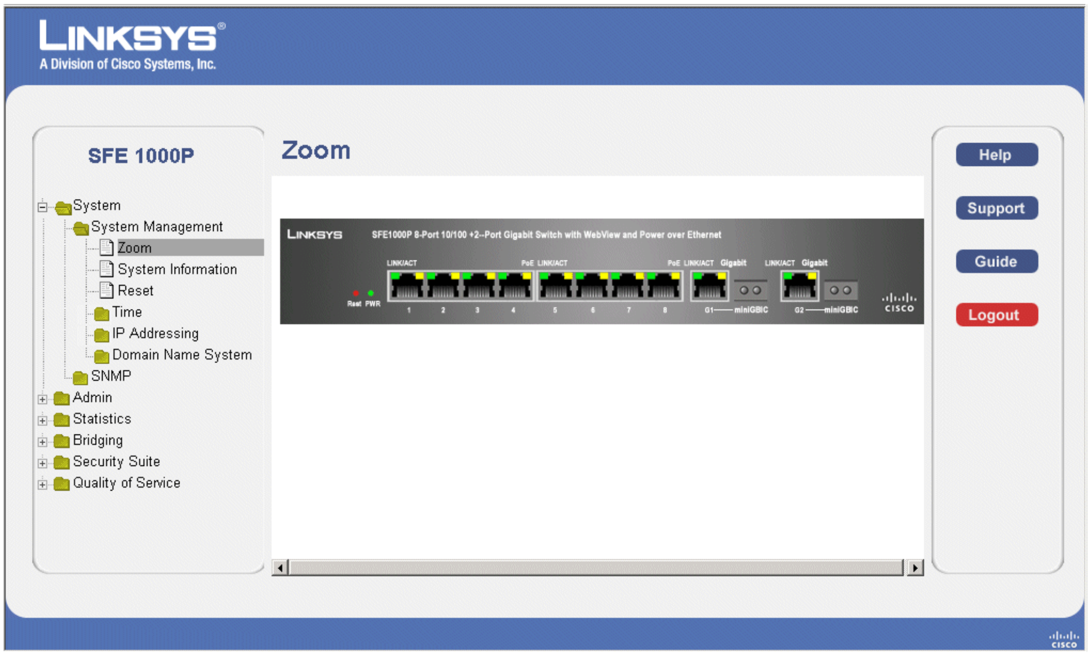
***Enter Network Password Page***



Enter a user name and password. The default user name is "admin". The device is not configured with a default password, and can be configured without entering a password. Passwords are both case sensitive and alpha-numeric.

**NOTE:** If you have logged in automatically via the Service Router user interface, the Tree and Device views appear and allow you to navigate through the various areas of the web interface. However, the following page will appear within the frame provided by the Service Router user interface.

***Embedded Web System Home Page***



## Understanding the Interface

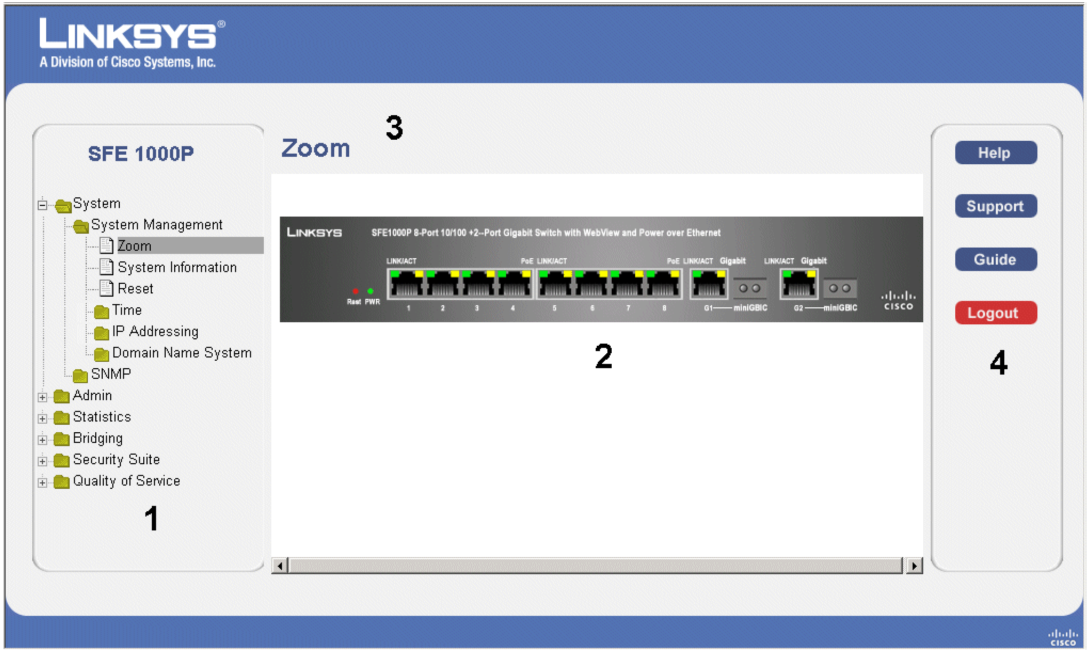
The following table lists the interface components with their corresponding numbers:

### 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. |

| Component | Description |
|---|---|
| 3 Table Area | The Table area enables navigating through the different device features. Click the tabs to view all the components under a specific feature. |
| 4 EWS Information | The EWS information tabs provide access to the online help, contains information about the EWS. |

***Linksys User Interface Components***



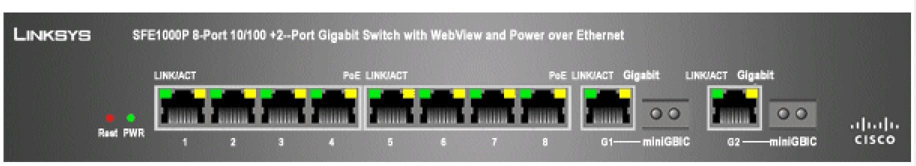
This section provides the following additional information:

- **Device Representation** — Provides an explanation of the Linksys user interface buttons, including both management buttons and task icons.
- **Using the Linksys Management Buttons** — Provides instructions for adding, modifying, and deleting device parameters.

## Device Representation

The Linksys home page displays a graphical representation of the device:

***Device Representation***



The Linksys home page contains a graphical SFE1000 and SFE1000P front panel illustration.

# Using the Linksys Management Buttons

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

***Device Management Buttons***

| Button Name | Button | Description |
|---|---|---|
| Apply | Apply | Applies changes to the device. |
| Clear Counters | Clear Counters | Clears statistic counters |
| Clear Logs | Clear Logs | Clears log files |
| Add | Add | Opens an Add page |
| Delete | Delete | Removes entries from tables |
| Reset | Reset | Resets the setllings of a selected port to the default settings |
| Test | Test | Performs cable tests immediately. |

# Using Screen and Table Options

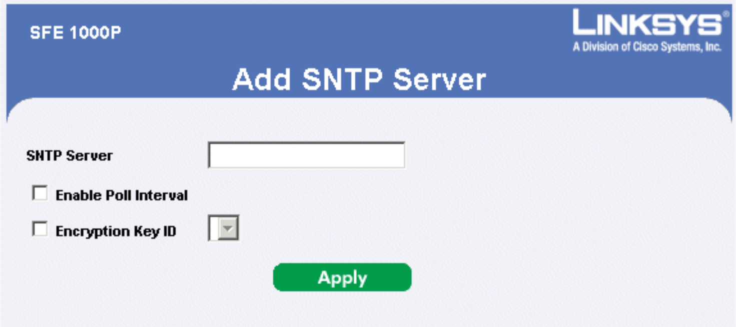
Linksys contains screens and tables for configuring devices. This section contains the following topics:

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

## Adding Device Information

User defined information can be added to specific EWS pages, by opening a new Add page.

***Add SNTP Server***



SNTP Server

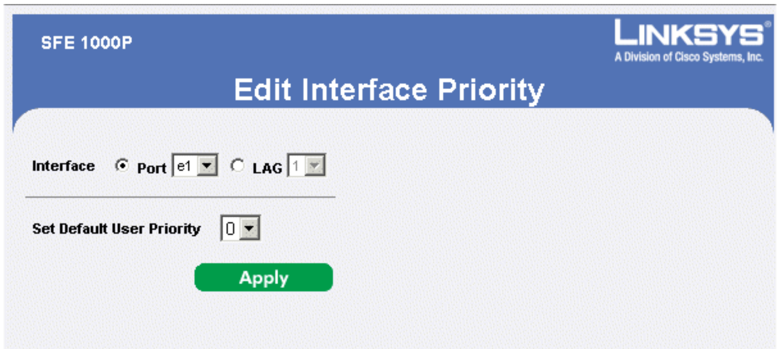
□ Enable Poll Interval

□ Encryption Key ID

## Modifying Device Information

User defined information can be modified on specific EWS pages, by opening the appropriate Edit page.

***Edit Interface Priority***



Interface ● Port e1 ○ LAG 1

Set Default User Priority 0

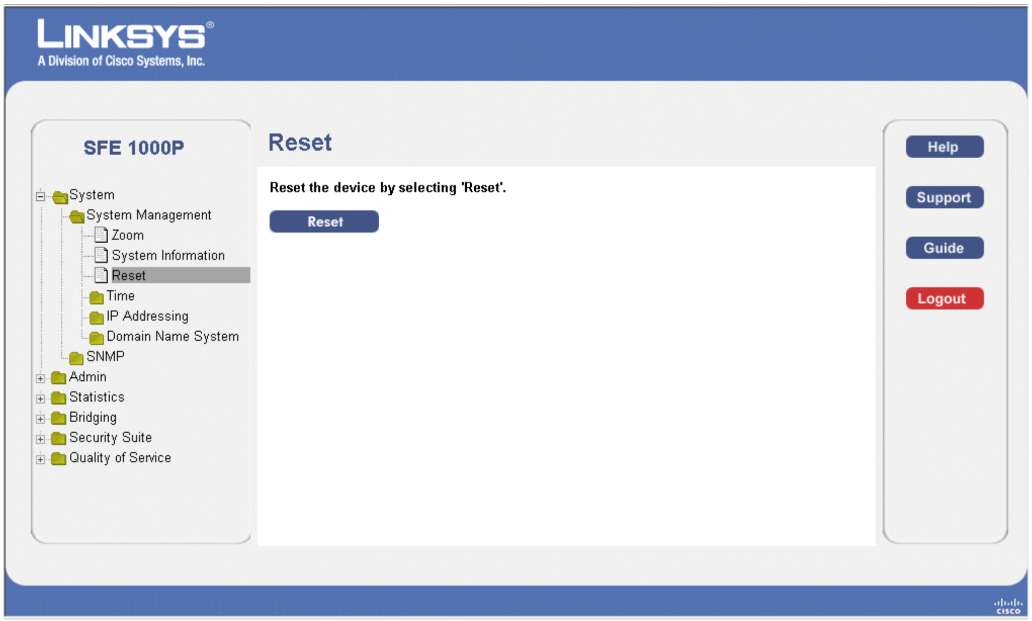
## Deleting Device Information

User defined information can be deleted on specific EWS pages, by opening the appropriate EWS page, selecting a table row, checking the remove checkbox, and then clicking the Delete button.

## Resetting the Device

The *Reset* page enables the device to be reset from a remote location. Save all changes to the Running Configuration file before resetting the device. This prevents the current device configuration from being lost. To reset the device:

***Reset Page***



Reset the device by selecting 'Reset'.

## Logging Off The Device

Click Logout . The system logs off. The *Embedded Web System Home Page* closes.

# Managing Device Information

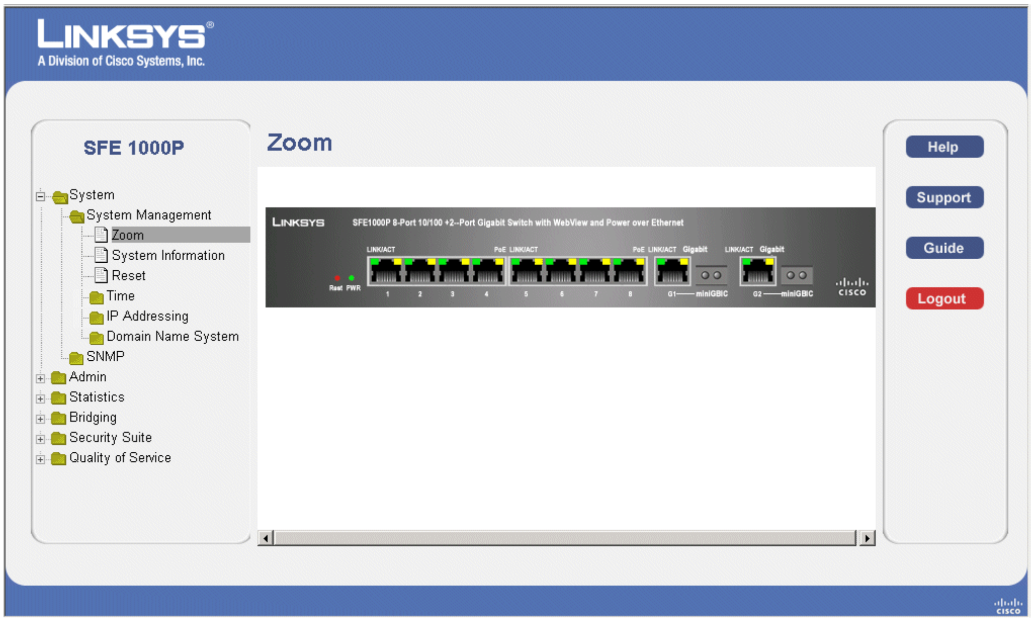
This section provides information for defining both basic and advanced system information. This section contains the following topics:

- Understanding the Device Zoom View
- Defining General System Information
- Resetting the Device

## Understanding the Device Zoom View

The *Zoom Page* is the main window used for viewing the device.

***Zoom Page***



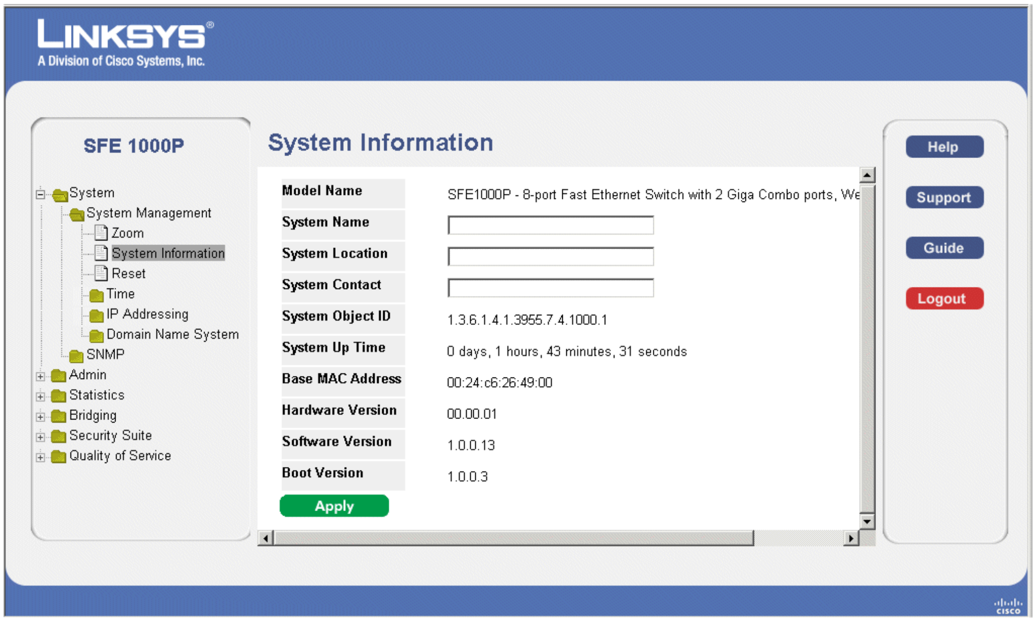
The *Zoom Page* contains the following port indicators:

- **Green —** Indicates the port is currently operating.

# Defining General System Information

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

***System Information Page***



System Information

| | |
|---|---|
| Model Name | SFE1000P - 8-port Fast Ethernet Switch with 2 Giga Combo ports, We |
| System Name | |
| System Location | |
| System Contact | |
| System Object ID | 1.3.6.1.4.1.3955.7.4.1000.1 |
| System Up Time | 0 days, 1 hours, 43 minutes, 31 seconds |
| Base MAC Address | 00:24:c6:26:49:00 |
| Hardware Version | 00.00.01 |
| Software Version | 1.0.0.13 |
| Boot Version | 1.0.0.3 |

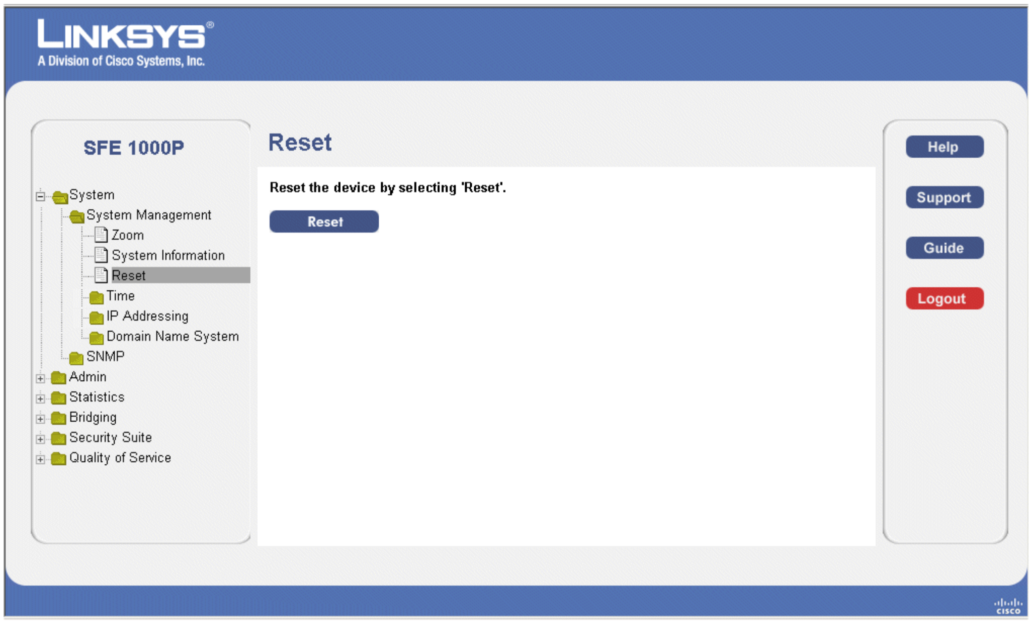
The *System Information Page* contains the following fields:

- **Model Name** — Displays the model name of 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.
- **Hardware Version** — Displays the hardware version number.
- **Software Version** — Displays the software version number.
- **Boot Version** — Indicates the system boot version currently running on the device.

# Resetting the Device

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

***Reset Page***



Reset the device by selecting 'Reset'.

# 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
- PDAs
- Audio and video remote monitoring

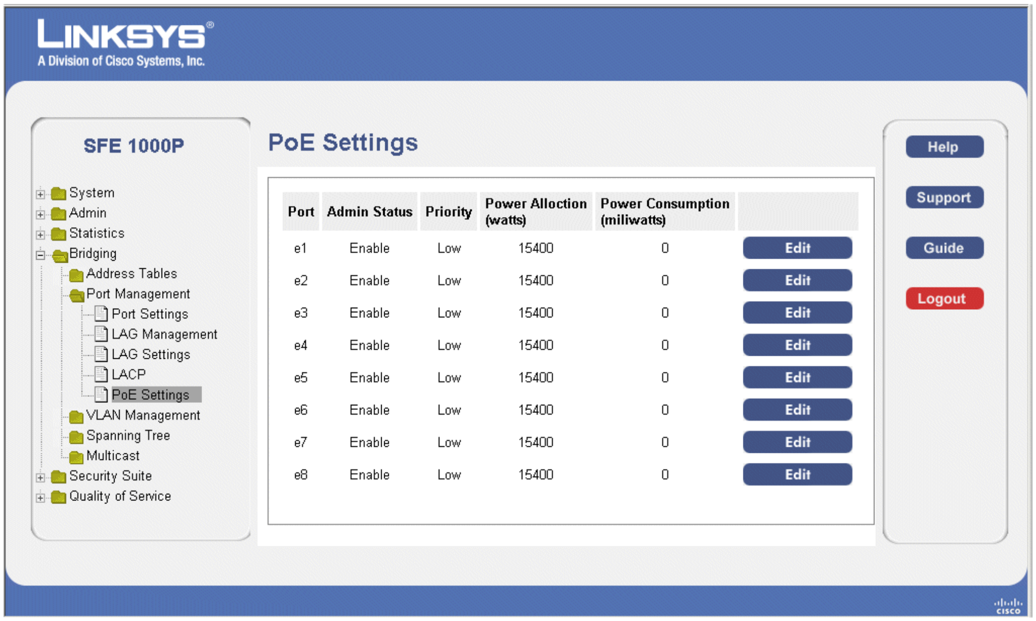
Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports. Guard Band protects the device from exceeding the maximum power level. For example, if 400W is maximum power level, and the Guard Band 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.

**NOTE:** Due to hardware limitations, the power measurement accuracy is 4%.

# PoE Settings

The *PoE Settings Page* contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps.

***PoE Settings Page***



PoE Settings

| Port | Admin Status | Priority | Power Allocation (watts) | Power Consumption (miliwatts) | |
|---|---|---|---|---|---|
| e1 | Enable | Low | 15400 | 0 | Edit |
| e2 | Enable | Low | 15400 | 0 | Edit |
| e3 | Enable | Low | 15400 | 0 | Edit |
| e4 | Enable | Low | 15400 | 0 | Edit |
| e5 | Enable | Low | 15400 | 0 | Edit |
| e6 | Enable | Low | 15400 | 0 | Edit |
| e7 | Enable | Low | 15400 | 0 | Edit |
| e8 | Enable | Low | 15400 | 0 | Edit |

The *PoE Settings Page* displays the currently configured PoE ports and contains the following information:

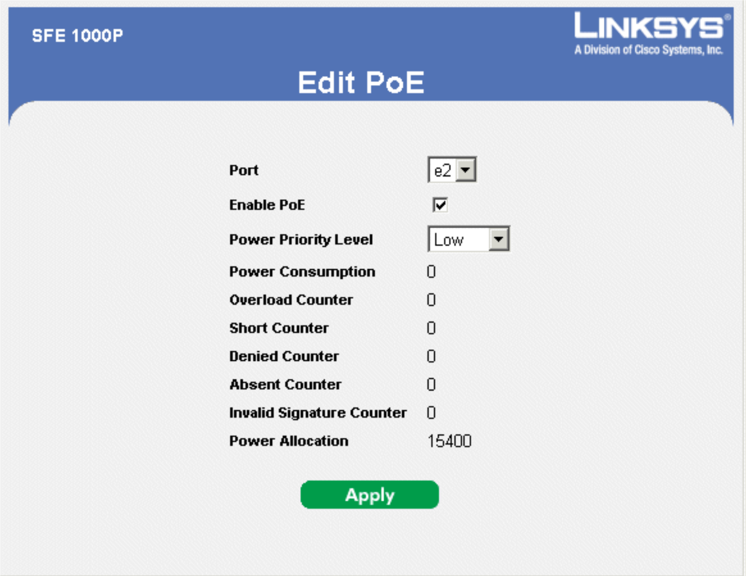
- **Port —** Displays the selected port's number.
- **Admin Status** — Indicates whether PoE is enabled or disabled on the port. The possible values are:
  - *Enable* — Enables PoE on the port. This is the default setting.
  - *Disable* — Disables PoE on the port.
- **Priority** — Indicates the PoE ports' priority. The possible values are *Critical, High* and *Low.* The default is *Low.*
- **Power Allocation (watts)** — Indicates the power allocated to the port. The range is 3 - 15.4 watts.
- **Power Consumption (milliwatts)** — Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used. The field values are represented in Watts. The possible field values are:
  - *0.44 – 12.95* — Indicates that the port is assigned a power consumption level of .44 to 12.95 watts.

- *0.44 – 3.8* — Indicates that the port is assigned a power consumption level of .44 to 3.8 watts.
- *3.84 – 6.49* — Indicates that the port is assigned a power consumption level of 3.84 to 6.49 watts.
- *6.49 – 12.95* — Indicates that the port is assigned a power consumption level of 6.49 to 12.95 watts.

## Edit PoE

Use the Edit PoE page to change settings for your devices.

***Edit PoE***



Edit PoE

| | |
|---|---|
| Port | e2 |
| Enable PoE | ☑ |
| Power Priority Level | Low |
| Power Consumption | 0 |
| Overload Counter | 0 |
| Short Counter | 0 |
| Denied Counter | 0 |
| Absent Counter | 0 |
| Invalid Signature Counter | 0 |
| Power Allocation | 15400 |

The *Edit PoE* 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:
  - *Enable* — Enables PoE on the port. This is the default setting.
  - *Disable* — 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. This is the default level.

  - *High* — Defines the PoE priority level as high.
  - *Critical* — Defines the PoE priority level as Critical. This is the highest PoE priority level.
- **Power Consumption** — Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used. The field values are represented in Watts. The possible field values are:
  - *0.44 – 12.95* — Indicates that the port is assigned a power consumption level of 0.44 to 12.95 Watts.
  - *0.44 – 3.8* — Indicates that the port is assigned a power consumption level of 0.44 to 3.8 Watts.
  - *3.84 – 6.49* — Indicates that the port is assigned a power consumption level of 3.84 to 6.49 Watts.
  - *6.49 – 12.95* — Indicates that the port is assigned a power consumption level of 6.49 to 12.95 Watts.
- **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** — Indicate 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.
- **Power Allocation** — Indicates the power allocated to the port. The range is 3 - 15.4 watts.

# Configuring Device Security

The Security Suite contains the following sections:

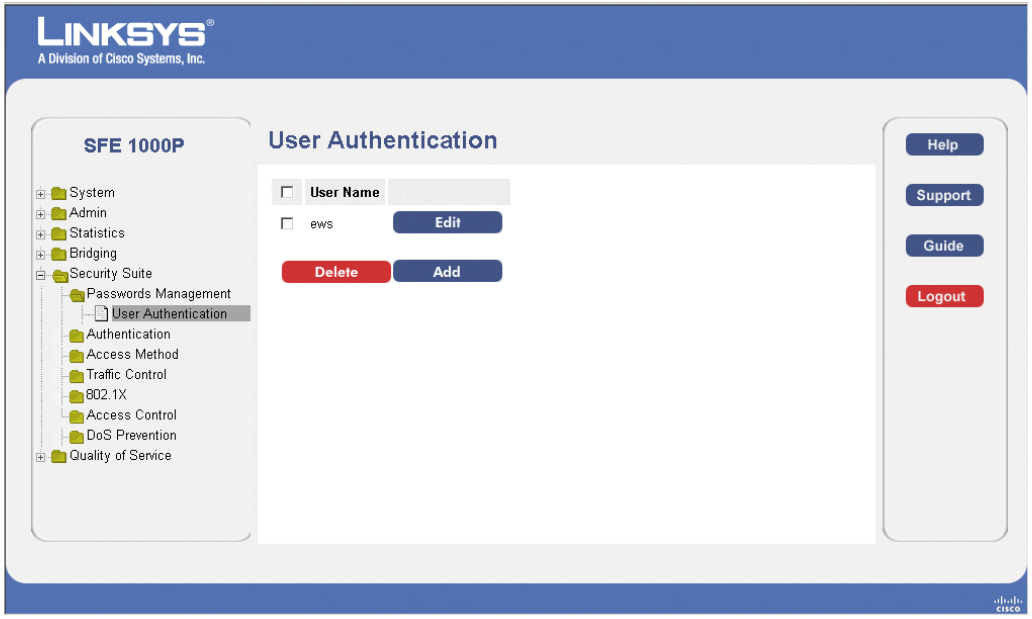
- Passwords Management
- Defining Authentication
- Defining Access Method
- Defining Traffic Control
- Defining 802.1x
- Defining Access Control
- Defining DoS Prevention

## Passwords Management

This section contains information for defining passwords. Passwords are used to authenticate users accessing the device.

**NOTE:** By default, a single user name is defined, "admin", with no password. An additional user name/ password is configured for use in the system.

***User Authentication Page***



User Authentication

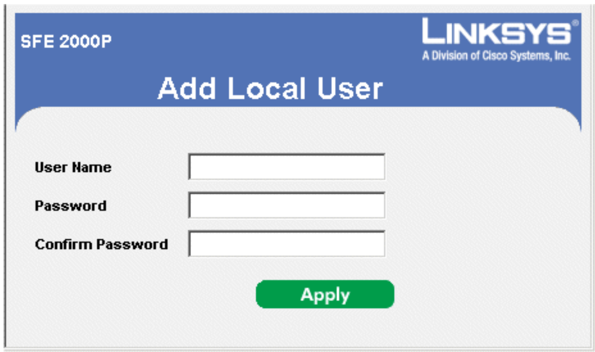
| □ | User Name |
|---|---|
| □ | ews |

The *User Authentication Page* contains the following fields:

- **User Name** — Displays the user name.
- **Edit** — Click to modify the user name and/or password.
- **Add** — Click to add a new user.
- **Delete** — To delete a user name, select the user name and click the Delete button.

## Add Local User

***Add Local User Page***

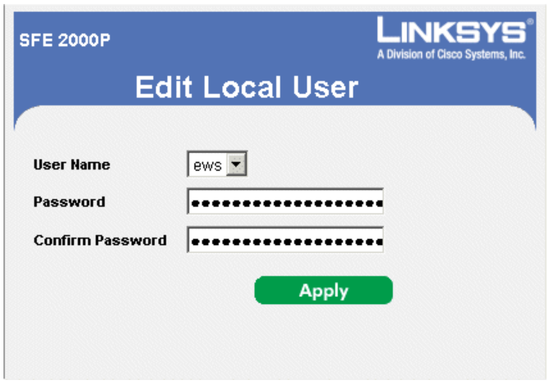


The Add Local User Page contains the following fields:

- **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.

## Modifying the Local User Settings

***Edit Local User Page***



User Name: ews
Password: •••••••••••••••••••
Confirm Password: •••••••••••••••••••

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.

# Defining Authentication

The Authentication section contains the following pages:

- Defining Authentication Profiles

- Mapping Authentication Profiles

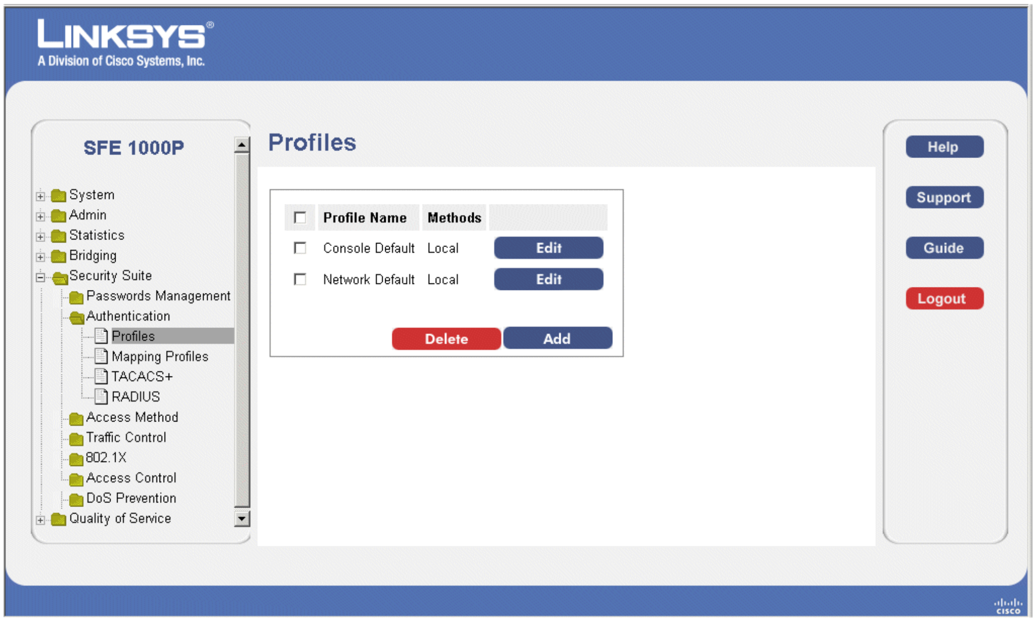
- Defining TACACS+

- Defining RADIUS

## Defining Authentication 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.

***Profiles Page***



| ☐ | Profile Name | Methods | |
|---|---|---|---|
| ☐ | Console Default | Local | Edit |
| ☐ | Network Default | Local | Edit |

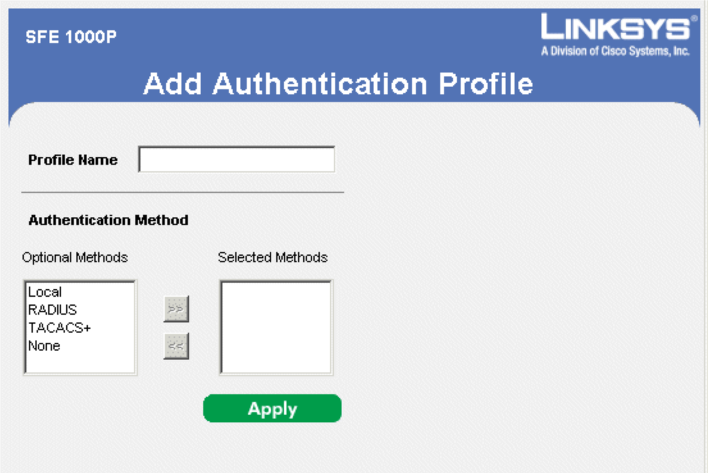
The *Profiles Page* contains the following fields:

- **Profile Name** — Displays the Profile name defined for the Login Table.

- **Methods** — Specifies the authentication method used for port authentication. 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 port.

## Add Authentication Profile

***Add Authentication Profile Page***



SFE 1000P

Add Authentication Profile

Profile Name

Authentication Method

Optional Methods: Local, RADIUS, TACACS+, None

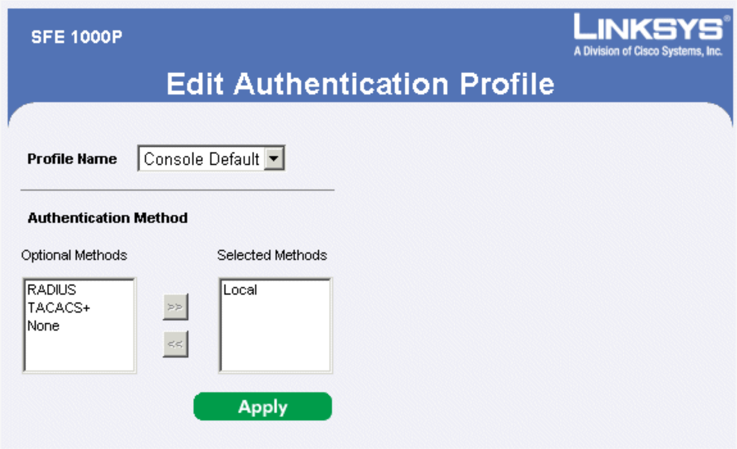
Selected Methods:

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 indicates 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 port.

## Modify the Authentication Profile

*Edit Authentication Profile Page*



SFE 1000P

Edit Authentication Profile

Profile Name: Console Default

Authentication Method

Optional Methods: RADIUS, TACACS+, None

Selected Methods: Local

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* — No user authentication is attempted.

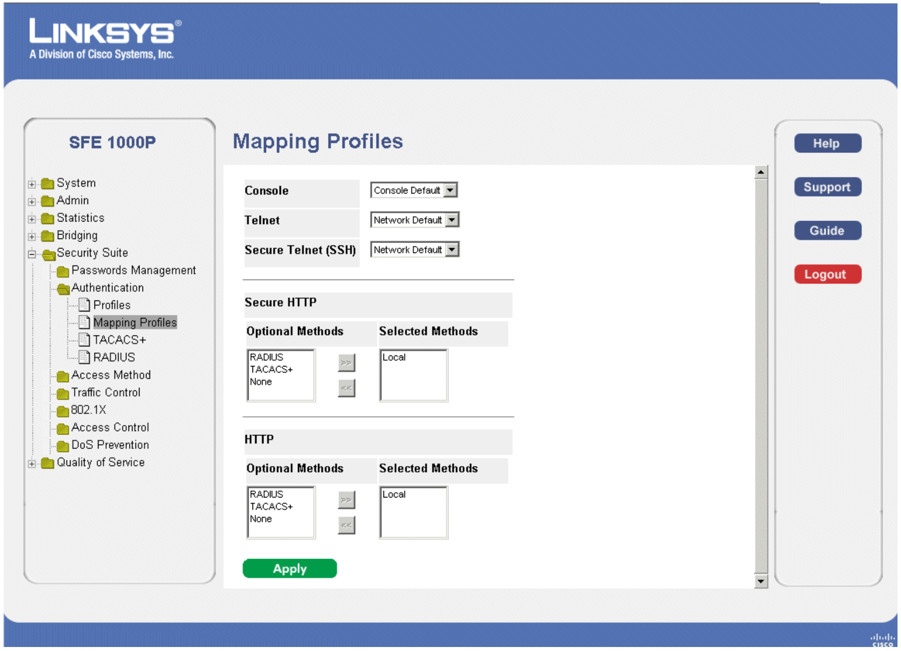
## Mapping Authentication Profiles

After authentication profiles are defined, they 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.

***Mapping Profiles Page***



Mapping Profiles

| | |
|---|---|
| Console | Console Default |
| Telnet | Network Default |
| Secure Telnet (SSH) | Network Default |

Secure HTTP

| Optional Methods | Selected Methods |
|---|---|
| RADIUS<br>TACACS+<br>None | Local |

HTTP

| Optional Methods | Selected Methods |
|---|---|
| RADIUS<br>TACACS+<br>None | Local |

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

## Defining TACACS+

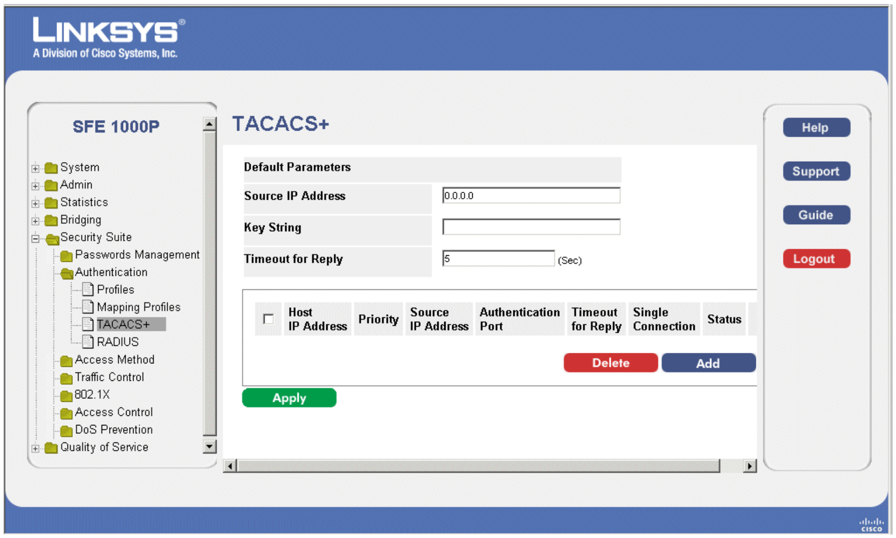
The devices provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication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



TACACS+

Default Parameters

| | |
|---|---|
| Source IP Address | 0.0.0.0 |
| Key String | |
| Timeout for Reply | 5 (Sec) |

| ☐ | Host IP Address | Priority | Source IP Address | Authentication Port | Timeout for Reply | Single Connection | Status |
|---|---|---|---|---|---|---|---|

The *TACACS+ Page* contains the following fields:

- **Source IP Address** — Displays the device source IP 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:

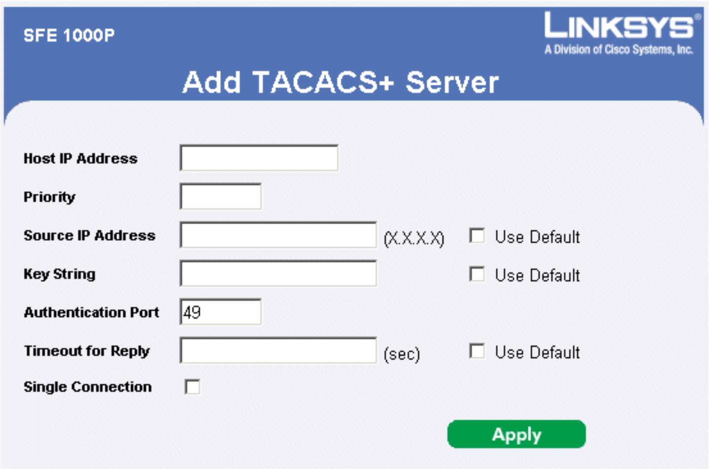
- **Host IP Address** — Displays the TACACS+ Server IP address.
- **Priority** — Displays the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication 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* — There is currently a connection between the device and the TACACS+ server.

- *Not Connected* — There is not currently a connection between the device and the TACACS+ server.

## Add TACACS+ Server

***Add TACACS+ Server Page***



Add TACACS+ Server

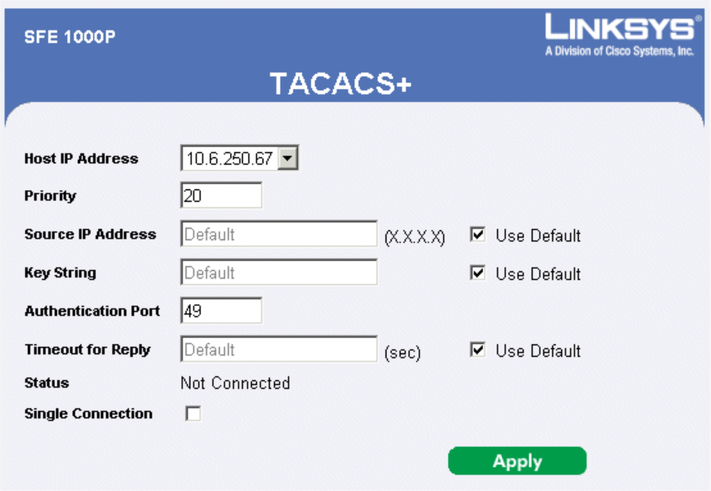
| | | | |
|---|---|---|---|
| Host IP Address | | | |
| Priority | | | |
| Source IP Address | | (X.X.X.X) | □ Use Default |
| Key String | | | □ Use Default |
| Authentication Port | 49 | | |
| Timeout for Reply | | (sec) | □ Use Default |
| Single Connection | □ | | |

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

- **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** — Defines the device source IP 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** — Displays 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.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server when selected.
- **Use Default** — Uses the default value for the parameter.

## Modifying TACACS+ Settings

*TACACS+ Page*



TACACS+

| | | | |
|---|---|---|---|
| Host IP Address | 10.6.250.67 ▾ | | |
| Priority | 20 | | |
| Source IP Address | Default | (X.X.X.X) | ☑ Use Default |
| Key String | Default | | ☑ Use Default |
| Authentication Port | 49 | | |
| Timeout for Reply | Default | (sec) | ☑ Use Default |
| Status | Not Connected | | |
| Single Connection | □ | | |

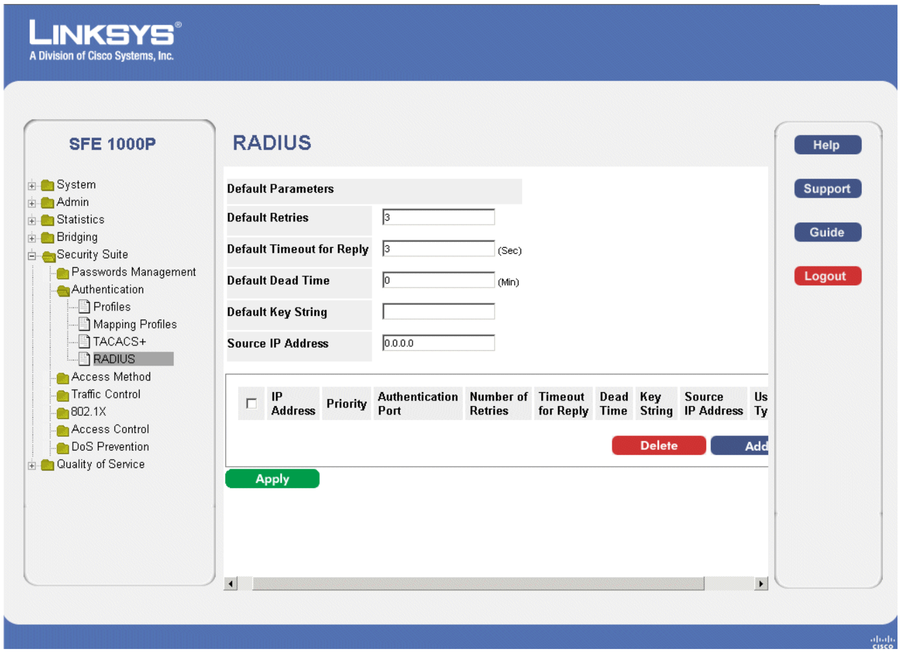
The *TACACS+ Page* contains the following fields:

- **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** — Defines the device source IP 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** — Displays 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* — There is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — There is not currently a 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** — Uses the default value for the parameter.

# 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.

***RADIUS Page***



RADIUS

| Default Parameters | |
|---|---|
| Default Retries | 3 |
| Default Timeout for Reply | 3 (Sec) |
| Default Dead Time | 0 (Min) |
| Default Key String | |
| Source IP Address | 0.0.0.0 |

| □ | IP Address | Priority | Authentication Port | Number of Retries | Timeout for Reply | Dead Time | Key String | Source IP Address | Us Ty |
|---|---|---|---|---|---|---|---|---|---|

The *RADIUS Page* contains the following fields:

- **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 IP Address** — Provides the device default Timeout for Reply.

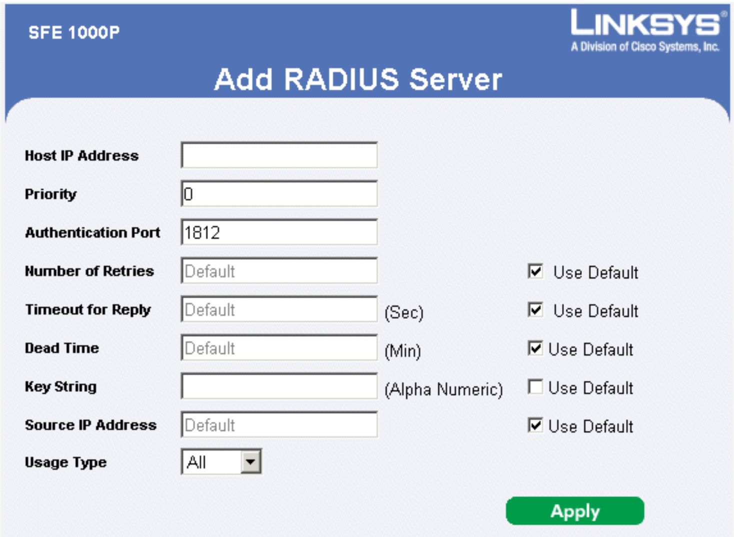
The following parameters are configured for each RADIUS server:

- **IP Address** — The Authentication Server IP addresses.
- **Priority** — 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.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.

- **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.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **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.

## Add RADIUS Server

***Add Radius Server Page***



SFE 1000P

Add RADIUS Server

| | | | |
|---|---|---|---|
| Host IP Address | | | |
| Priority | 0 | | |
| Authentication Port | 1812 | | |
| Number of Retries | Default | | ☑ Use Default |
| Timeout for Reply | Default | (Sec) | ☑ Use Default |
| Dead Time | Default | (Min) | ☑ Use Default |
| Key String | | (Alpha Numeric) | □ Use Default |
| Source IP Address | Default | | ☑ Use Default |
| Usage Type | All | | |

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

- **Host IP Address** — Displays the *RADIUS* Server IP address.

- **Priority** — 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.

- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.

- **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.

- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.

- **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.

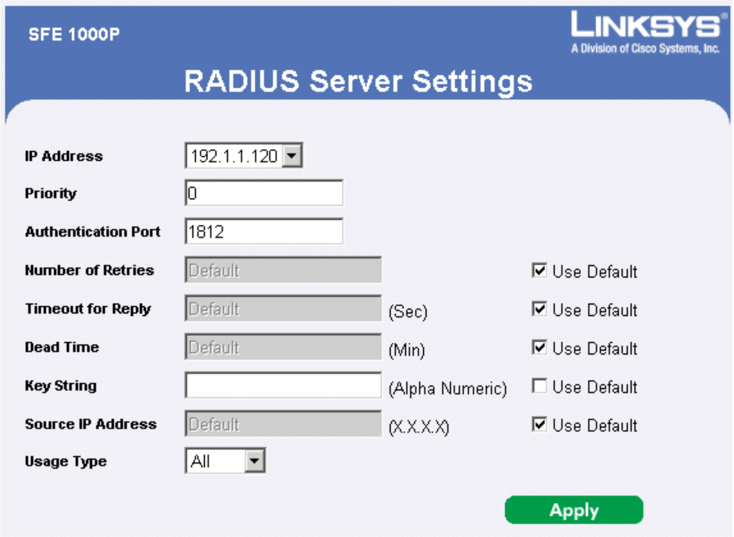
  - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.

  - *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.

## Modifying RADIUS Server Settings

*Edit RADIUS Settings Page*



RADIUS Server Settings

| | | | |
|---|---|---|---|
| IP Address | 192.1.1.120 ▾ | | |
| Priority | 0 | | |
| Authentication Port | 1812 | | |
| Number of Retries | Default | | ☑ Use Default |
| Timeout for Reply | Default | (Sec) | ☑ Use Default |
| Dead Time | Default | (Min) | ☑ Use Default |
| Key String | | (Alpha Numeric) | □ Use Default |
| Source IP Address | Default | (X.X.X.X) | ☑ Use Default |
| Usage Type | All ▾ | | |

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

- **IP Address** — Displays the *RADIUS* Server IP address.
- **Priority** — 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.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **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.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **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.

# Defining Access Method

The access method section contains the following pages:

- Defining Access Profiles
- Defining Profile Rules

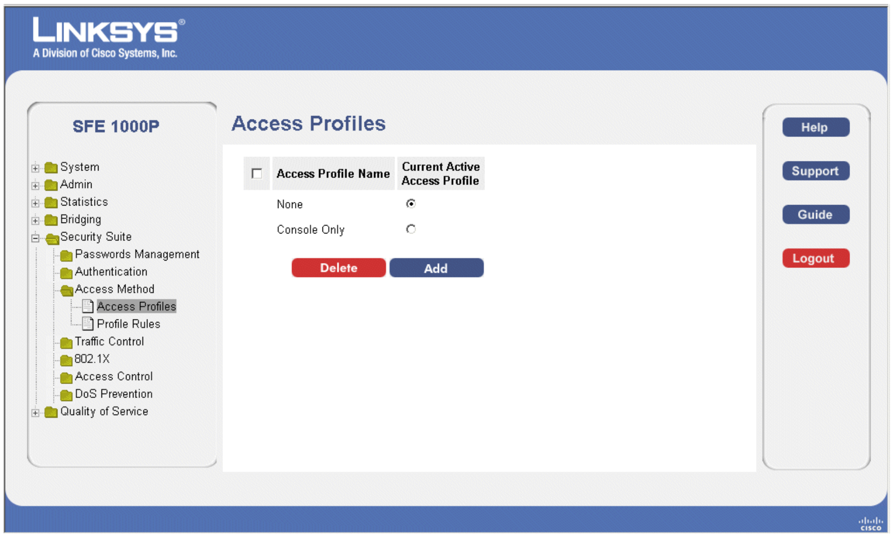
## Defining Access Profiles

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.

***Access Profiles Page***



Access Profiles

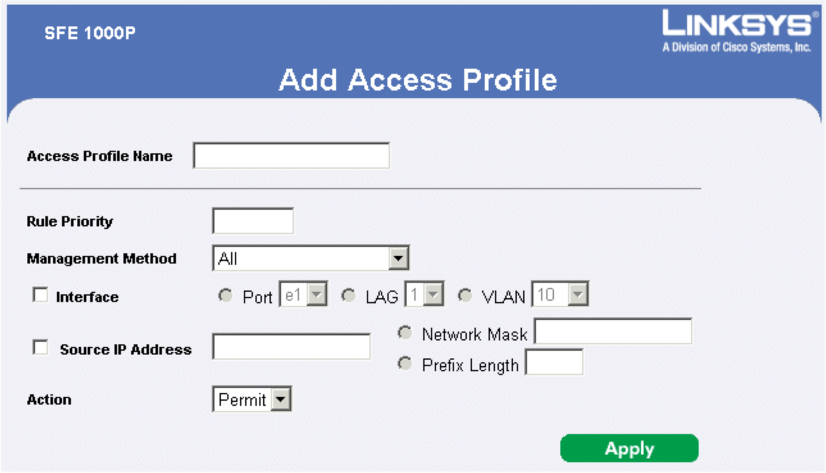
| □ | Access Profile Name | Current Active Access Profile |
|---|---|---|
| | None | ● |
| | Console Only | ○ |

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.
- **Delete** — Deletes the selected access profile. The possible field values are:
  - *Checked* — Deletes the selected access profile.
  - *Unchecked* — Maintains the access profiles.

## Add Access Profile Page

***Add Access Profile Page***



Add Access Profile

| | |
|---|---|
| Access Profile Name | |
| Rule Priority | |
| Management Method | All |
| □ Interface | ○ Port e1 ○ LAG 1 ○ VLAN 10 |
| □ Source IP Address | ○ Network Mask ○ Prefix Length |
| Action | Permit |

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

- **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.
  - *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.
  - *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.
- **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.

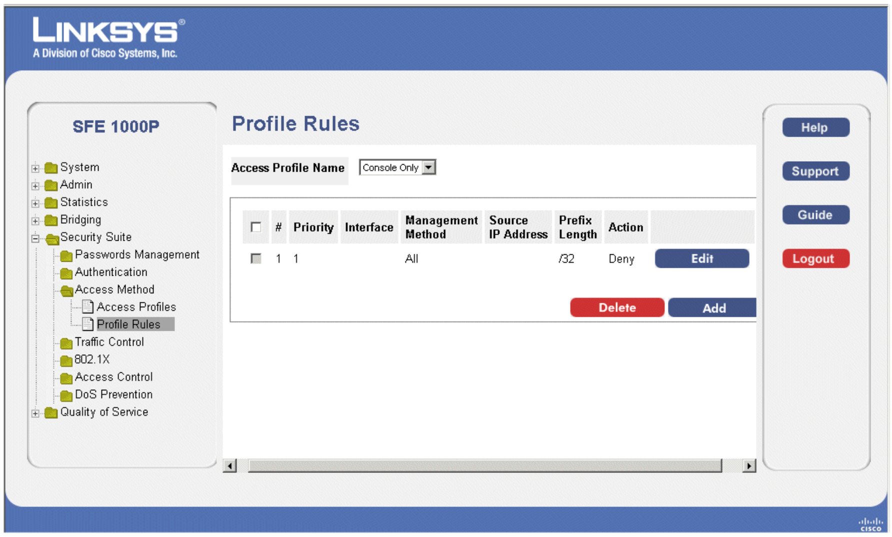
- *Deny* — Denies access to the device. This is the default.

## 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

***Profile Rules Page***



Profile Rules

Access Profile Name: Console Only

| □ | # | Priority | Interface | Management Method | Source IP Address | Prefix Length | Action | |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | 1 | | All | | /32 | Deny | Edit |

The *Profile Rules Page* contains the following fields:

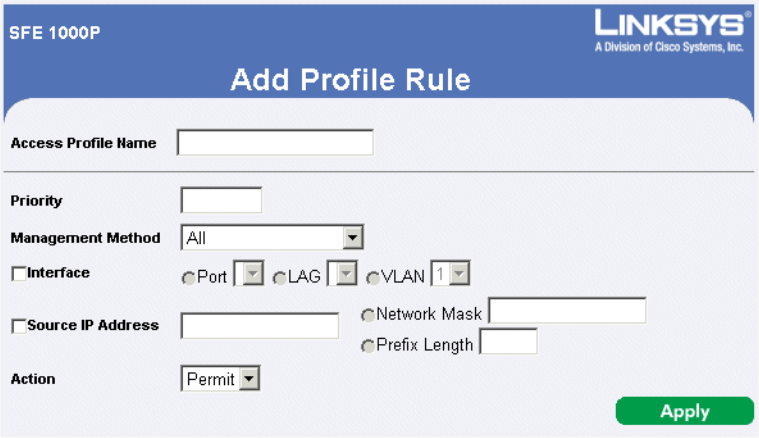
- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, 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 (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.
  - *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.

## Add Profile Rule

*Add Profile Rule Page*



SFE 1000P

LINKSYS® A Division of Cisco Systems, Inc.

Add Profile Rule

| | |
|---|---|
| Access Profile Name | |
| Priority | |
| Management Method | All |
| □ Interface | ○ Port ○ LAG ○ VLAN 1 |
| □ Source IP Address | ○ Network Mask<br>○ Prefix Length |
| Action | Permit |

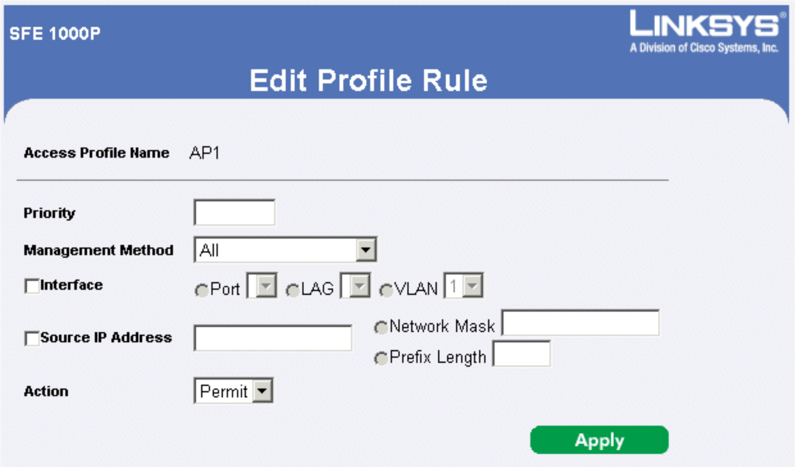
The *Add Profile Rule Page* contains the following fields:

- **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.

## Modifying Profile Rules

***Edit Profile Rule Page***



Edit Profile Rule

Access Profile Name AP1

Priority

Management Method All

☐ Interface ○ Port ○ LAG ○ VLAN 1

☐ Source IP Address ○ Network Mask ○ Prefix Length

Action Permit

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

- **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.

# Defining Traffic Control

The Traffic Control section contains the following pages:

- Defining Storm Control
- Defining Port Security

## Defining Storm Control

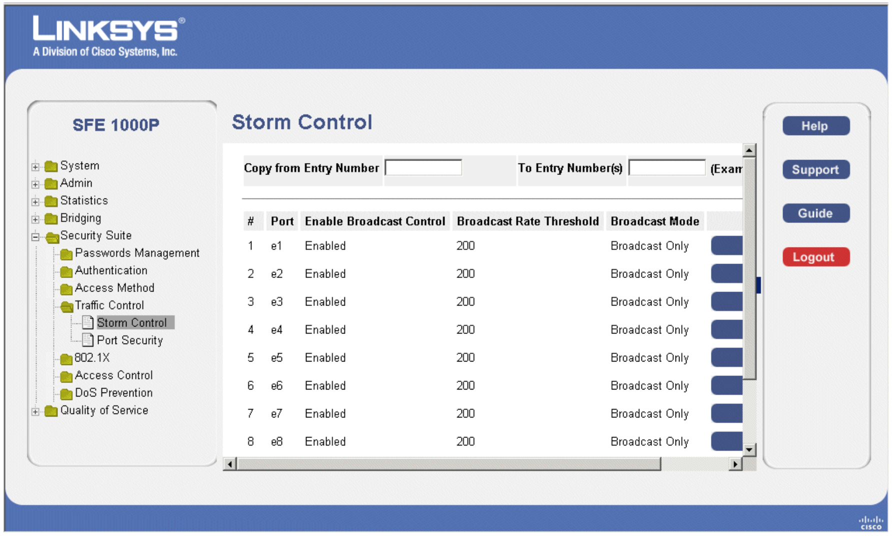
Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports.

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 all ports 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.

***Storm Control Page***



Storm Control

Copy from Entry Number ____ To Entry Number(s) ____ (Exam

| # | Port | Enable Broadcast Control | Broadcast Rate Threshold | Broadcast Mode |
|---|---|---|---|---|
| 1 | e1 | Enabled | 200 | Broadcast Only |
| 2 | e2 | Enabled | 200 | Broadcast Only |
| 3 | e3 | Enabled | 200 | Broadcast Only |
| 4 | e4 | Enabled | 200 | Broadcast Only |
| 5 | e5 | Enabled | 200 | Broadcast Only |
| 6 | e6 | Enabled | 200 | Broadcast Only |
| 7 | e7 | Enabled | 200 | Broadcast Only |
| 8 | e8 | Enabled | 200 | Broadcast Only |

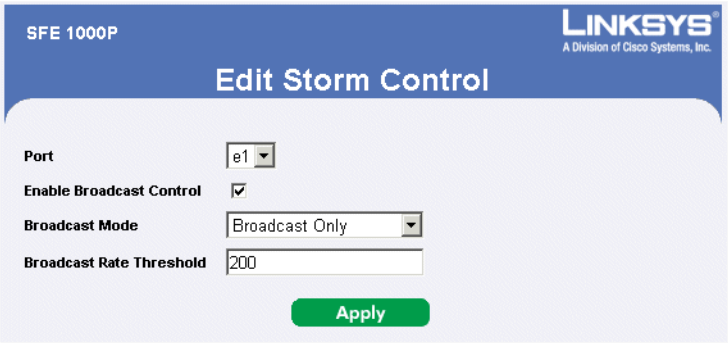
The *Storm Control Page* contains the following fields:

- **Copy From Entry Number** — Indicates the row number from which storm control parameters are copied.
- **To Entry Number(s)** — Indicates the row number to which storm control parameters are copied.

- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — Indicates if Broadcast packet types are forwarded on the specific interface. The possible field values are:
  - *Enable* — Enables Broadcast packet types to be forwarded.
  - *Disable* — Disables Broadcast packet types to be forwarded.
- **Broadcast Rate Threshold** — 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.

## Modifying Storm Control

***Edit Storm Control Page***



SFE 1000P

Edit Storm Control

| | |
|---|---|
| Port | e1 |
| Enable Broadcast Control | ☑ |
| Broadcast Mode | Broadcast Only |
| Broadcast Rate Threshold | 200 |

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

- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — Indicates if Broadcast packet types are forwarded on the specific interface. The possible field values are:
  - *Checked* — Enables Broadcast packet types to be forwarded.
  - *Unchecked* — Disables Broadcast packet types to be forwarded.
- **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.

- **Broadcast Rate Threshold** — 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.

## Defining Port Security

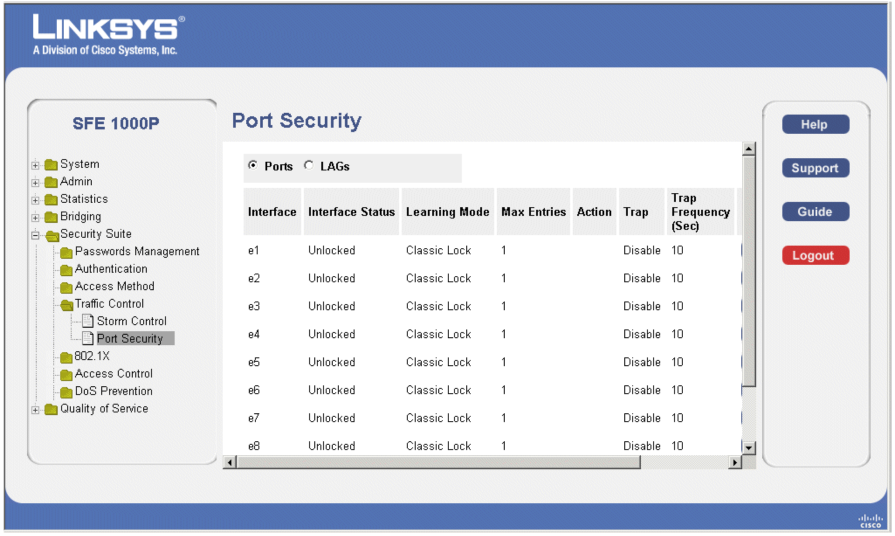
Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the 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 Management* page.

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

***Port Security Page***



Port Security

● Ports ○ LAGs

| Interface | Interface Status | Learning Mode | Max Entries | Action | Trap | Trap Frequency (Sec) |
|---|---|---|---|---|---|---|
| e1 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e2 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e3 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e4 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e5 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e6 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e7 | Unlocked | Classic Lock | 1 | | Disable | 10 |
| e8 | Unlocked | Classic Lock | 1 | | Disable | 10 |

The *Port Security Page* contains the following fields:

- **Ports** — Indicates the port number 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.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.

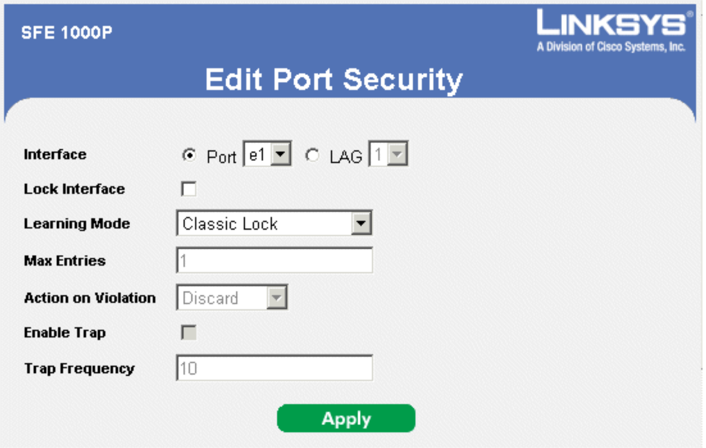
  In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated.
- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the 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)** — The amount of time (in seconds) between traps. The default value is 10 seconds.

## Modifying Port Security

***Edit Port Security Page***



| | |
|---|---|
| Interface | ● Port e1 ○ LAG 1 |
| Lock Interface | ☐ |
| Learning Mode | Classic Lock |
| Max Entries | 1 |
| Action on Violation | Discard |
| Enable Trap | ☐ |
| Trap Frequency | 10 |

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

- **Interface** — Displays 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.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.

  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.

- **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** — The amount of time (in seconds) between traps. The default value is 10 seconds.

# Defining 802.1x

Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the port, which is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **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.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The 802.1x page configures port to use Extensible Authentication Protocol (EAP).

The 802.1x section contains the following pages:

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

## Defining 802.1X Properties

Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the port, which is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **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.

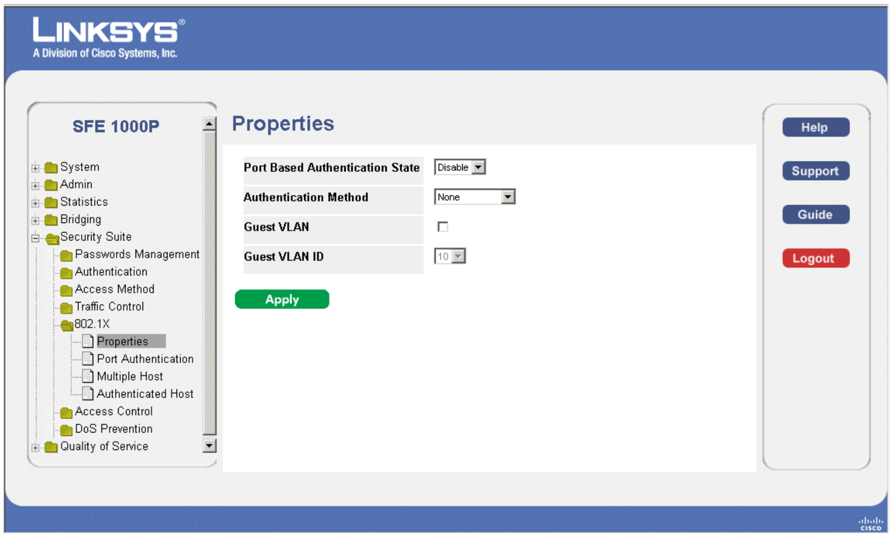
Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.

- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The *802.1x* page configures port to use Extensible Authentication Protocol (EAP).

***802.1X Properties Page***



Properties

| | |
|---|---|
| Port Based Authentication State | Disable |
| Authentication Method | None |
| Guest VLAN | □ |
| Guest VLAN ID | 10 |

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

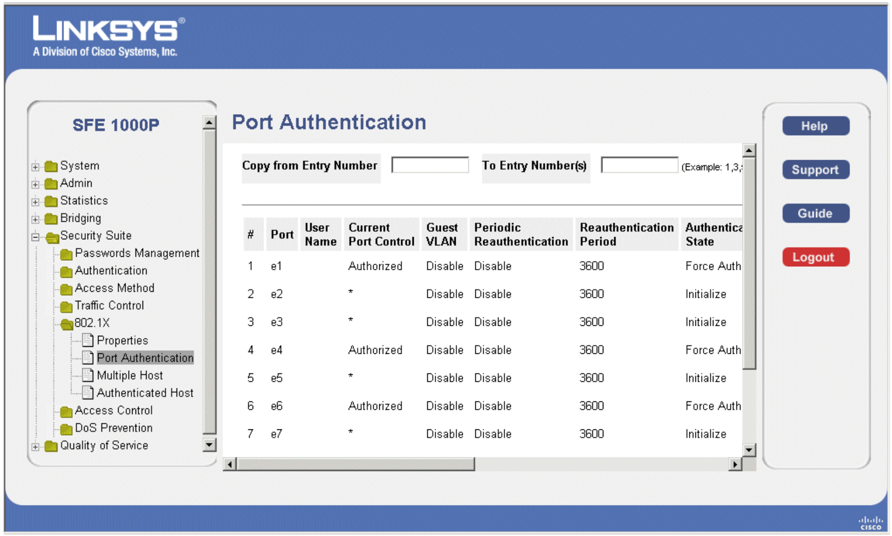
- **Port Based Authentication State** — Enables Port-based Authentication ion the device. The possible field values are:
  - *Enable* — Enables port-based authentication on the device.
  - *Disable* — Disables port-based authentication on the device.

- **Authentication Method** — Defines the user authentication methods. The possible field values are:
  - *RADIUS, None* — 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.

## Defining Port Authentication

**802.1X *Port Authentication Page***



Port Authentication

Copy from Entry Number □ To Entry Number(s) □ (Example: 1,3,

| # | Port | User Name | Current Port Control | Guest VLAN | Periodic Reauthentication | Reauthentication Period | Authentica State |
|---|---|---|---|---|---|---|---|
| 1 | e1 |  | Authorized | Disable | Disable | 3600 | Force Auth |
| 2 | e2 |  | * | Disable | Disable | 3600 | Initialize |
| 3 | e3 |  | * | Disable | Disable | 3600 | Initialize |
| 4 | e4 |  | Authorized | Disable | Disable | 3600 | Force Auth |
| 5 | e5 |  | * | Disable | Disable | 3600 | Initialize |
| 6 | e6 |  | Authorized | Disable | Disable | 3600 | Force Auth |
| 7 | e7 |  | * | Disable | Disable | 3600 | Initialize |

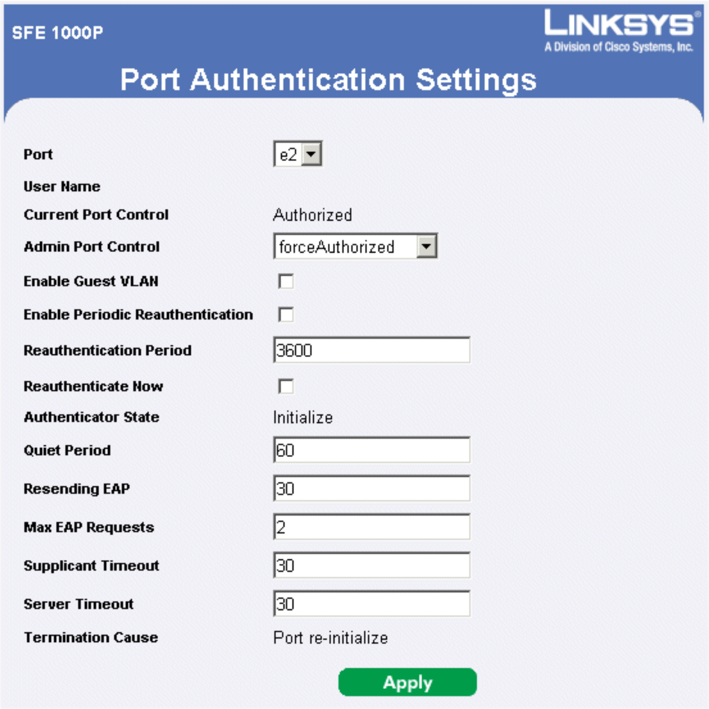
The *802.1X Port Authentication Page* contains the following fields:

- **Copy From Entry Number** — Indicates the row number from which port authentication parameters are copied.
- **To Entry Number(s)** — Indicates the row number to which port authentication parameters are copied.
- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the user name.
- **Current Port Control** — Displays the current port authorization state.
- **Guest VLAN** — Displays the Guest VLAN.
- **Periodic Reauthentication** — Permits immediate 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.

- **Authenticator State** — Specifies the port authorization state. The possible field values are as follows:
  - *Force-Authorized* — The controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized* — 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** — 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.

## Modifying 8021X Security

*Port Authentication Settings Page*



Port Authentication Settings

| | |
|---|---|
| Port | e2 |
| User Name | |
| Current Port Control | Authorized |
| Admin Port Control | forceAuthorized |
| Enable Guest VLAN | □ |
| Enable Periodic Reauthentication | □ |
| Reauthentication Period | 3600 |
| Reauthenticate Now | □ |
| Authenticator State | Initialize |
| Quiet Period | 60 |
| Resending EAP | 30 |
| Max EAP Requests | 2 |
| Supplicant Timeout | 30 |
| Server Timeout | 30 |
| Termination Cause | Port re-initialize |

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** — Displays 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 re-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:

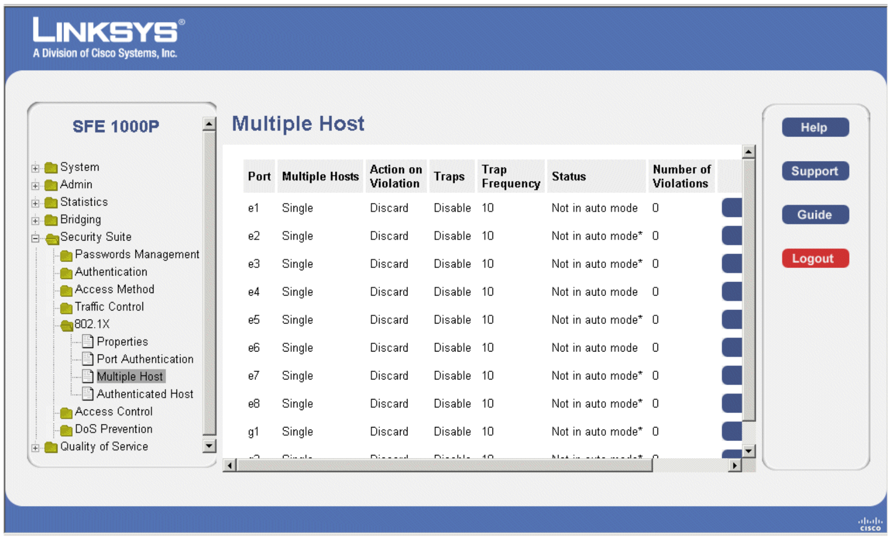
  - *Checked* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
  - *Unchecked* — Disables port-based authentication on the device. This is the default.

- **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* — The controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized* — 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** — 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.

## Defining Multiple Hosts

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

**802.1X Multiple Host Page**



Multiple Host

| Port | Multiple Hosts | Action on Violation | Traps | Trap Frequency | Status | Number of Violations |
|---|---|---|---|---|---|---|
| e1 | Single | Discard | Disable | 10 | Not in auto mode | 0 |
| e2 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |
| e3 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |
| e4 | Single | Discard | Disable | 10 | Not in auto mode | 0 |
| e5 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |
| e6 | Single | Discard | Disable | 10 | Not in auto mode | 0 |
| e7 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |
| e8 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |
| g1 | Single | Discard | Disable | 10 | Not in auto mode* | 0 |

The *802.1X Multiple Host Page* contains the following fields:

- **Port** — Displays the port number for which the Multiple Hosts configuration is displayed.
- **Multiple Hosts** — Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
  - *Single* — Only the authorized host can access the port.
  - *Multiple* — 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.
- **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.

  - *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.

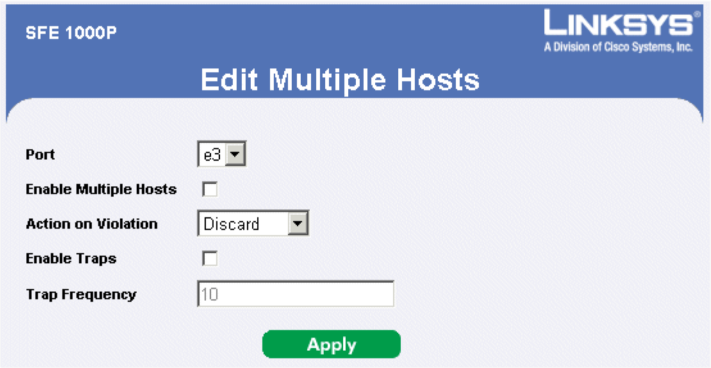
  - *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.

  - *No Single Host* — Indicates that Multiple Host is enabled.

- **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 Multiple Host Settings

***Edit Multiple Host Page***



SFE 1000P

Edit Multiple Hosts

| | |
|---|---|
| Port | e3 |
| Enable Multiple Hosts | □ |
| Action on Violation | Discard |
| Enable Traps | □ |
| Trap Frequency | 10 |

The *Edit Multiple Host Page* contains the following fields:

- **Port** — Displays the port number for which advanced port-based authentication is enabled.

- **Enable Multiple Hosts** — Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:

  - *Checked* — Multiple host mode is enabled.

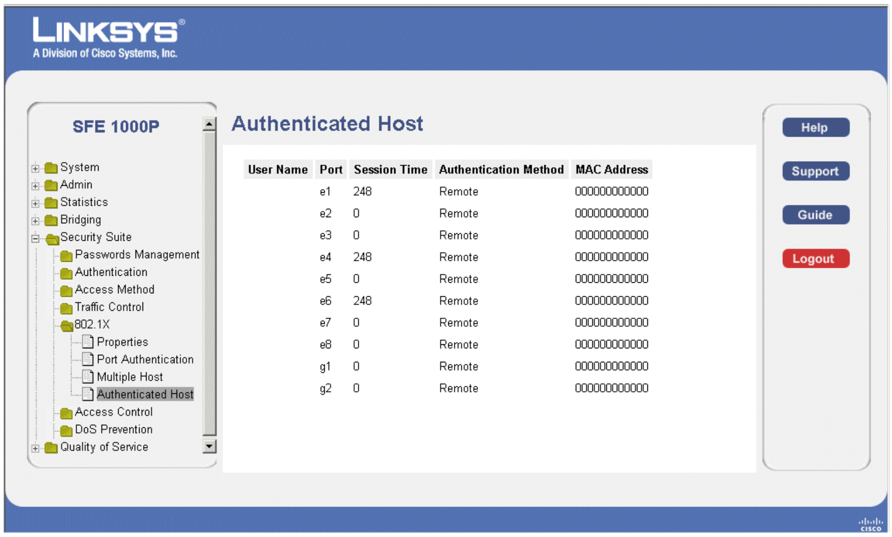
  - *Unchecked* — Single host mode is enabled. This is the default value.

- **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.
  - *DiscardDisable* — 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.

## Defining Authenticated Host

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

***Authenticated Host Page***



Authenticated Host

| User Name | Port | Session Time | Authentication Method | MAC Address |
|---|---|---|---|---|
| | e1 | 248 | Remote | 000000000000 |
| | e2 | 0 | Remote | 000000000000 |
| | e3 | 0 | Remote | 000000000000 |
| | e4 | 248 | Remote | 000000000000 |
| | e5 | 0 | Remote | 000000000000 |
| | e6 | 248 | Remote | 000000000000 |
| | e7 | 0 | Remote | 000000000000 |
| | e8 | 0 | Remote | 000000000000 |
| | g1 | 0 | Remote | 000000000000 |
| | g2 | 0 | Remote | 000000000000 |

The *Authenticated Host 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* — 802.1x authentication is not used on this port (port is forced-authorized).
  - *None* — The supplicant was not authenticated.
  - *RADIUS* — The supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

# 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.

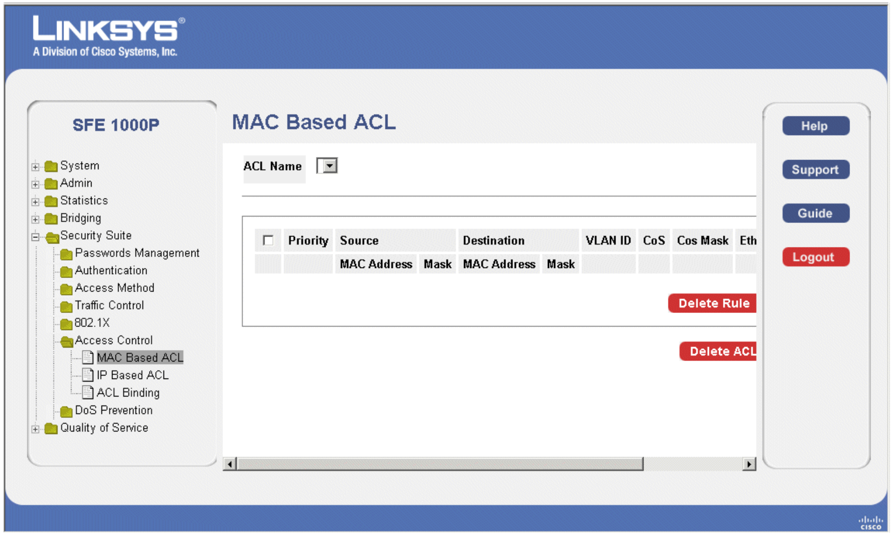
The Access Control section contains the following pages:

- Defining MAC Based ACL
- Defining IP Based ACL
- Defining ACL Binding

## Defining MAC Based ACL

The *MAC Based ACL Page* 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.

***MAC Based ACL Page***



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

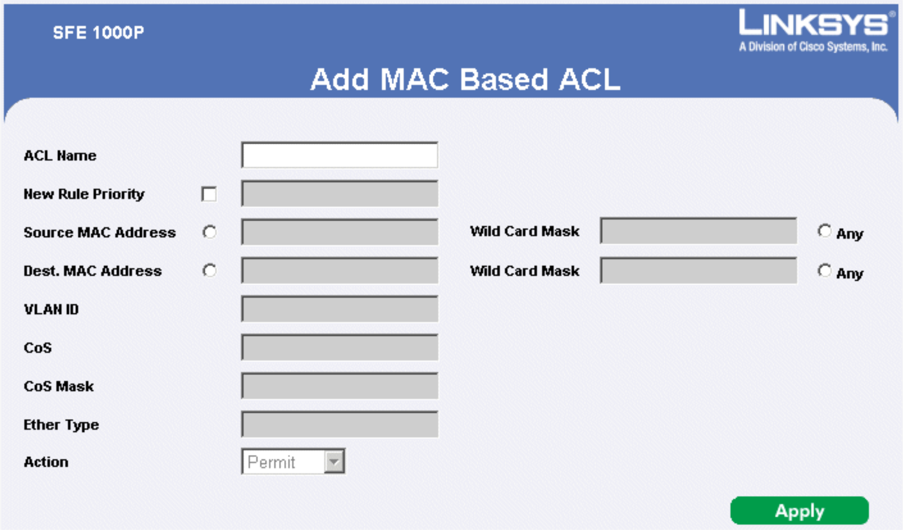
- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Defines the source MAC address to match the ACE.
- **Source 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.
- **CoS** — Class of Service of the packet.
- **CoS Mask** — Wildcard bits to be applied to the CoS.
- **Ether Type** — 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 Interface Configuration Page.

- **Delete ACL** — To remove an ACL, click the **Delete ACL** button.
- **Delete Rule** — To remove an ACE rule, click the rule's checkbox and click the **Delete Rule** button.

## Adding an ACL

***Add MAC Based ACL Page***



SFE 1000P

LINKSYS A Division of Cisco Systems, Inc.

Add MAC Based ACL

| | | | | | |
|---|---|---|---|---|---|
| ACL Name | | | | | |
| New Rule Priority | □ | | | | |
| Source MAC Address | ○ | | Wild Card Mask | | ○ Any |
| Dest. MAC Address | ○ | | Wild Card Mask | | ○ Any |
| VLAN ID | | | | | |
| CoS | | | | | |
| CoS Mask | | | | | |
| Ether Type | | | | | |
| Action | | Permit | | | |

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 Address**

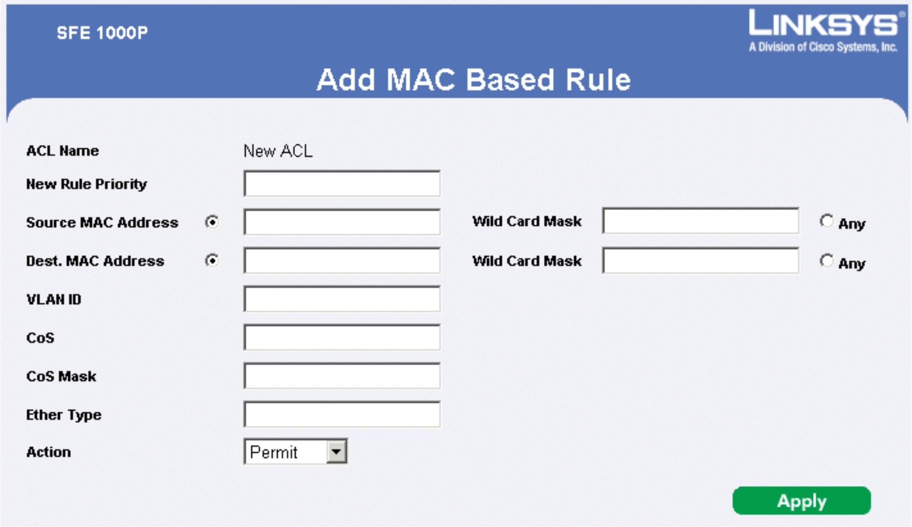
  - *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
  - *Wild Card Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card 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 Address**

  - *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
  - *Wild Card Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card 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 4093.
- **CoS** — Class of Service of the packet.
- **CoS Mask** — Wildcard bits to be applied to the CoS.
- **Ether Type** — 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 Interface Configuration Page.

## Adding Rule to MAC Based ACL

***Add MAC Based Rule Page***



| | | | | |
|---|---|---|---|---|
| ACL Name | New ACL | | | |
| New Rule Priority | | | | |
| Source MAC Address | ● | Wild Card Mask | | ○ Any |
| Dest. MAC Address | ● | Wild Card Mask | | ○ Any |
| VLAN ID | | | | |
| CoS | | | | |
| CoS Mask | | | | |
| Ether Type | | | | |
| Action | Permit | | | |

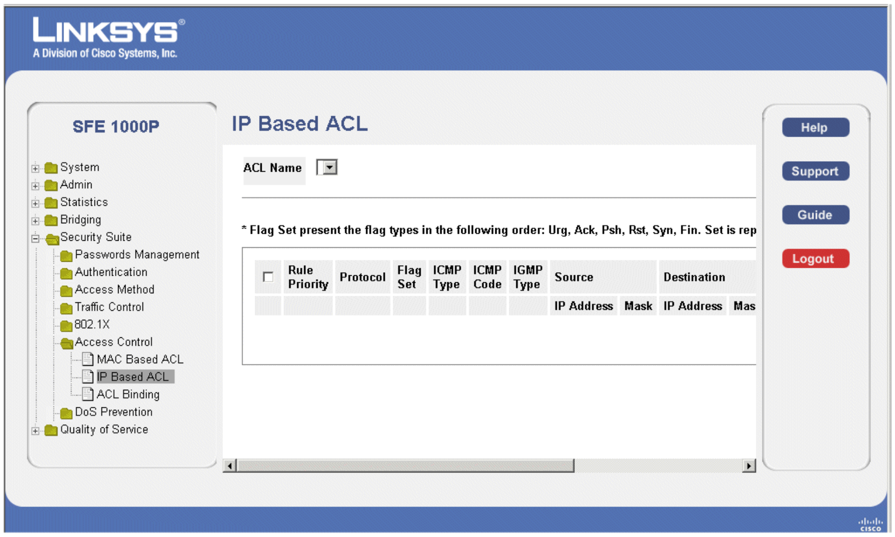
The *Add MAC Based Rule Page* contains the following fields:

- **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 Address**
  - *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
  - *Wild Card Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card 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 Address**
  - *MAC Address* **—** Matches the destination MAC address to which packets are addressed to the ACE.
  - *Wild Card Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card 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 4093.
- **CoS** — Class of Service of the packet.
- **CoS Mask** — Wildcard bits to be applied to the CoS.
- **Ether Type** — 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.

## 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.

***IP Based ACL Page***



IP Based ACL

ACL Name ▾

* Flag Set present the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is rep

| ☐ | Rule Priority | Protocol | Flag Set | ICMP Type | ICMP Code | IGMP Type | Source | | Destination | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | IP Address | Mask | IP Address | Mas |

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 available protocols are:
  - *ICMP — Internet Control Message Protoco*l (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* — I*nternet 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).

- I*PV6: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  I*nternet 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 over 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).

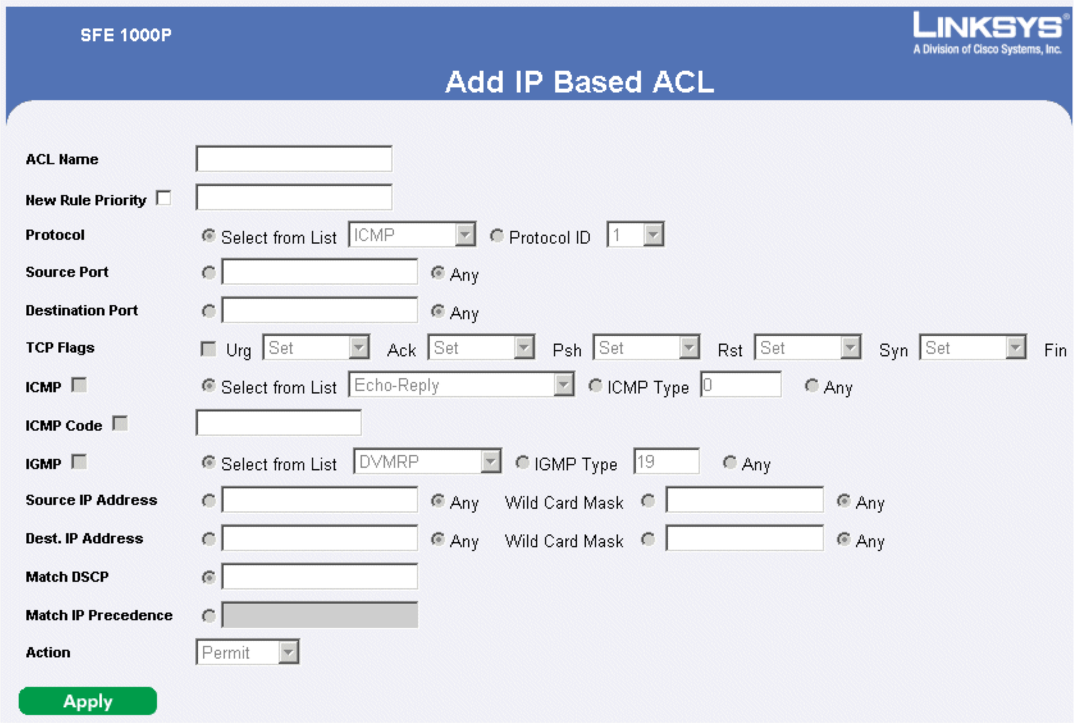
- – *ISIS — Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks.
- – *ANY* — Matches the protocol to any protocol.

- **Flag Set** — Sets the indicated TCP flag that can be triggered.
- **ICMP Type** — Filters packets by ICMP message type. The field values are 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** Address
  - – ***IP Address*** — Matches the source port IP address from which packets are addressed to the ACE.
  - – *Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card 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** Address
  - – ***IP Address*** — Matches the destination port IP address to which packets are addressed to the ACE.
  - – *Mask* — Defines the destination IP address wildcard mask.
- **DSCP** — Matches the packets DSCP value.
- **IP Perch.** — 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.
- **Delete ACL** — To remove an ACL, click the **Delete ACL** button.

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

## Add IP Based ACL

***Add IP Based ACL Page***



ACL Name:

New Rule Priority □:

Protocol: ● Select from List ICMP ○ Protocol ID 1

Source Port: ○ ● Any

Destination Port: ○ ● Any

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

ICMP □: ● Select from List Echo-Reply ○ ICMP Type 0 ○ Any

ICMP Code □:

IGMP □: ● Select from List DVMRP ○ IGMP Type 19 ○ Any

Source IP Address: ○ ● Any Wild Card Mask ○ ● Any

Dest. IP Address: ○ ● Any Wild Card Mask ○ ● Any

Match DSCP: ●

Match IP Precedence: ○

Action: Permit

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.
- **ICMP** — Indicates if ICMP packets are permitted on the network.

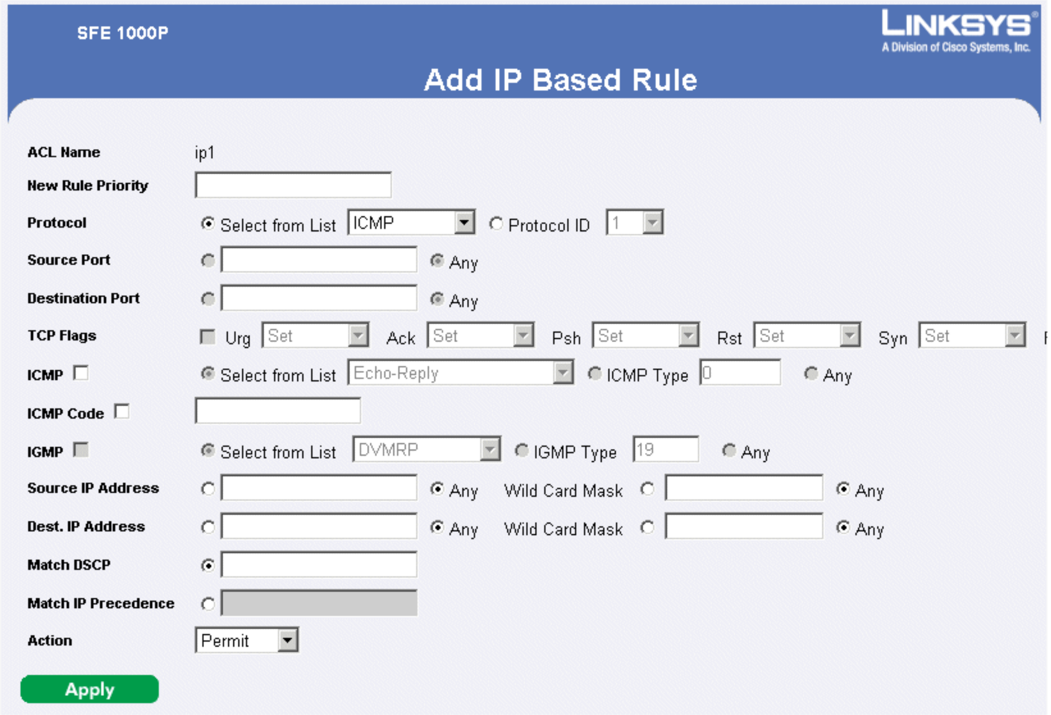
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP** — Filters packets by IGMP message or message types.
- **Source** Address
  - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
  - *Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card 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.
- **Best.** Address
  - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
  - *Mask* — Defines the destination IP address wildcard mask.

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.

## Adding an IP Based Rule

*Add IP Based Rule Page*



SFE 1000P

Add IP Based Rule

| | |
|---|---|
| ACL Name | ip1 |
| New Rule Priority | |
| Protocol | ● Select from List ICMP ○ Protocol ID 1 |
| Source Port | ○ ● Any |
| Destination Port | ○ ● Any |
| TCP Flags | □ Urg Set Ack Set Psh Set Rst Set Syn Set F |
| ICMP □ | ● Select from List Echo-Reply ○ ICMP Type 0 ○ Any |
| ICMP Code □ | |
| IGMP □ | ● Select from List DVMRP ○ IGMP Type 19 ○ Any |
| Source IP Address | ○ ● Any Wild Card Mask ○ ● Any |
| Dest. IP Address | ○ ● Any Wild Card Mask ○ ● Any |
| 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.

- **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.
- **Best. IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.

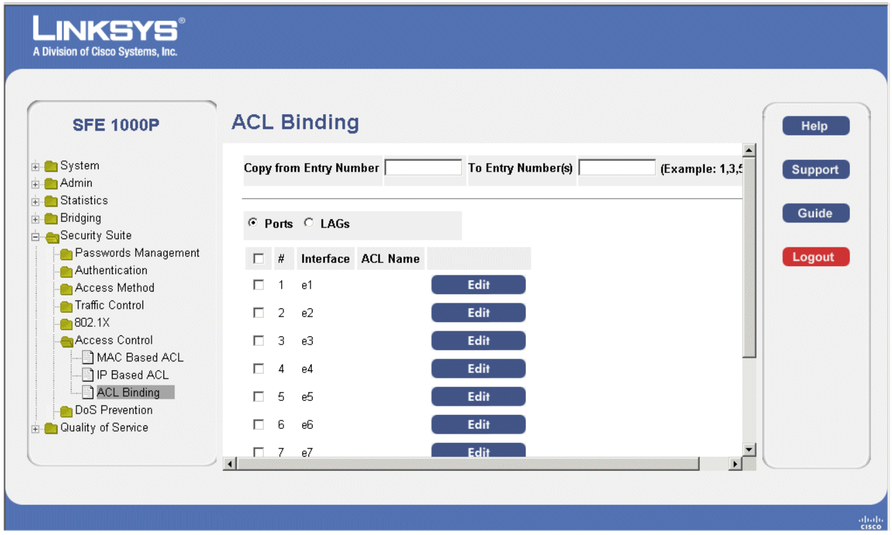
**Match DSCP** or **Match IP.**

- **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.

## 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.

***ACL Binding Page***



ACL Binding

Copy from Entry Number [ ] To Entry Number(s) [ ] (Example: 1,3,5

● Ports ○ LAGs

| □ | # | Interface | ACL Name | |
|---|---|---|---|---|
| □ | 1 | e1 | | Edit |
| □ | 2 | e2 | | Edit |
| □ | 3 | e3 | | Edit |
| □ | 4 | e4 | | Edit |
| □ | 5 | e5 | | Edit |
| □ | 6 | e6 | | Edit |
| □ | 7 | e7 | | Edit |

The *ACL Binding Page* contains the following fields:

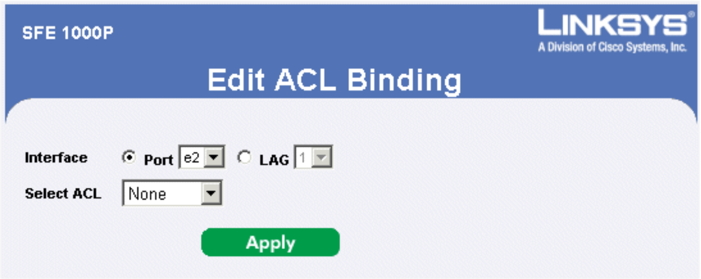
- **Copy From Entry Number** — Copies the ACL information from the defined interface.
- **To Entry Number(s)** — Assigns the copied ACL information to the defined interface.
- **Ports/LAGs** — Indicates the interface to which the ACL is bound.

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.

## Modifying ACL Binding

*Edit ACL Binding Page*



Interface ● Port e2 ○ LAG 1

Select ACL None

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

- **Interface** — Indicates the interface to which the ACL is bound.
- **Select ACL** — Indicates the ACL which is bound to the interface.

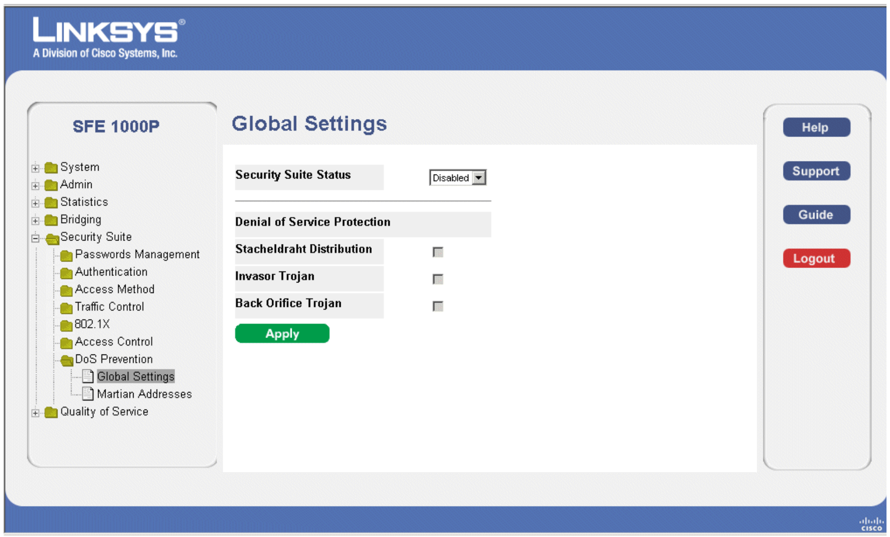
# Defining DoS Prevention

The DoS Prevention section contains the following pages:

- Global Settings
- Defining Martian Addresses

## Global Settings

***Global Settings Page***



Global Settings

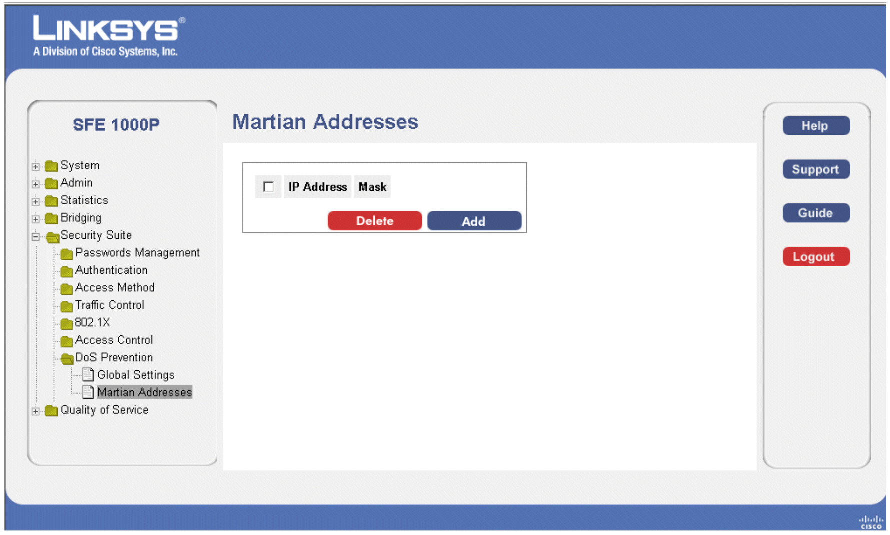
| | |
|---|---|
| Security Suite Status | Disabled |
| Denial of Service Protection | |
| Stacheldraht Distribution | □ |
| Invasor Trojan | □ |
| Back Orifice Trojan | □ |

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:
  - *Enable* — Enables DOS security.
  - *Disable* — 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 Office 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.

## Defining Martian Addresses

*Martian Addresses Page*

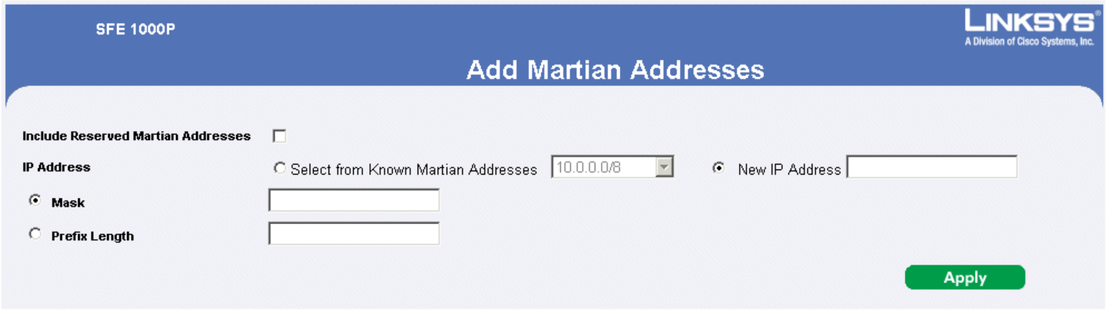


The *Martian Addresses Page* contains the following fields:

- **IP Address** — Displays the IP addresses for which DoS attack is enabled.
- **Mask** — Displays the Mask for which DoS attack is enabled.
- **Delete** — To remove a Martian address, click the entry's checkbox and click the Delete button.

## Add Martian Address Page

***Add Martian Addresses Page***



SFE 1000P

Add Martian Addresses

| | | |
|---|---|---|
| Include Reserved Martian Addresses | □ | |
| IP Address | ○ Select from Known Martian Addresses 10.0.0.0/8 | ● New IP Address |
| ● Mask | | |
| ○ Prefix Length | | |

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

- **Include Reserved Martian Addresses** — Indicates that packets arriving from Martian addresses are dropped.

  The possible values are:

  – *Checked* — Includes specially reserved IP addresses in the Martian Address list. 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)

  – *Unchecked* — Does not include specially reserved IP addresses in the Martian Address list.

- **IP Address** — Enter the Martian IP addresses for which DoS attack is enabled. The possible values are:

  – One of the addresses in the known Martian IP address list. If the **Include Reserved Martian Addresses** option is checked, this list includes reserved Martian Addresses.

  – 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.

# Configuring Device Interfaces

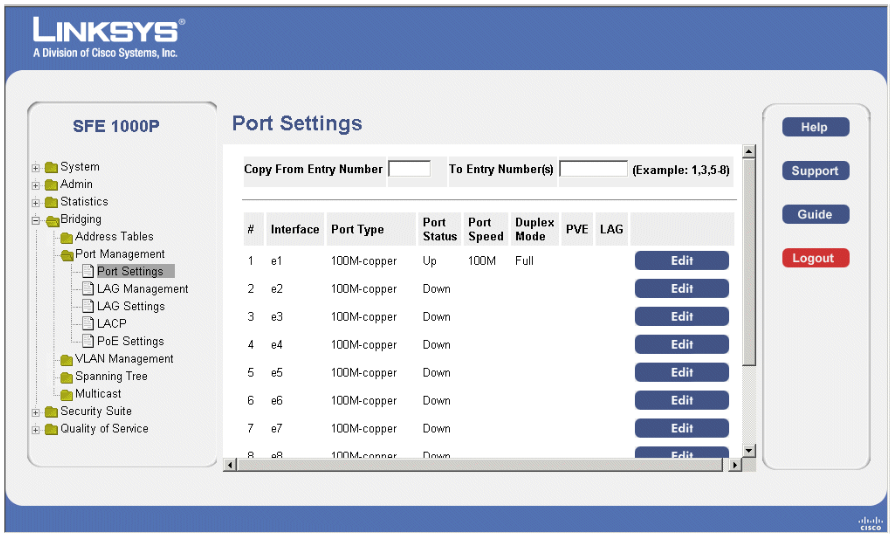
This section contains information for configuring ports and contains the following topic:

- Defining Port Settings
- Defining LAG Management
- Defining LAG Settings
- Configuring LACP

## Defining Port Settings

The Port Settings Page contains fields for defining port parameters.

***Port Settings Page***



Port Settings

Copy From Entry Number ▭ To Entry Number(s) ▭ (Example: 1,3,5-8)

| # | Interface | Port Type | Port Status | Port Speed | Duplex Mode | PVE | LAG | |
|---|---|---|---|---|---|---|---|---|
| 1 | e1 | 100M-copper | Up | 100M | Full | | | Edit |
| 2 | e2 | 100M-copper | Down | | | | | Edit |
| 3 | e3 | 100M-copper | Down | | | | | Edit |
| 4 | e4 | 100M-copper | Down | | | | | Edit |
| 5 | e5 | 100M-copper | Down | | | | | Edit |
| 6 | e6 | 100M-copper | Down | | | | | Edit |
| 7 | e7 | 100M-copper | Down | | | | | Edit |
| 8 | e8 | 100M-copper | Down | | | | | Edit |

The Port Settings Page contains the following fields:

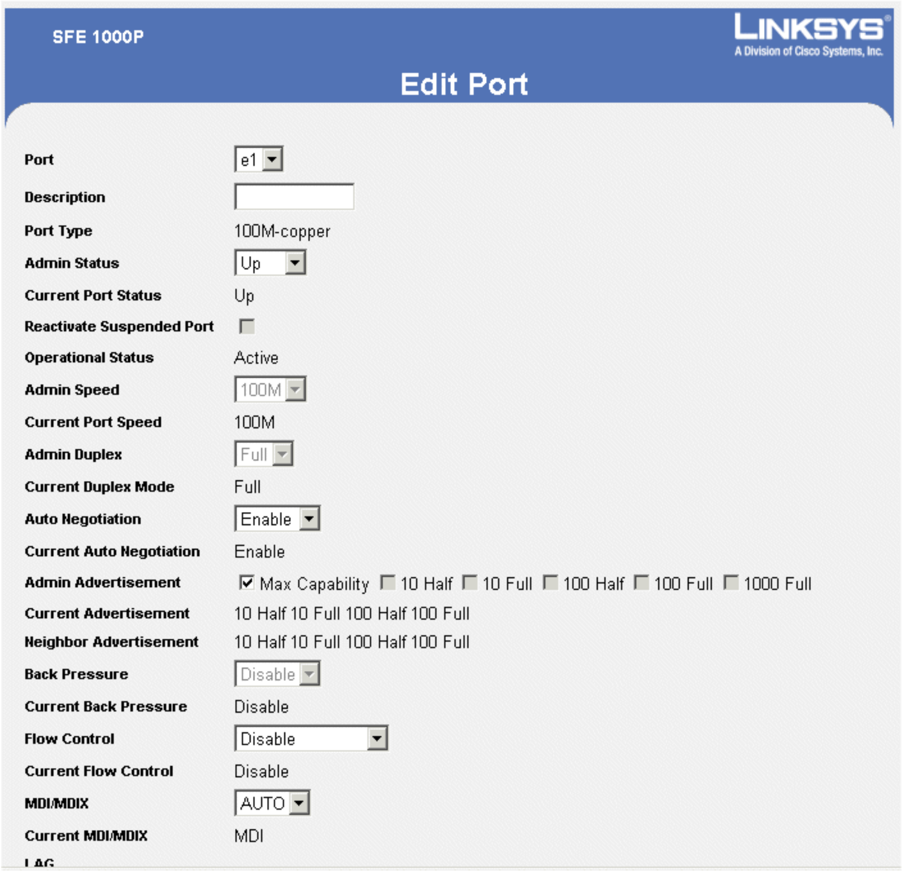
- **Copy from Entry Number** — Copies the port settings from the specified port.
- **to Entry Number(s)** — Assigns the copied port information to a specified port.
- **Interface** — Displays the port number.
- **Port Type** — Displays the port type. The possible field values are:
  - *100M-Copper/1000M-Copper/ComboF/ComboC* — Indicates the port has a copper port connection.
  - *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.
- **LAG** — Defines if the port is part of a Link Aggregation (LAG).

## Modifying Port Settings

***Edit Port Settings Page***



Edit Port

| | |
|---|---|
| **Port** | e1 ▾ |
| **Description** | |
| **Port Type** | 100M-copper |
| **Admin Status** | Up ▾ |
| **Current Port Status** | Up |
| **Reactivate Suspended Port** | □ |
| **Operational Status** | Active |
| **Admin Speed** | 100M ▾ |
| **Current Port Speed** | 100M |
| **Admin Duplex** | Full ▾ |
| **Current Duplex Mode** | Full |
| **Auto Negotiation** | Enable ▾ |
| **Current Auto Negotiation** | Enable |
| **Admin Advertisement** | ☑ Max Capability □ 10 Half □ 10 Full □ 100 Half □ 100 Full □ 1000 Full |
| **Current Advertisement** | 10 Half 10 Full 100 Half 100 Full |
| **Neighbor Advertisement** | 10 Half 10 Full 100 Half 100 Full |
| **Back Pressure** | Disable ▾ |
| **Current Back Pressure** | Disable |
| **Flow Control** | Disable ▾ |
| **Current Flow Control** | Disable |
| **MDI/MDIX** | AUTO ▾ |
| **Current MDI/MDIX** | MDI |
| **LAG** | |

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

- **Port** — Displays the port number.
- **Description** — The port's user-defined name.
- **Port Type** — Displays the port type. The possible field values are:
  - *100M-Copper/1000M-Copper/ComboF/ComboC* — Indicates the port has a copper port connection.
  - *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.
- **Operational Status** — Indicates whether the port is currently active or inactive.

- **Admin Speed** — 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 is a protocol between two link partners that 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** — 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.
- **Current Flow Control** — Displays the current Flow Control setting.
- **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).
- **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.

## Defining LAG Management

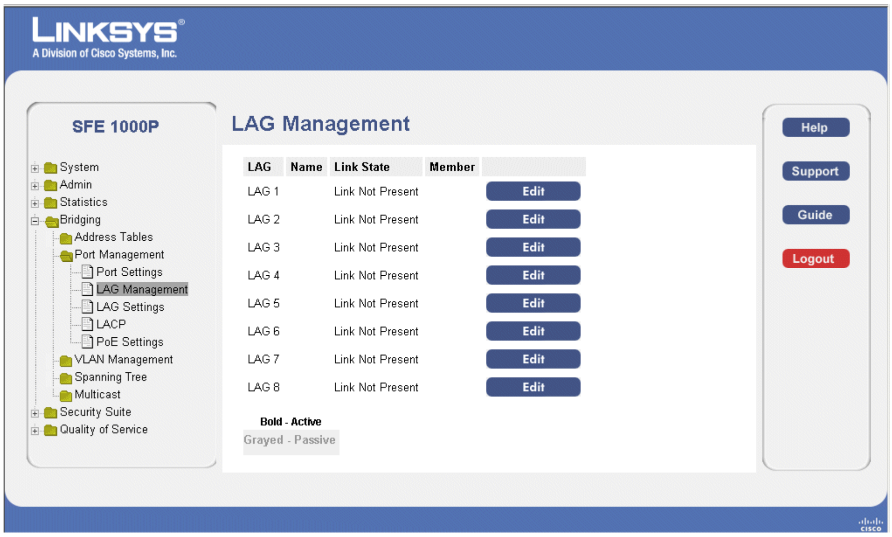
Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

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 8 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.

***LAG Management Page***



LAG Management

| LAG | Name | Link State | Member | |
|---|---|---|---|---|
| LAG 1 | | Link Not Present | | Edit |
| LAG 2 | | Link Not Present | | Edit |
| LAG 3 | | Link Not Present | | Edit |
| LAG 4 | | Link Not Present | | Edit |
| LAG 5 | | Link Not Present | | Edit |
| LAG 6 | | Link Not Present | | Edit |
| LAG 7 | | Link Not Present | | Edit |
| LAG 8 | | Link Not Present | | Edit |

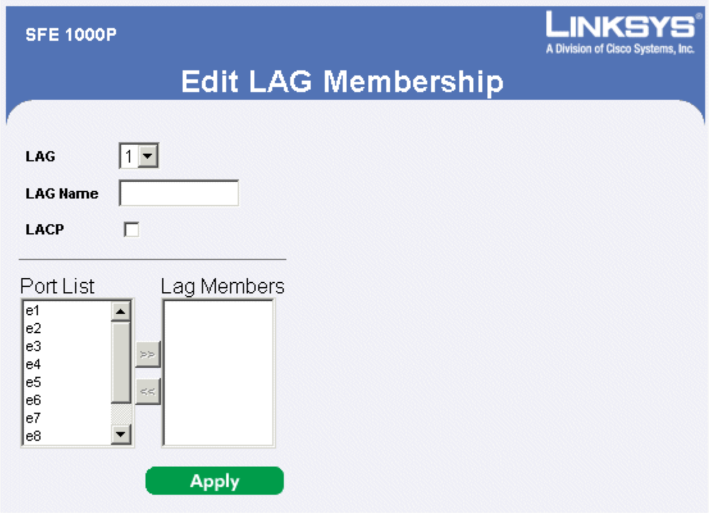
**Bold - Active**
Grayed - Passive

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.

## Modifying LAG Membership

*Edit LAG Membership Page*



LAG 1

LAG Name

LACP □

The *Edit LAG Membership Page* contains the following fields.

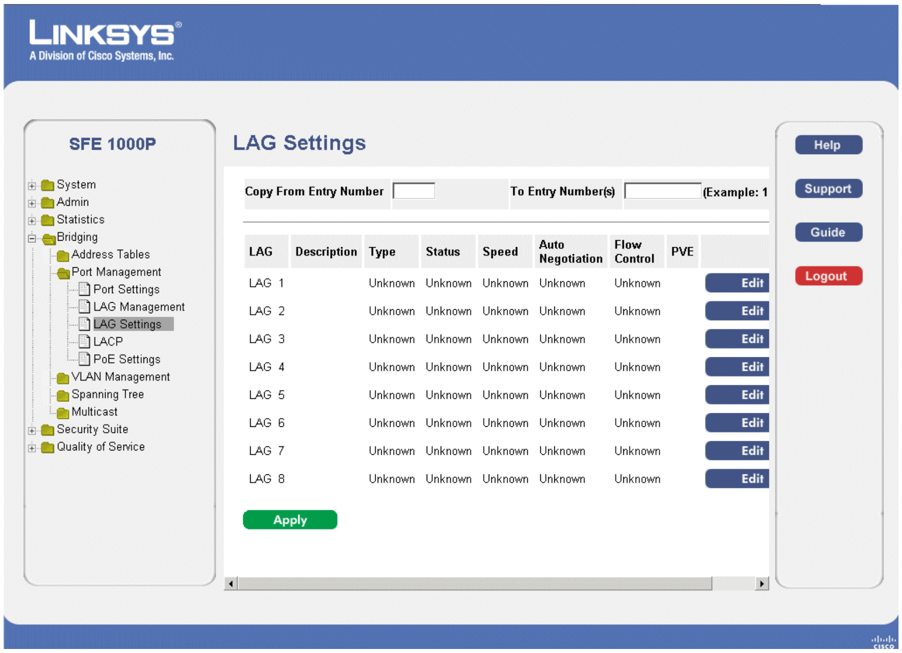
- **LAG** — Displays the LAG number.
- **LAG Name** — Displays the LAG name.
- **LACP** — Indicates that LACP is enable on the LAG.

# 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.

***LAG Settings Page***



LAG Settings

Copy From Entry Number □ To Entry Number(s) □ (Example: 1

| LAG | Description | Type | Status | Speed | Auto Negotiation | Flow Control | PVE | |
|---|---|---|---|---|---|---|---|---|
| LAG 1 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 2 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 3 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 4 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 5 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 6 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 7 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |
| LAG 8 | | Unknown | Unknown | Unknown | Unknown | Unknown | | Edit |

The *LAG Settings Page* contains the following fields:

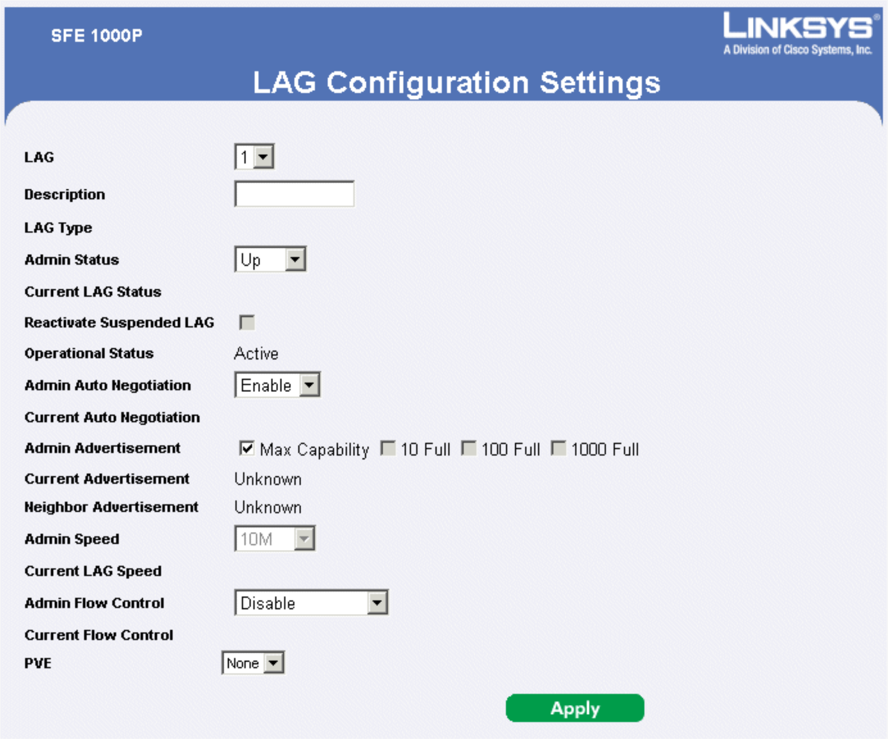
- **Copy from Entry Number** — Copies the LAG settings from the specified port.
- **To Entry Number(s)** — Assigns the copied LAG settings to the specified ports.
- **LAG** — Displays the LAG ID number.
- **Description** — Displays the user-defined port name.
- **Type** — The port types that comprise the LAG.
- **Status** — Indicates if the LAG is currently operating.
- **Speed** — The configured speed at which the LAG is operating.
- **Auto Negotiation** — The current Auto Negotiation setting. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

- **Flow Control** — 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.

## LAG Configuration Settings

*LAG Configuration Settings*



SFE 1000P

LAG Configuration Settings

| | |
|---|---|
| LAG | 1 |
| Description | |
| LAG Type | |
| Admin Status | Up |
| Current LAG Status | |
| 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 |

The *LAG Configuration Settings* contains the following fields:

- **LAG** — Displays the LAG ID number.

- **Description** — Displays the user-defined port name.

- **LAG Type** — 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.

- **Operational Status** — Defines 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, duplex mode and flow control (the flow control default is disabled) abilities to its partner.

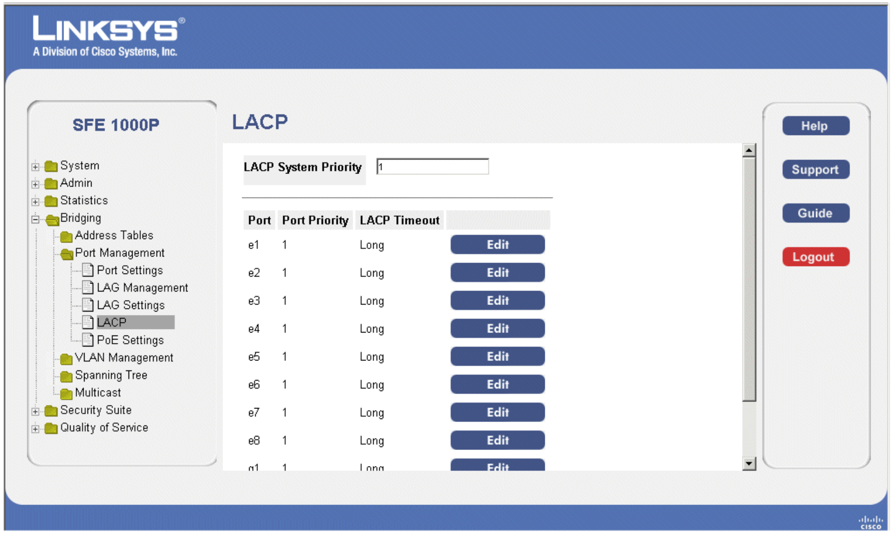
- **Current Auto Negotiation** — The current Auto Negotiation setting.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the LAG. The possible field values are:
  - *Max Capability* — Indicates that all LAG speeds and Duplex mode settings can be accepted.
  - *10 Half* — Indicates that the LAG is advertising a 10 Mbps speed and half Duplex mode setting.
  - *10 Full* — Indicates that the LAG is advertising a 10 Mbps speed and full Duplex mode setting.
  - *100 Half* — Indicates that the LAG is advertising a 100 Mbps speed and half 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** — 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.

# 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.

***LACP Page***



LACP

LACP System Priority: 1

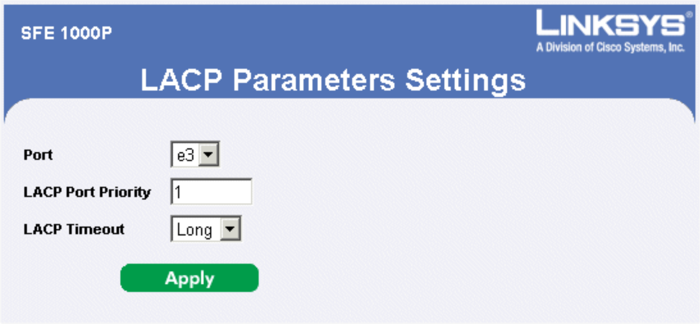
| Port | Port Priority | LACP Timeout | |
|---|---|---|---|
| e1 | 1 | Long | Edit |
| e2 | 1 | Long | Edit |
| e3 | 1 | Long | Edit |
| e4 | 1 | Long | Edit |
| e5 | 1 | Long | Edit |
| e6 | 1 | Long | Edit |
| e7 | 1 | Long | Edit |
| e8 | 1 | Long | Edit |
| g1 | 1 | Long | Edit |

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.
- **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

***Edit LACP Page***



SFE 1000P

LACP Parameters Settings

| | |
|---|---|
| Port | e3 |
| LACP Port Priority | 1 |
| LACP Timeout | Long |

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.
  - *Long* — Defines a long timeout value. This is the default value.

# Configuring VLANs

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router working at a protocol level is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

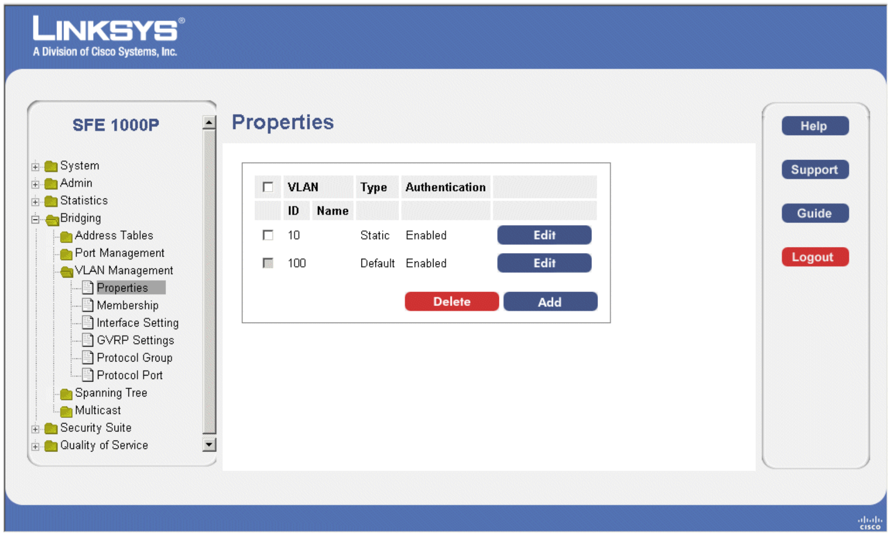
Combining VLANs and GARP (Generic Attribute Registration Protocol) allows network managers to define network nodes into Broadcast domains. The VLAN Management section contains the following pages:

- Defining VLAN Properties
- Defining VLAN Membership
- Defining Interface Settings
- Configuring GVRP Settings

## Defining VLAN Properties

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

***Properties Page***



Properties

| ☐ | VLAN ID | VLAN Name | Type | Authentication | |
|---|---|---|---|---|---|
| ☐ | 10 | | Static | Enabled | Edit |
| ☐ | 100 | | Default | Enabled | Edit |

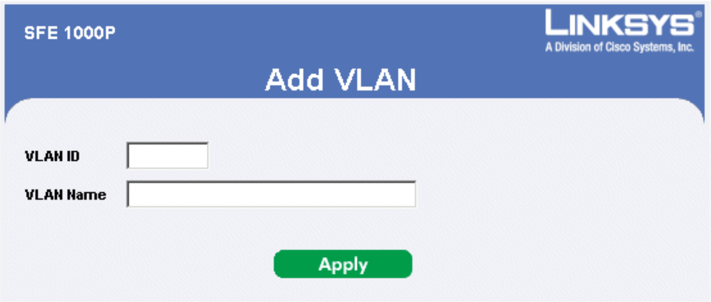
Delete Add

The *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 GARP.
  - *Static* — Indicates the VLAN is user-defined.
  - *Default* — Indicates the VLAN is the default VLAN.
- **Authentication** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - *Enable* — Enables unauthorized users to use the Guest VLAN.
  - *Disable* — Disables unauthorized users from using the Guest VLAN.

## Add VLAN

***Add VLAN Page***



SFE 1000P

Add VLAN

VLAN ID

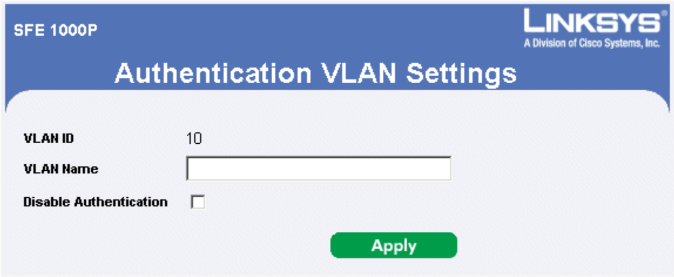
VLAN Name

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

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

## Modifying VLANs

***Edit VLAN Page***



SFE 1000P

Authentication VLAN Settings

VLAN ID 10

VLAN Name

Disable Authentication □

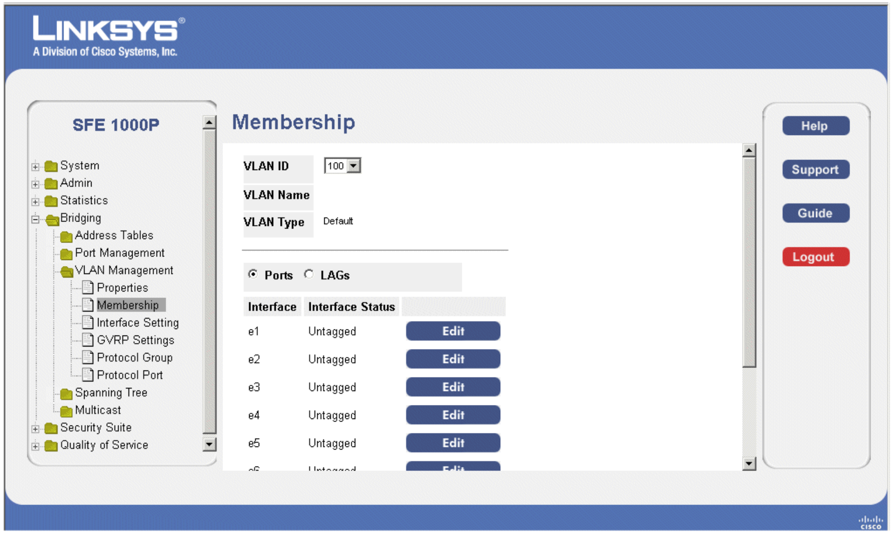
The *Edit VLAN Page* contains information for enabling VLAN guest authentication, and includes the following fields:

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

# Defining VLAN Membership

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

***Membership Page***



Membership

| | |
|---|---|
| VLAN ID | 100 |
| VLAN Name | |
| VLAN Type | Default |

● Ports ○ LAGs

| Interface | Interface Status | |
|---|---|---|
| e1 | Untagged | Edit |
| e2 | Untagged | Edit |
| e3 | Untagged | Edit |
| e4 | Untagged | Edit |
| e5 | Untagged | Edit |
| e6 | Untagged | Edit |

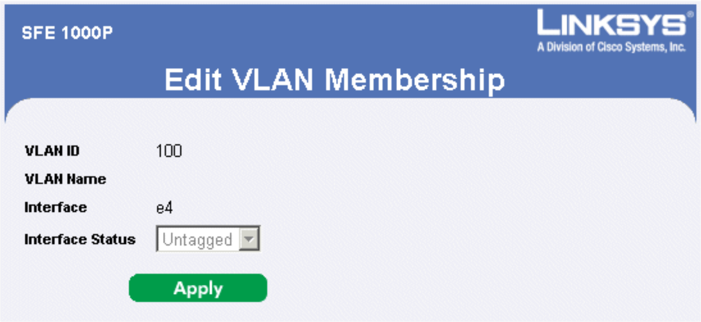
The *Membership Page* contains the following fields:

- **VLAN ID —** Displays 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 GARP.
  - *Static* — Indicates the VLAN is user-defined.
  - *Default* — Indicates the VLAN is the default VLAN.
- **Port** — Indicates that ports are described in the page.
- **LAG** — 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

***Edit VLAN Membership Page***



| | |
|---|---|
| VLAN ID | 100 |
| VLAN Name | |
| Interface | e4 |
| Interface Status | Untagged |

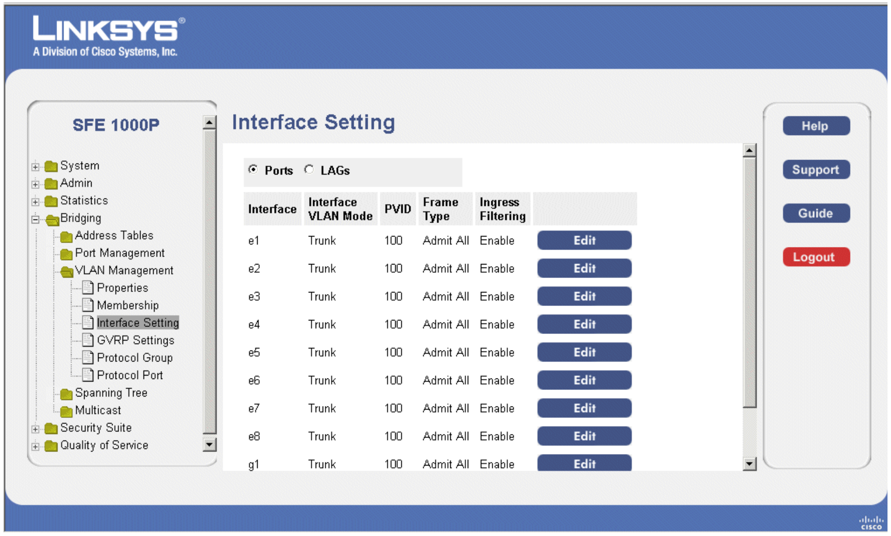
The *Edit VLAN Membership Page* contains the following fields:

- **VLAN ID —** Displays the VLAN ID.
- **VLAN Name** — Displays the VLAN name.
- **Interface** — Displays the port or LAG attached to the VLAN.
- **Interface Status** — Displays 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.

# Defining 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.

***Interface Setting Page***



Interface Setting

● Ports ○ LAGs

| Interface | Interface VLAN Mode | PVID | Frame Type | Ingress Filtering | |
|---|---|---|---|---|---|
| e1 | Trunk | 100 | Admit All | Enable | Edit |
| e2 | Trunk | 100 | Admit All | Enable | Edit |
| e3 | Trunk | 100 | Admit All | Enable | Edit |
| e4 | Trunk | 100 | Admit All | Enable | Edit |
| e5 | Trunk | 100 | Admit All | Enable | Edit |
| e6 | Trunk | 100 | Admit All | Enable | Edit |
| e7 | Trunk | 100 | Admit All | Enable | Edit |
| e8 | Trunk | 100 | Admit All | Enable | Edit |
| g1 | Trunk | 100 | Admit All | Enable | Edit |

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

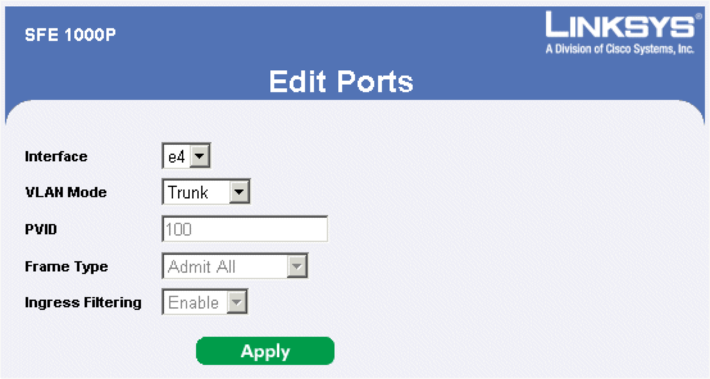
- **Port** — Indicates that ports are described in the page.
- **LAG** — Indicates that LAGs are described in the page.
- **Interface** — The port or LAG number included in the VLAN.
- **Interface VLAN Mode** — Indicates the interface membership status in the VLAN. The possible values are:
  - *General* — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (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 belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 2 to 4092, 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.

## Modifying VLAN Interface Settings

***Edit Ports Page***


SFE 1000P

Edit Ports

| | |
|---|---|
| Interface | e4 |
| VLAN Mode | Trunk |
| PVID | 100 |
| Frame Type | Admit All |
| Ingress Filtering | Enable |

The *Edit Ports Page* contains the following fields:

- **Interface** — The port or LAG associated with this interface configuration.
- **VLAN Mode** — Indicates the port mode. Possible values are:
  - *General* — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (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 belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 2 to 4092, 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.

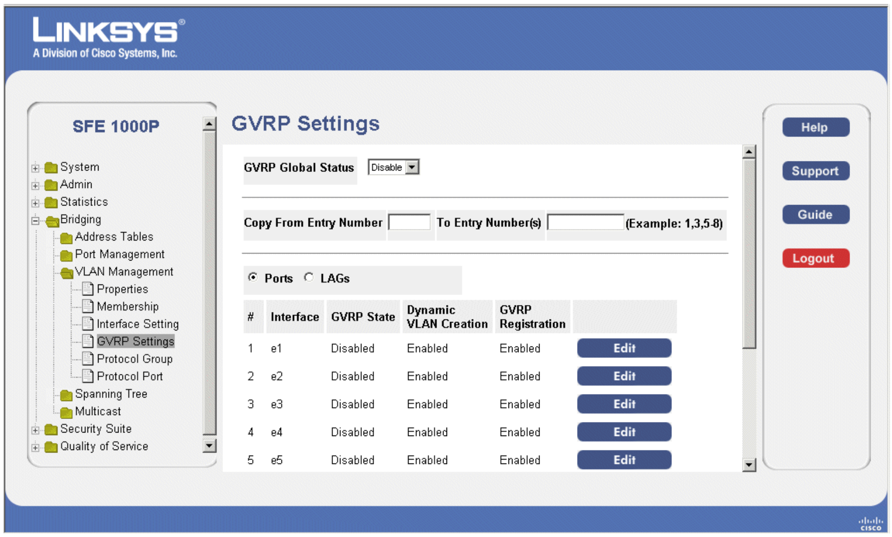
## Configuring GVRP Settings

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.

To define GVRP:

**NOTE:** The Global System LAG information displays the same field information as the ports, but represent the LAG GVRP information.

***GVRP Settings Page***



GVRP Settings

GVRP Global Status: Disable

Copy From Entry Number ____ To Entry Number(s) ____ (Example: 1,3,5-8)

● Ports ○ LAGs

| # | Interface | GVRP State | Dynamic VLAN Creation | GVRP Registration | |
|---|---|---|---|---|---|
| 1 | e1 | Disabled | Enabled | Enabled | Edit |
| 2 | e2 | Disabled | Enabled | Enabled | Edit |
| 3 | e3 | Disabled | Enabled | Enabled | Edit |
| 4 | e4 | Disabled | Enabled | Enabled | Edit |
| 5 | e5 | Disabled | Enabled | Enabled | Edit |

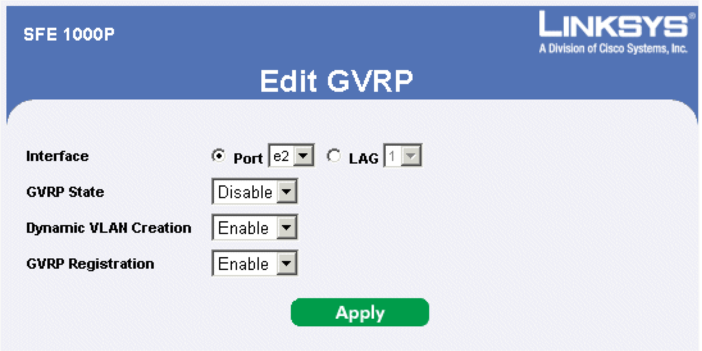
The *GVRP Settings Page* contains the following fields:

- **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** — Specifies the row number from which GVRP parameters are copied.
- **To Entry Number** — Specifies the row to which the copied GVRP parameters are assigned.
- **Port** — Displays the GVRP configurations for specified port number.
- **LAGs** — Displays the GVRP configurations for LAGs.

- **Interface** — Indicates the interface for which the GVRP configuration is displayed.
- **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.

## Modifying GVRP Settings

***Edit GVRP Page***



| | |
|---|---|
| Interface | ● Port e2 ○ LAG 1 |
| GVRP State | Disable |
| Dynamic VLAN Creation | Enable |
| GVRP Registration | Enable |

The *Edit GVRP Page* contains the following fields:

- **Interface** — Displays the interface on which GVRP is enabled. The possible field values are:
  - *Port* — Indicates the port number on which GVRP is enabled.
  - *LAG* — Indicates the LAG number on which GVRP is enabled.
- **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:

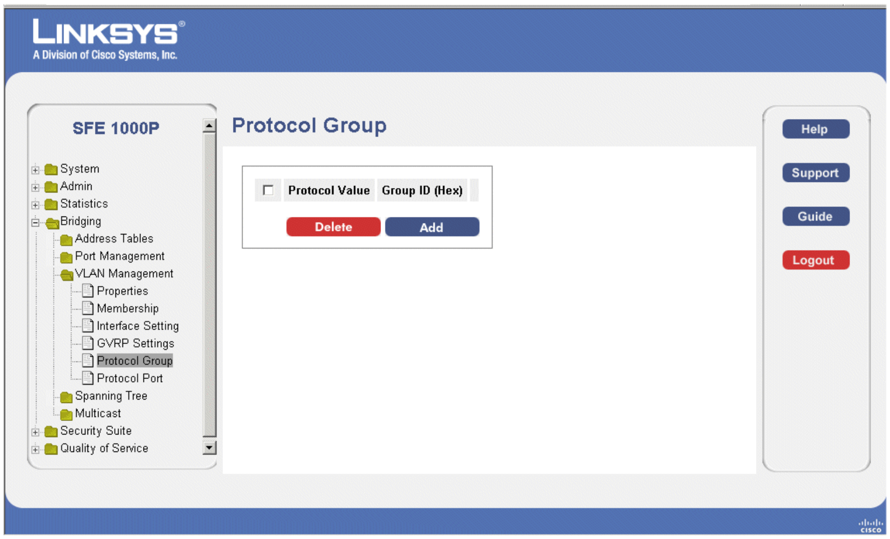
- *Enable* — Enables Dynamic VLAN creation on the interface.
- *Disable* — Disables Dynamic VLAN creation on the interface.

- **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.

# Defining VLAN Protocol Group

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 Group Page***



Protocol Group

| □ | Protocol Value | Group ID (Hex) |
|---|---|---|

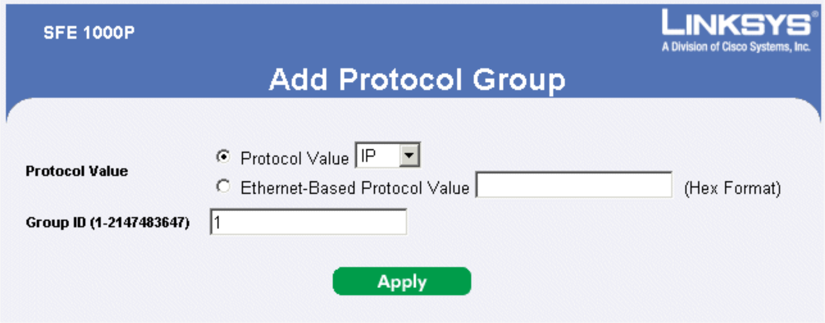
The *Protocol Group Page* contains the following fields:

- **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.

## Add Protocol Group

The *Add Protocol Group Page* provides information for configuring new VLAN protocol groups.

***Add Protocol Group Page***



Add Protocol Group

Protocol Value: ● Protocol Value IP
○ Ethernet-Based Protocol Value (Hex Format)

Group ID (1-2147483647): 1

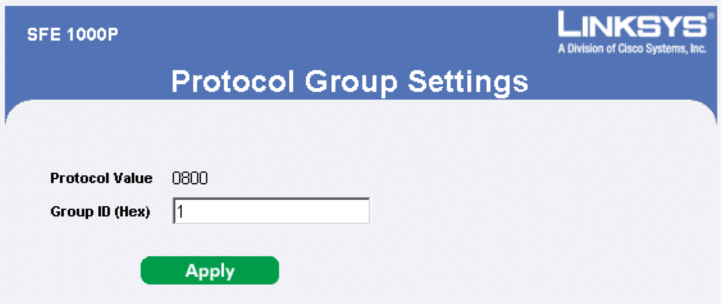
The *Add Protocol Group Page* contains the following fields.

- **Protocol Value —** Displays 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. The possible value range is 1-2147483647 in hexadecimal format.

## Modifying Protocol Groups

The *Protocol Group Settings Page* provides information for configuring existing VLAN protocol groups.

***Protocol Group Settings Page***



Protocol Group Settings

Protocol Value: 0800

Group ID (Hex): 1

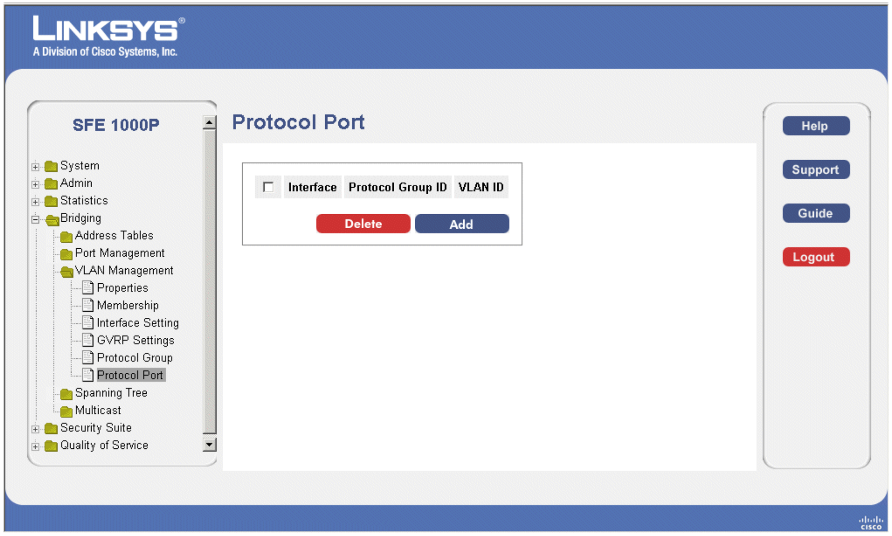
The *Protocol Group Settings Page* contains the following fields.

- **Protocol Value —** Displays the User-defined protocol value.
- **Group ID (Hex) —** Defines the Protocol group ID to which the interface is assigned. The possible value range is 1-2147483647 in hexadecimal format.

# Defining VLAN Protocol Port

The *Protocol Port Page* adds interfaces to Protocol groups.

***Protocol Port Page***



| □ | Interface | Protocol Group ID | VLAN ID |
|---|---|---|---|

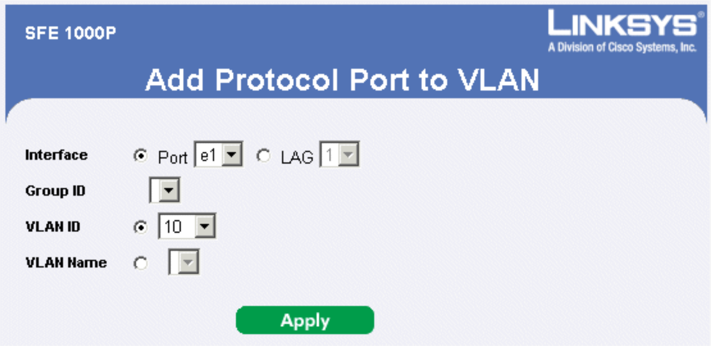
The *Protocol Port Page* contains the following fields.

- **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.

## Add Protocol Port to VLAN

The *Add Protocol Port to VLAN Page* provides parameters for adding protocol port configurations.

***Add Protocol Port to VLAN Page***



| | | |
|---|---|---|
| Interface | ● Port e1 | ○ LAG 1 |
| Group ID | | |
| VLAN ID | ● 10 | |
| VLAN Name | ○ | |

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.

# Configuring IP Information

This section provides information for defining device IP addresses, and includes the following topics:

- Domain Name System
- Configuring Layer 2IP Addresses
- Configuring Layer 3

## 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:

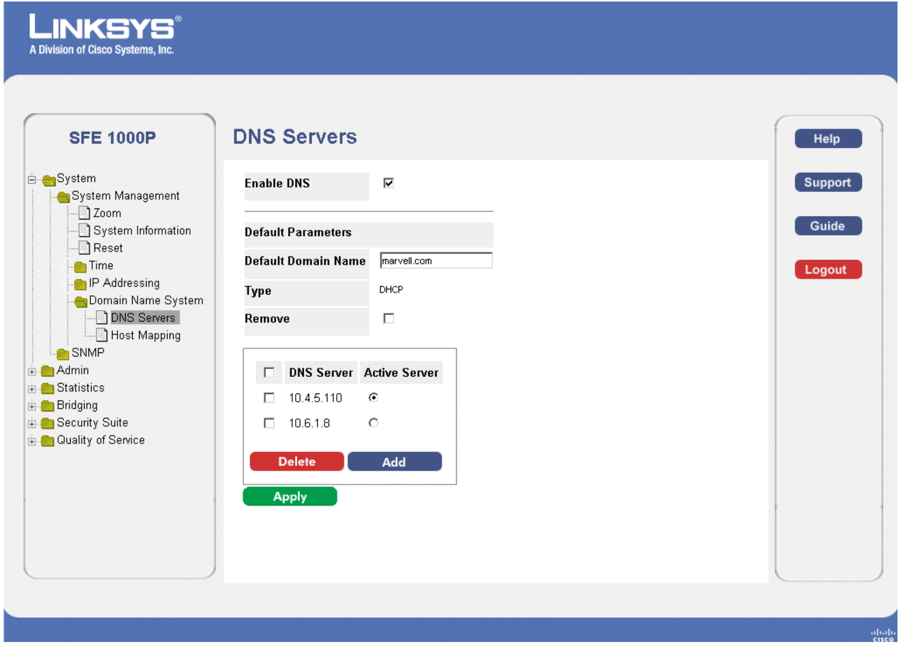
- Defining DNS Server
- Mapping DNS Hosts

### Defining DNS Server

*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 *DNS Servers Page* contains fields for enabling and activating specific DNS servers.

***DNS Servers Page***



DNS Servers

| | |
|---|---|
| Enable DNS | ☑ |
| Default Parameters | |
| Default Domain Name | marvell.com |
| Type | DHCP |
| Remove | □ |

| □ | DNS Server | Active Server |
|---|---|---|
| □ | 10.4.5.110 | ● |
| □ | 10.6.1.8 | ○ |

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

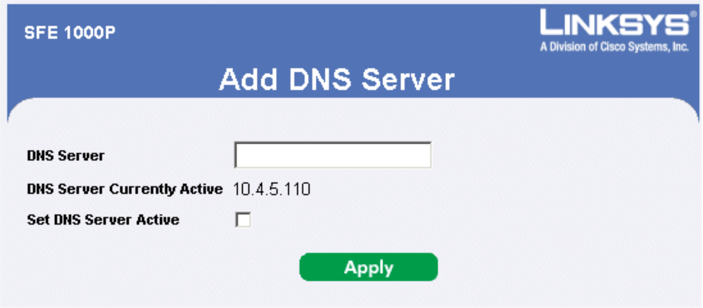
- **DNS Server** — Displays the DNS server's IP address.

- **Active Server** — Specifies the DNS server that is currently active.

## Add DNS Server

The *Add DNS Server Page* allows system administrators to define new DNS servers.

***Add DNS Server Page***



| | |
|---|---|
| DNS Server | |
| DNS Server Currently Active | 10.4.5.110 |
| Set DNS Server Active | □ |

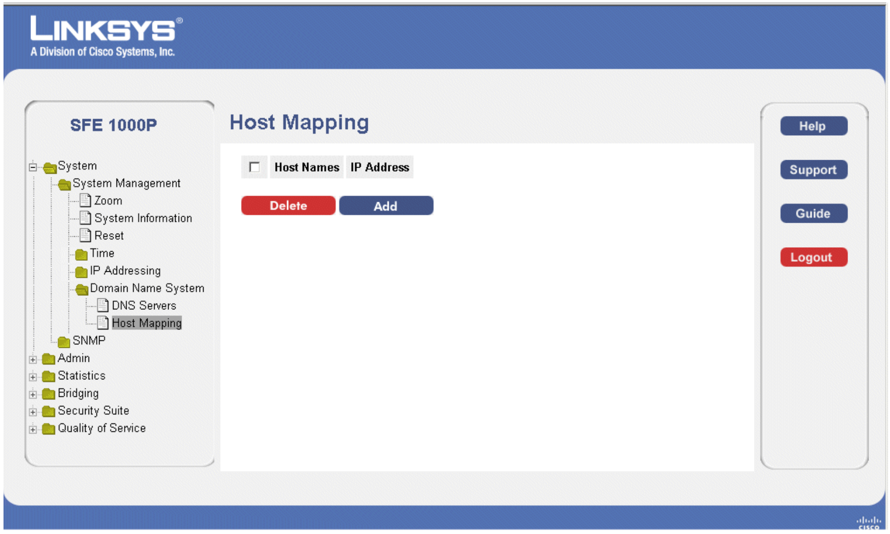
The Add DNS Server Page page contains the following fields.

- **DNS Server** — Displays the DNS server's IP address.
- **DNS Server Currently Active** — Displays the DNS server which is currently active.
- **Set DNS Server Active** — Indicates 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.

## Mapping DNS Hosts

The *Host Mapping Page* provides information for defining DNS Host Mapping.

***Host Mapping Page***



The *Host Mapping Page* contains the following fields:

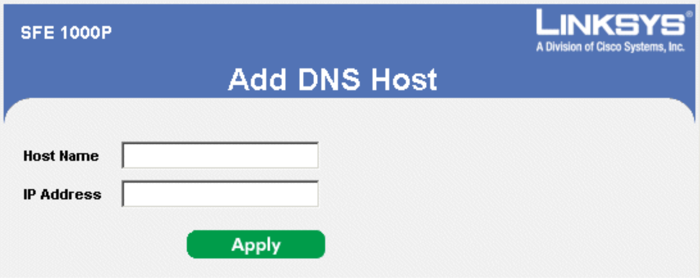
- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.

- **IP Address** — Displays the DNS host IP address.

## Add DNS Host

The *Add DNS Host Page* provides information for defining DNS Host Mapping.

***Add DNS Host Page***



The *Add DNS Host* page contains the following fields:

- **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.

# Configuring Layer 2 IP Addresses

The IP address and default gateway can be either dynamically or statically configured. In Layer 2, a static IP address is configured on the *VLAN Management Properties Page*. The Management VLAN is set to VLAN 100 by default, but can be modified.

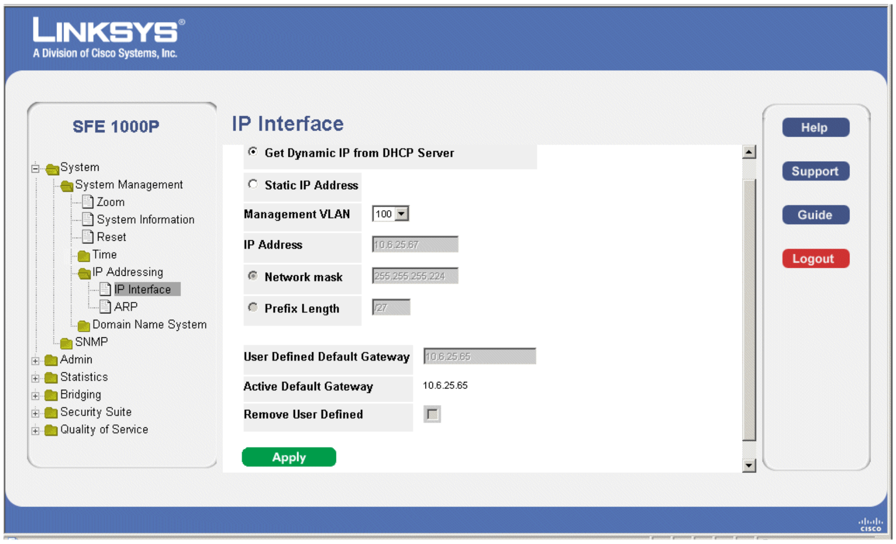
This section provides information for configuring Layer 2 features, and includes the following topics:

- Defining IP Routing
- Enabling ARP

## Defining IP Interfaces

The *IP Interface Page* contains fields for assigning IP 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.

***IP Interface Page***



IP Interface

● Get Dynamic IP from DHCP Server

○ Static IP Address

| | |
|---|---|
| Management VLAN | 100 |
| IP Address | 10.6.25.67 |
| ● Network mask | 255.255.255.224 |
| ○ Prefix Length | /27 |
| User Defined Default Gateway | 10.6.25.65 |
| Active Default Gateway | 10.6.25.65 |
| Remove User Defined | □ |

The *IP Interface Page* contains the following fields:

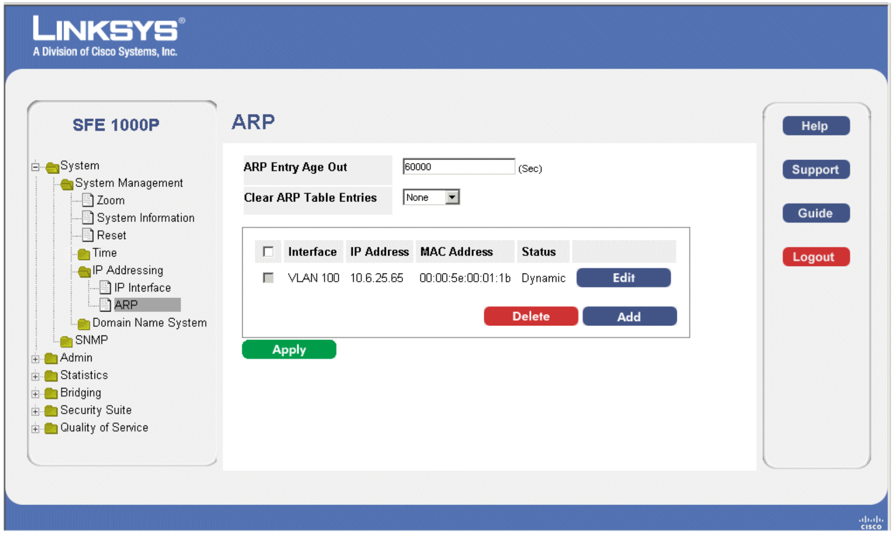
- **Get Dynamic IP from DHCP Server** — Retrieves the IP addresses using DHCP.
- **Static IP Address** — Permanent IP addresses are defined by the administrator. IP addresses are either configured on the Default VLAN or are user-defined.
- **Management VLAN** — Sets the management VLAN. The switch uses this VLAN to watch for management packets from Telnet and web browser management sessions.
- **IP Address** — Displays the currently configured IP address.
- **Network Mask** — Displays the currently configured IP address mask.

- **Prefix Length** — Specifies the number of bits that comprise the source IP address prefix, or the network source IP address mask.
- **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.

## Enabling ARP

The *Address Resolution Protocol* (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. 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.

***ARP Page***



ARP

ARP Entry Age Out: 60000 (Sec)

Clear ARP Table Entries: None

| □ | Interface | IP Address | MAC Address | Status | |
|---|---|---|---|---|---|
| □ | VLAN 100 | 10.6.25.65 | 00:00:5e:00:01:1b | Dynamic | Edit |

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:
  - *None* — ARP entries are not cleared.

  - *All* — All ARP entries are cleared.
  - *Dynamic* — Only dynamic ARP entries are cleared.
  - *Static* — Only static ARP entries are cleared.

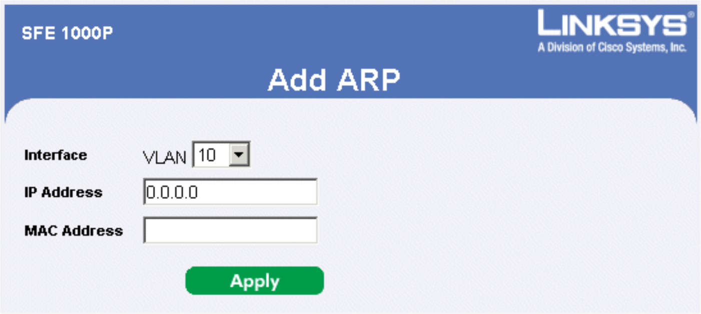
ARP Entries

- **Interface** — Indicates the interface connected to the device.
- **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** — 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.

## Add ARP

The *Add ARP Page* allows you to enter ARP addresses.

***Add ARP Page***



| | |
|---|---|
| Interface | VLAN 10 |
| IP Address | 0.0.0.0 |
| MAC Address | |

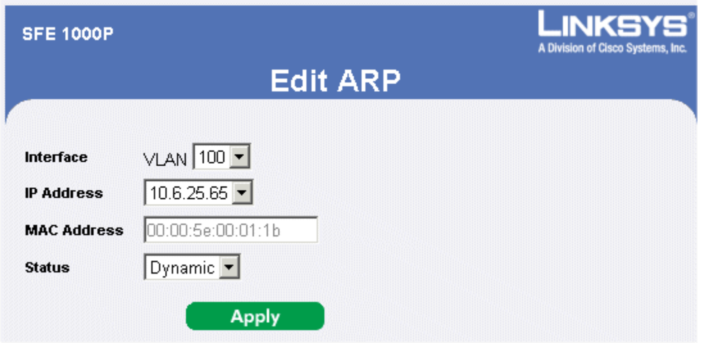
The *Add ARP Page* contains the following fields:

- **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.**

## Modifying ARP Settings

The *Edit ARP Page* allows you to manually edit ARP addresses.

***Edit ARP Page***



SFE 1000P

Edit ARP

| | |
|---|---|
| Interface | VLAN 100 |
| IP Address | 10.6.25.65 |
| MAC Address | 00:00:5e:00:01:1b |
| Status | Dynamic |

The *Edit ARP Page* contains the following fields:

- **Interface** — Indicates the interface connected to the device.
- **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** — 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.

# 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.

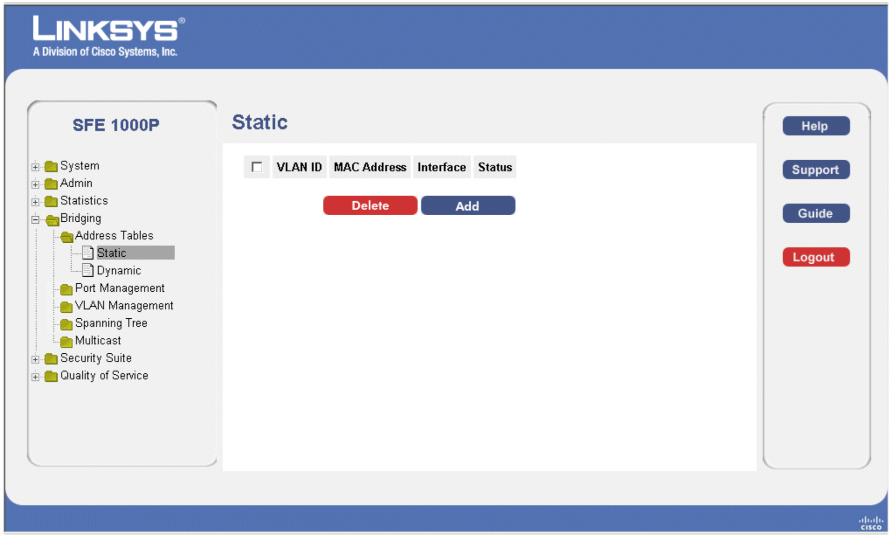
This section contains information for defining both static and dynamic Forwarding Database entries, and includes the following topics:

- 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.

***Static Page***



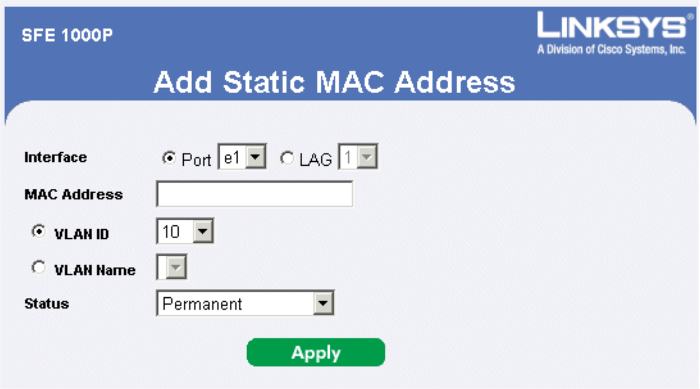
The *Static Page* contains the following fields:

- **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:
  - *Secure* — The MAC Address is defined for locked ports.
  - *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.

## Add Static MAC Address

***Add Static MAC Address Page***



Add Static MAC Address

| | |
|---|---|
| Interface | ● Port e1 ○ LAG 1 |
| MAC Address | |
| ● VLAN ID | 10 |
| ○ VLAN Name | |
| Status | Permanent |

The *Add Static MAC Address Page* contains the following fields:

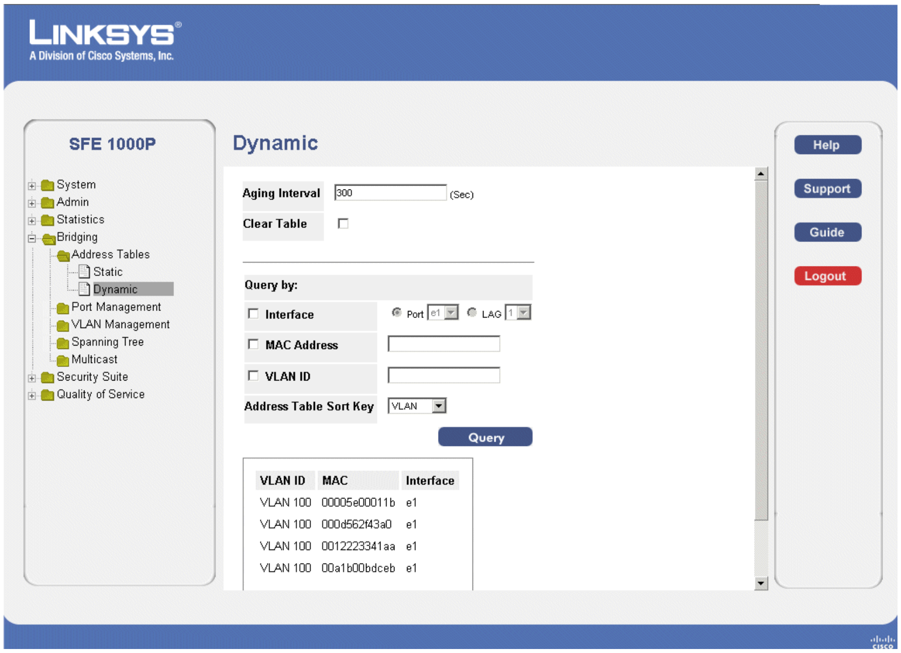
- **Interface** — Displays the interface to which the entry refers:
  - *Port* — The specific port number to which the forwarding database parameters refer.
  - *LAG* — The specific LAG number to which the forwarding database parameters refer.
- **MAC Address** — Displays the MAC address to which the 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.

# 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.

***Dynamic Page***



Dynamic

Aging Interval 300 (Sec)

Clear Table □

Query by:

□ Interface ● Port e1 ○ LAG 1

□ MAC Address

□ VLAN ID

Address Table Sort Key VLAN

Query

| VLAN ID | MAC | Interface |
|---|---|---|
| VLAN 100 | 00005e00011b | e1 |
| VLAN 100 | 000d562f43a0 | e1 |
| VLAN 100 | 0012223341aa | e1 |
| VLAN 100 | 00a1b00bdceb | e1 |

The *Dynamic Page* contains the following fields:

- **Aging Interval (secs)** — 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.

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.

# Configuring Multicast Forwarding

The Multicast section contains the following pages:

- IGMP Snooping
- Defining Multicast Bridging Groups
- Defining Multicast Forwarding

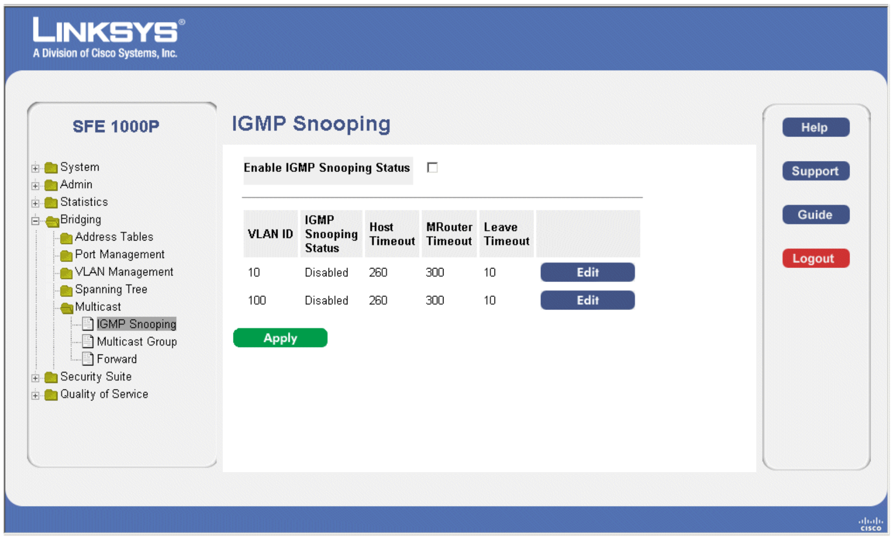
## IGMP Snooping

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.

***IGMP Snooping Page***



IGMP Snooping

Enable IGMP Snooping Status □

| VLAN ID | IGMP Snooping Status | Host Timeout | MRouter Timeout | Leave Timeout | |
|---|---|---|---|---|---|
| 10 | Disabled | 260 | 300 | 10 | Edit |
| 100 | Disabled | 260 | 300 | 10 | Edit |

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:

  - – *Enable* — Enables IGMP Snooping on the VLAN.

  - – *Disable* — Disables IGMP Snooping 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.

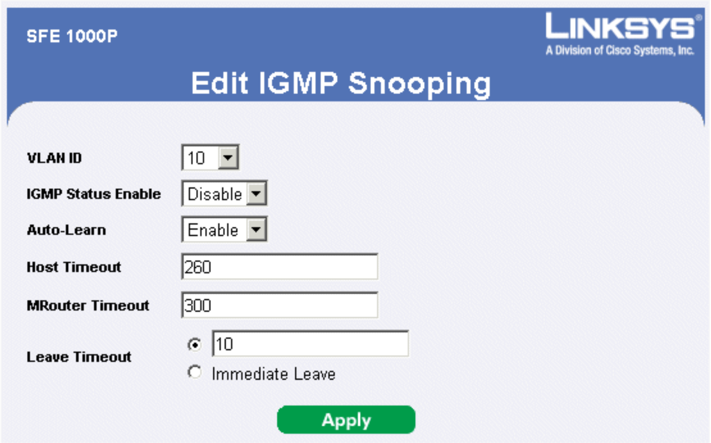
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.

- **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.

## Modifying IGMP Snooping

The *Edit IGMP Snooping Page* provides a means of configuring snooping parameters.

***Edit IGMP Snooping Page***



SFE 1000P

Edit IGMP Snooping

| | |
|---|---|
| VLAN ID | 10 |
| IGMP Status Enable | Disable |
| Auto-Learn | Enable |
| Host Timeout | 260 |
| MRouter Timeout | 300 |
| Leave Timeout | ● 10<br>○ Immediate Leave |

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.

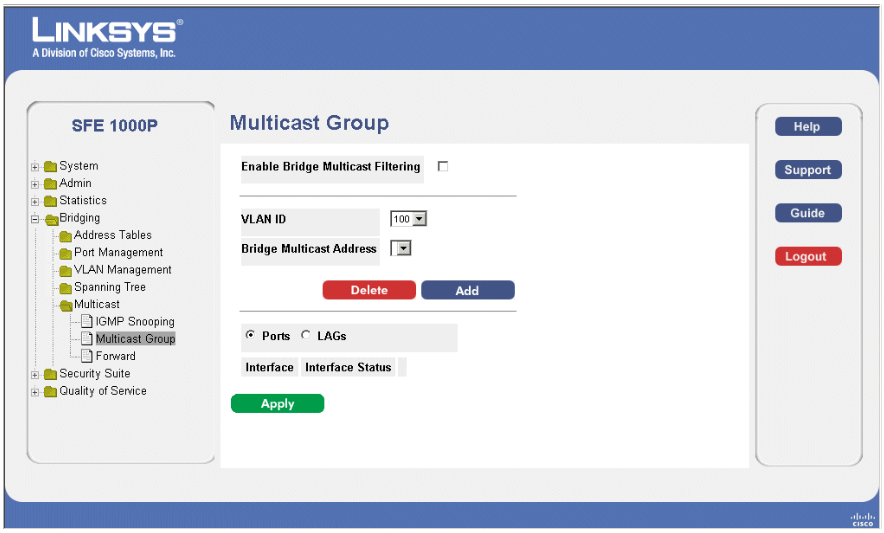
  - – *Disable* — Disables IGMP Snooping on the VLAN.

- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device.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.

## Defining Multicast Bridging Groups

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.

***Multicast Group Page***



Multicast Group

Enable Bridge Multicast Filtering ☐

VLAN ID 100

Bridge Multicast Address

● Ports ○ LAGs

Interface | Interface Status

The *Multicast Group Page* contains the following fields:

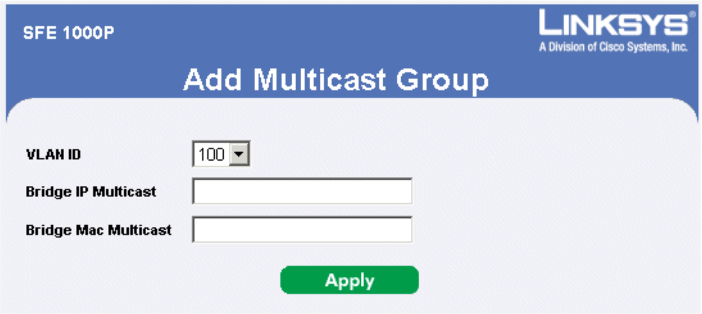
- **Enable Bridge Multicast Filtering** — Indicates if Bridge Multicast Filtering is enabled on the device. Bridge Multicast Filtering can be enabled only if IGMP Snooping is enabled. The possible field values are:

- *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 device'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.
  - *Dynamic* — Attaches the interface dynamically to the Multicast group.
  - *Excluded* — The interface is not part of a Multicast group.

## Add Multicast Group

***Add Multicast Group Page***



SFE 1000P

Add Multicast Group

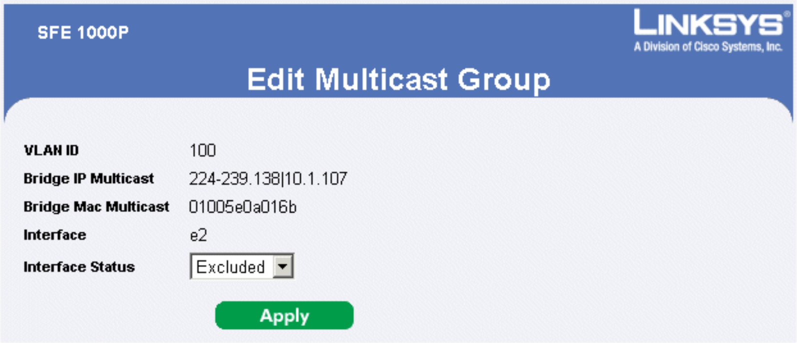
| | |
|---|---|
| VLAN ID | 100 ▾ |
| Bridge IP Multicast | |
| Bridge Mac Multicast | |

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.

## Modifying a Multicast Group

***Edit Multicast Group Page***



| | |
|---|---|
| VLAN ID | 100 |
| Bridge IP Multicast | 224-239.138\|10.1.107 |
| Bridge Mac Multicast | 01005e0a016b |
| Interface | e2 |
| Interface Status | Excluded |

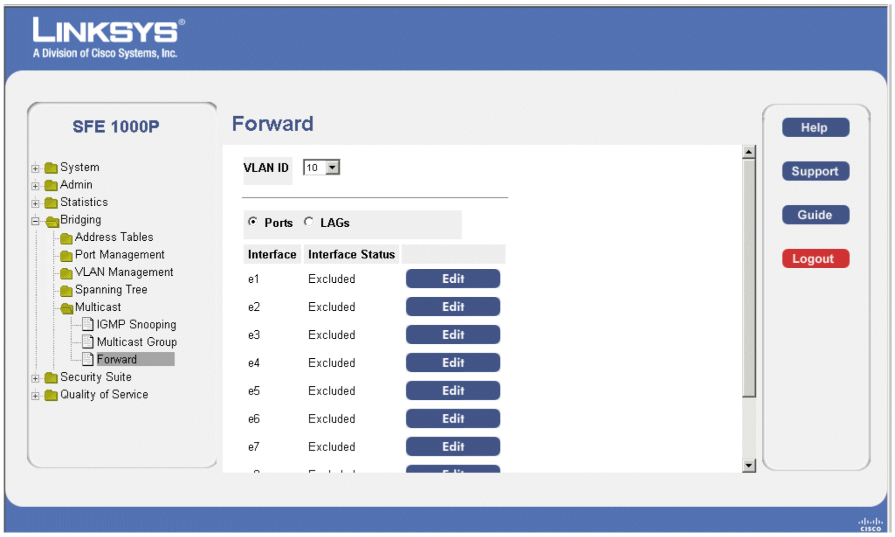
The *Edit Multicast Group Page* contains the following fields:

- **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.
- **Interface** — Displays the interface attached to the Multicast Group.
- **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.
  - *Dynamic* — Attaches the interface dynamically to the Multicast group.
  - *Excluded* — The interface is not part of a Multicast group.

# 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.

***Multicast Forward Page***



Forward

VLAN ID 10

● Ports ○ LAGs

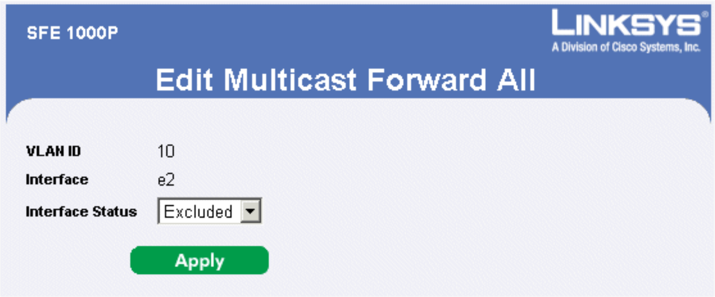
| Interface | Interface Status | |
|---|---|---|
| e1 | Excluded | Edit |
| e2 | Excluded | Edit |
| e3 | Excluded | Edit |
| e4 | Excluded | Edit |
| e5 | Excluded | Edit |
| e6 | Excluded | Edit |
| e7 | Excluded | Edit |

The *Multicast Forward Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Ports** — Displays the Multicast Forwarding status of all of the device'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 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.
  - *Dynamic* — Attaches the interface or LAG dynamically to the Multicast group.
  - *Excluded* — The interface is not part of a Multicast group.

## Modifying Multicast Forwarding

***Edit Multicast Forward All Page***



Edit Multicast Forward All

VLAN ID 10

Interface e2

Interface Status Excluded

The *Edit Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Interface** — Displays the port or LAG on which Multicast forwarding is configured.
- **Interface Status** — Displays the interface status. The possible values are:
  - *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.
  - *Dynamic* — Attaches the interface dynamically to the Multicast group.
  - *Excluded* — The interface is not part of a Multicast group.

# 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.

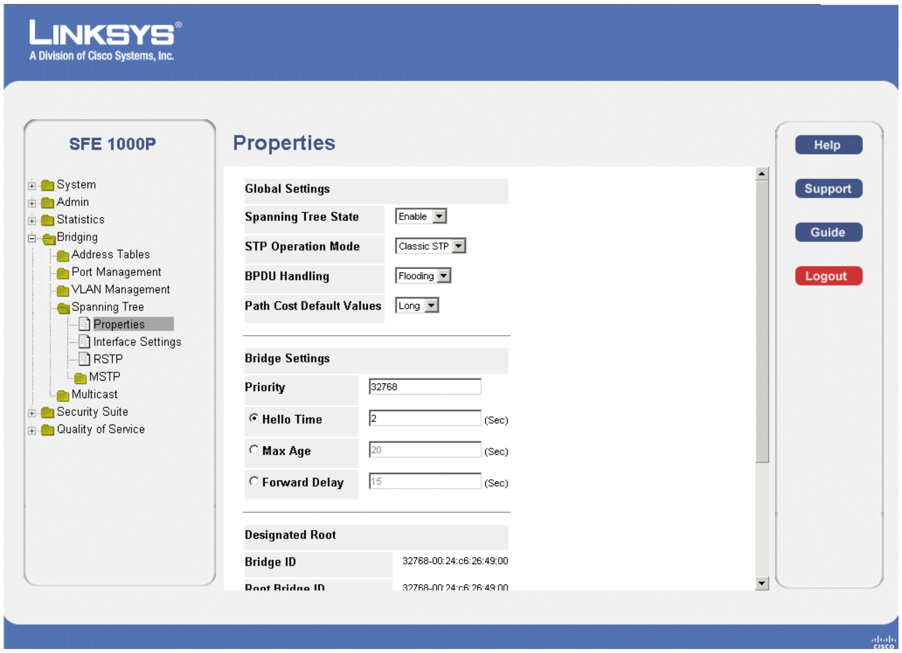
The device supports the following Spanning Tree versions:

- **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.
- The Spanning Tree section contains the following pages:
- Defining STP Properties
- Defining Interface Settings
- Defining Rapid Spanning Tree
- Defining Multiple 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.

***STP Properties Page***



Properties

| | |
|---|---|
| **Global Settings** | |
| Spanning Tree State | Enable |
| STP Operation Mode | Classic STP |
| BPDU Handling | Flooding |
| Path Cost Default Values | Long |
| **Bridge Settings** | |
| Priority | 32768 |
| ● Hello Time | 2 (Sec) |
| ○ Max Age | 20 (Sec) |
| ○ Forward Delay | 15 (Sec) |
| **Designated Root** | |
| Bridge ID | 32768-00:24:c6:26:49:00 |
| Root Bridge ID | 32768-00:24:c6:26:49:00 |

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 65535.
- **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.

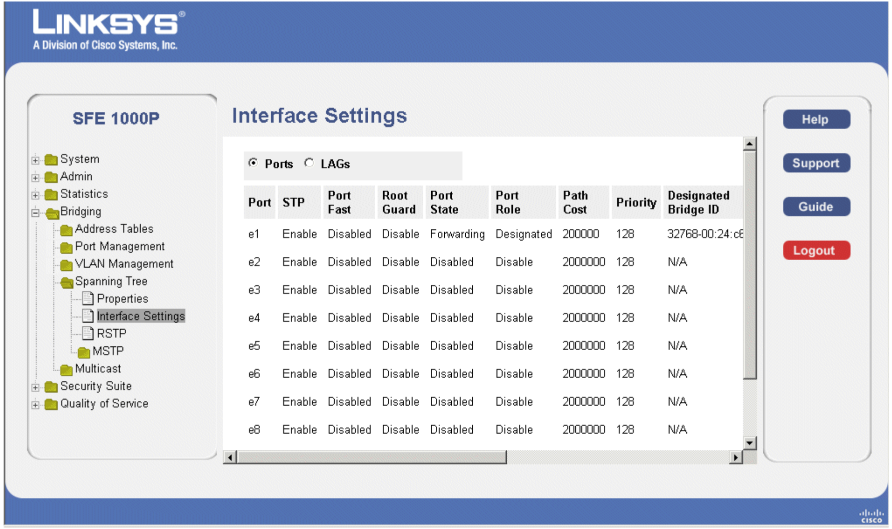
The Designated Root area contains the following fields:

- **Bridge ID** — Identifies the Bridge ID 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. The default is zero.
- **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.

# Defining Interface Settings

Network administrators can assign STP settings to specific interfaces using the *STP Interface Settings Page*.

***Interface Settings Page***



Interface Settings

● Ports ○ LAGs

| Port | STP | Port Fast | Root Guard | Port State | Port Role | Path Cost | Priority | Designated Bridge ID |
|---|---|---|---|---|---|---|---|---|
| e1 | Enable | Disabled | Disable | Forwarding | Designated | 200000 | 128 | 32768-00:24:c6 |
| e2 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e3 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e4 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e5 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e6 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e7 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |
| e8 | Enable | Disabled | Disable | Disabled | Disable | 2000000 | 128 | N/A |

The *STP Interface Settings Page* contains the following fields:

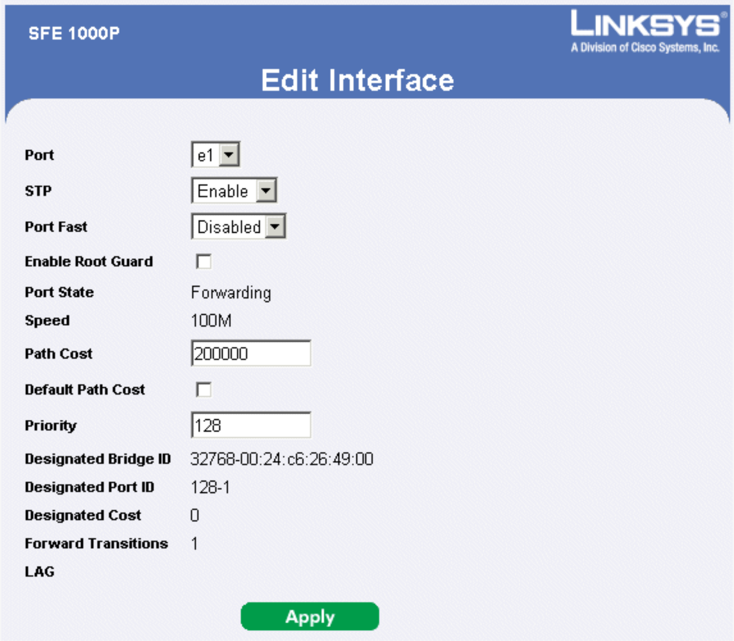
- **Ports** — Display the STP Interface settings of device ports.
- **LAGs** — Display the STP Interface settings of device LAGs.
- **Port** — Indicates the port or LAG on which STP is enabled.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enable* — Indicates that STP is enabled on the port.
  - *Disables* — 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:
  - *Enable* — Port Fast is enabled.
  - *Disable* — 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.

- **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 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.

## Modifying Interface Settings

***Edit Interface Settings Page***



| | |
|---|---|
| Port | e1 |
| STP | Enable |
| Port Fast | Disabled |
| Enable Root Guard | □ |
| Port State | Forwarding |
| Speed | 100M |
| Path Cost | 200000 |
| Default Path Cost | □ |
| Priority | 128 |
| Designated Bridge ID | 32768-00:24:c6:26:49:00 |
| Designated Port ID | 128-1 |
| Designated Cost | 0 |
| Forward Transitions | 1 |
| LAG | |

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

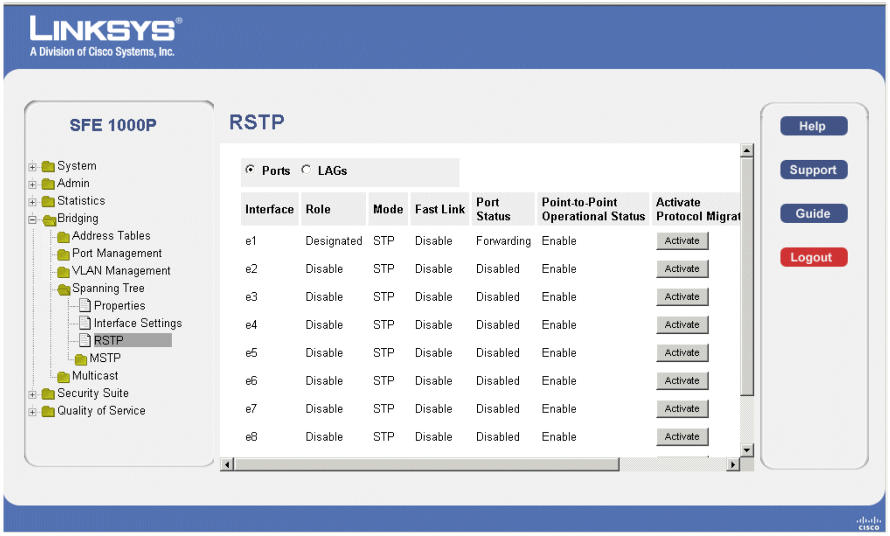
- **Port** — Indicates the port number on which Spanning Tree is configured.
- **STP** — Indicates if STP is enable on the port. The possible field values are:
  - *Enable* — Indicates that STP is enabled on the port.
  - *Disable* — Indicates that STP is disabled on the port.
- **Port Fast** — Indicates 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:
  - *Enable* — Port Fast is enabled.
  - *Disable* — Port Fast is disabled.
  - *Auto* — Port Fast mode is enabled 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.

- **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.
- **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.

# 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.

***RSTP Page***



RSTP

● Ports ○ LAGs

| Interface | Role | Mode | Fast Link | Port Status | Point-to-Point Operational Status | Activate Protocol Migrat |
|---|---|---|---|---|---|---|
| e1 | Designated | STP | Disable | Forwarding | Enable | Activate |
| e2 | Disable | STP | Disable | Disabled | Enable | Activate |
| e3 | Disable | STP | Disable | Disabled | Enable | Activate |
| e4 | Disable | STP | Disable | Disabled | Enable | Activate |
| e5 | Disable | STP | Disable | Disabled | Enable | Activate |
| e6 | Disable | STP | Disable | Disabled | Enable | Activate |
| e7 | Disable | STP | Disable | Disabled | Enable | Activate |
| e8 | Disable | STP | Disable | Disabled | Enable | Activate |

The *RSTP Page* contains the following fields:

- **Ports/LAG** — Specifies whether the RSTP configurations for ports or LAGs are displayed in the table.
- **Interface** — Indicates the port or LAG on which RSTP is enabled.
- **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.
  - *Enable* — Fast Link is enabled.
  - *Disable* — Fast Link is disabled.
  - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.

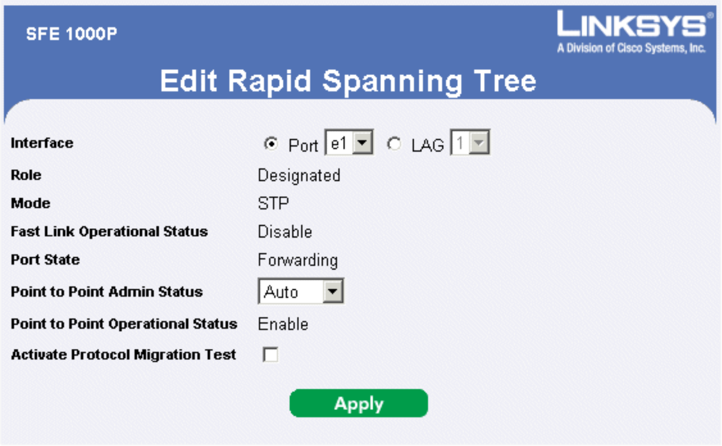
- **Port Status** — Indicates the RSTP status on the specific port. The possible field values are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward 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.

- **Point-to-Point Operational Status** — Indicates the Point-to-Point operating state.

- **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.

## Modifying RTSP

***Edit Rapid Spanning Tree Page***



Edit Rapid Spanning Tree

| | |
|---|---|
| Interface | ● Port e1 ○ LAG 1 |
| Role | Designated |
| Mode | STP |
| Fast Link Operational Status | Disable |
| Port State | Forwarding |
| Point to Point Admin Status | Auto |
| Point to Point Operational Status | Enable |
| Activate Protocol Migration Test | □ |

The *Edit Rapid Spanning Tree Page* contains the following fields:

- **Interface** — Specifies whether Rapid STP is enabled 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 Status** — Indicates the RSTP 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.

- **Point-to-Point Admin Status** — Indicates if a point-to-point links is established, or permits the device to establish a point-to-point link. The possible field values are:
  - *Enable* — Enables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.
  - *Disable* — Disables point-to-point link.
  - *Auto* — The device automatically establishes a point-to-point link.

- **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* — Protocol Migration is enabled.
  - *Unchecked* — Protocol Migration is disabled.

## 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.

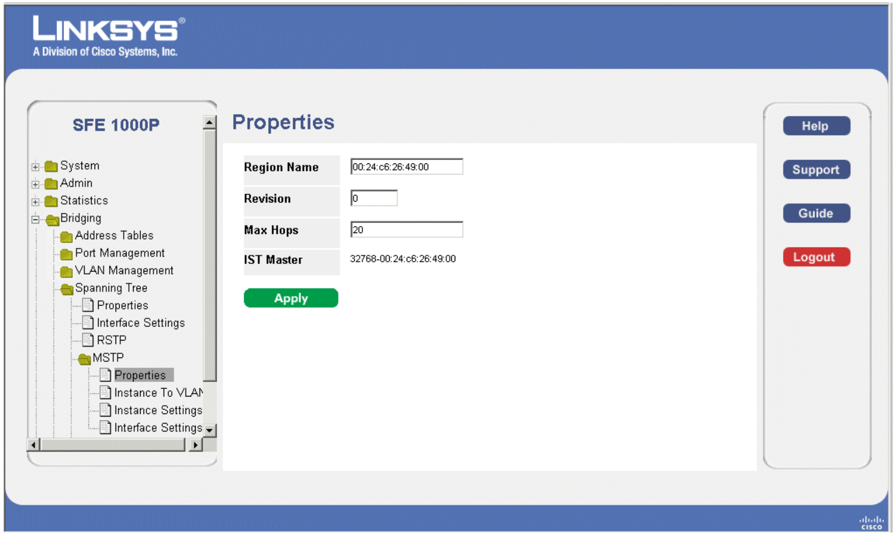
The MSTP section contains the following pages:

- Defining MSTP Properties
- Mapping MSTP Instances 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.

***MSTP Properties Page***



Properties

| | |
|---|---|
| Region Name | 00:24:c6:26:49:00 |
| Revision | 0 |
| Max Hops | 20 |
| IST Master | 32768-00:24:c6:26:49:00 |

The *MSTP Properties Page* contains the following fields:

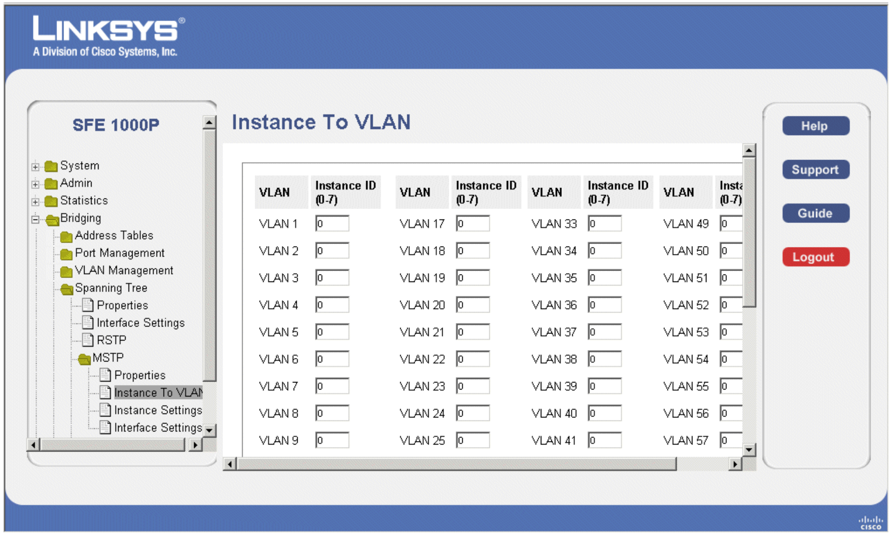
- **Region Name** — Provides a user-defined STP region name.
- **Revision** — Defines unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration. The possible field range 0-65535.
- **Max Hops** — Indicates the 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.

## Mapping MSTP Instances 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.

***Instance to VLAN Page***



Instance To VLAN

| VLAN | Instance ID (0-7) | VLAN | Instance ID (0-7) | VLAN | Instance ID (0-7) | VLAN | Insta (0-7) |
|---|---|---|---|---|---|---|---|
| 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 |

The *Instance to VLAN Page* contains the following fields:

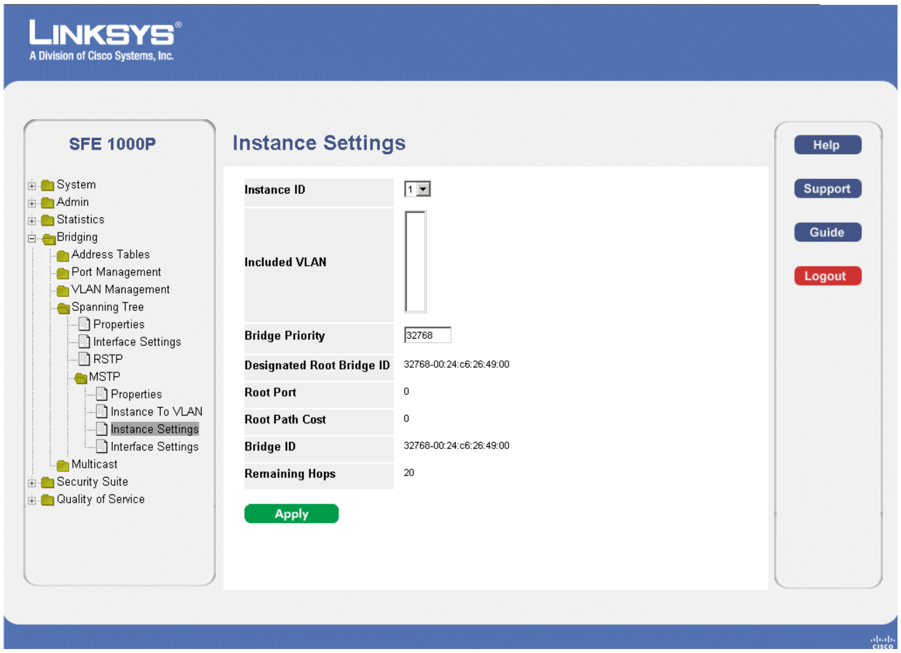
- **VLAN** — Indicates the VLAN for which the MSTP instance ID is defined.
- **Instance ID (0-7)** — Indicates the MSTP instance ID assigned to the VLAN. The possible field range is 0-7.

## 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*.

***MSTP Instance Settings Page***



Instance Settings

| | |
|---|---|
| Instance ID | 1 |
| Included VLAN | |
| Bridge Priority | 32768 |
| Designated Root Bridge ID | 32768-00:24:c6:26:49:00 |
| Root Port | 0 |
| Root Path Cost | 0 |
| Bridge ID | 32768-00:24:c6:26:49:00 |
| Remaining Hops | 20 |

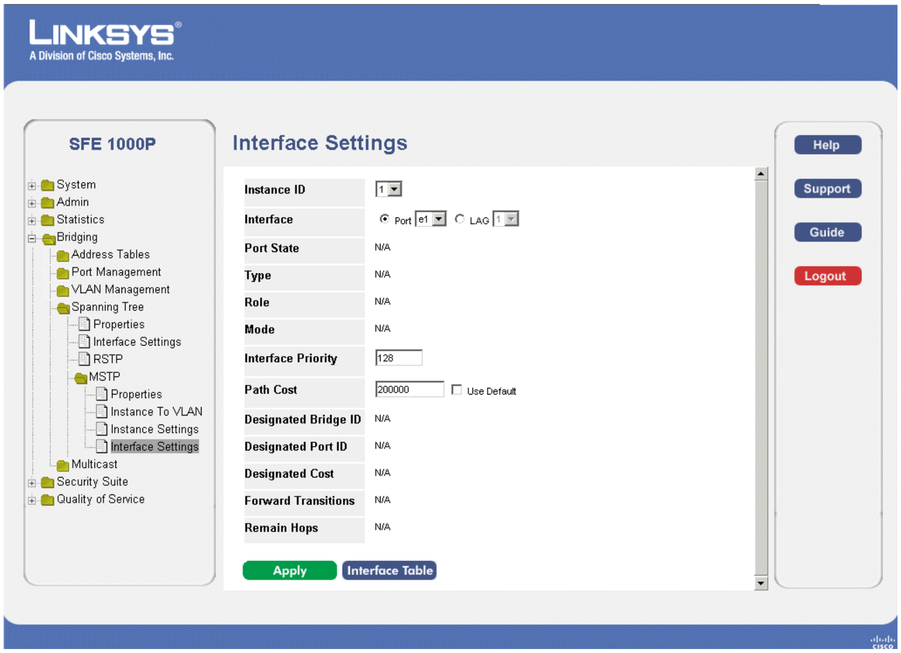
The *MSTP Instance Settings Page* contains the following fields:

- **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 ID 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 bridge ID of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

## Defining MSTP Interface Settings

Network Administrators can define MSTP Instances settings using the *MSTP Interface Settings Page*.

***MSTP Interface Settings Page***



Interface Settings

| | |
|---|---|
| Instance ID | 1 |
| Interface | ● Port e1 ○ LAG 1 |
| Port State | N/A |
| Type | N/A |
| Role | N/A |
| Mode | N/A |
| Interface Priority | 128 |
| Path Cost | 200000 □ Use Default |
| Designated Bridge ID | N/A |
| Designated Port ID | N/A |
| Designated Cost | N/A |
| Forward Transitions | N/A |
| Remain Hops | N/A |

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. 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.

- **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.
- **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 should always be 1-200,000,000.
- **Designated Bridge ID** — Indicates that the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates that 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.

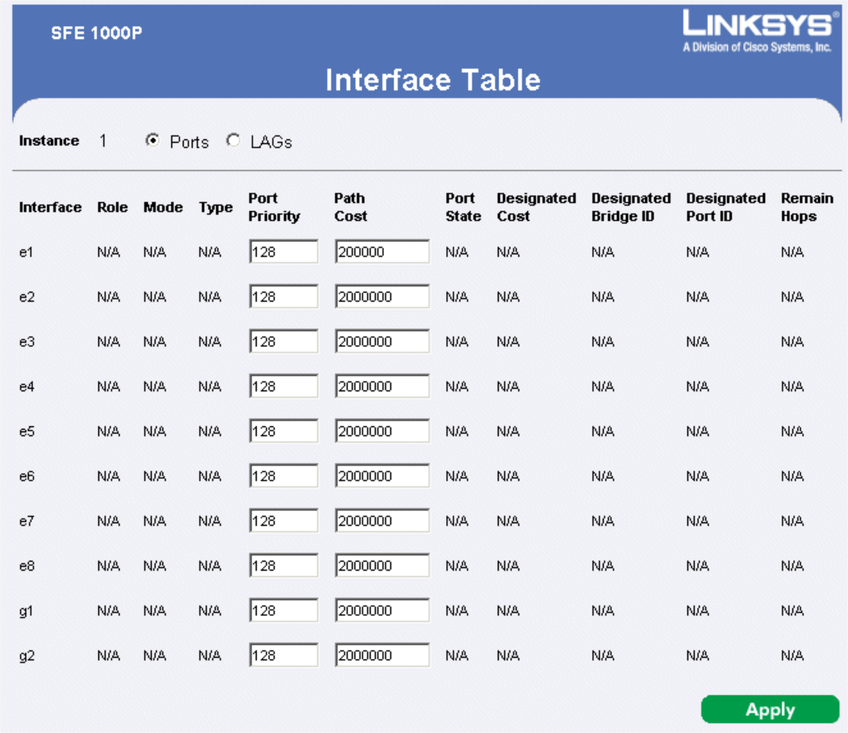
- **Forward Transitions** — Indicates the number of times the port has changed from Forwarding state to Blocking state.

- **Remain Hops** — Indicates the hops remaining to the next destination.

- **Interface State** — Indicates whether the port is enabled or disabled in the specific instance.

## Interface Table

***Interface Table Page***



Interface Table

Instance 1 ● Ports ○ LAGs

| Interface | Role | Mode | Type | Port Priority | Path Cost | Port State | Designated Cost | Designated Bridge ID | Designated Port ID | Remain Hops |
|---|---|---|---|---|---|---|---|---|---|---|
| e1 | N/A | N/A | N/A | 128 | 200000 | N/A | N/A | N/A | N/A | N/A |
| e2 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e3 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e4 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e5 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e6 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e7 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| e8 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| g1 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |
| g2 | N/A | N/A | N/A | 128 | 2000000 | N/A | N/A | N/A | N/A | N/A |

The *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 that the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates that 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.
  - *Static* — Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
  - *Forbidden* — Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
  - *None* — The port is not part of a Multicast group.

# 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 Bock-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 copy traps.

The SNMP section contains the following sections:

- Configuring SNMP Security
- Defining Trap Management

# Configuring SNMP Security

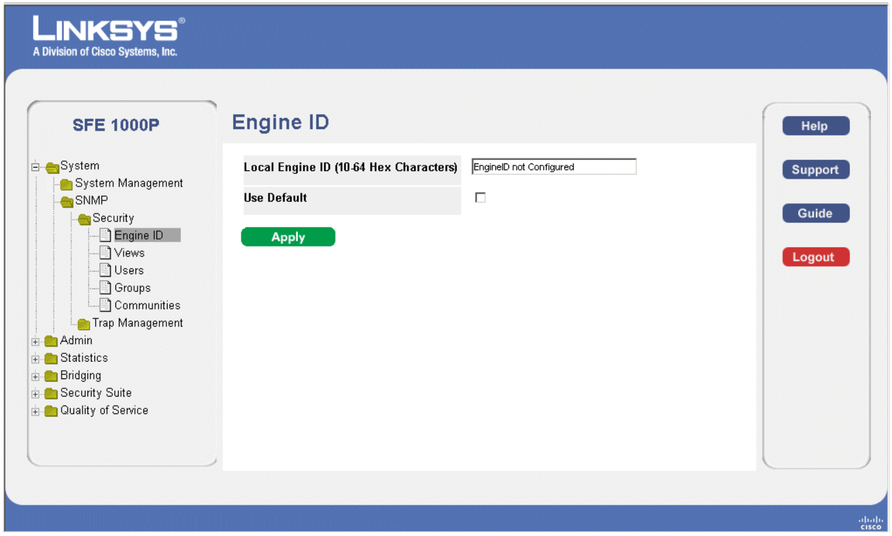
The Security section contains the following pages:

- Defining the SNMP Engine ID
- Defining SNMP Views
- Defining SNMP Users
- Define SNMP Groups
- Defining SNMP Communities

## Defining the SNMP Engine ID

The *Engine ID Page* provides information for defining the device engine ID.

***Engine ID Page***



Engine ID

| | |
|---|---|
| Local Engine ID (10-64 Hex Characters) | EngineID not Configured |
| Use Default | □ |

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. 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.
- **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:

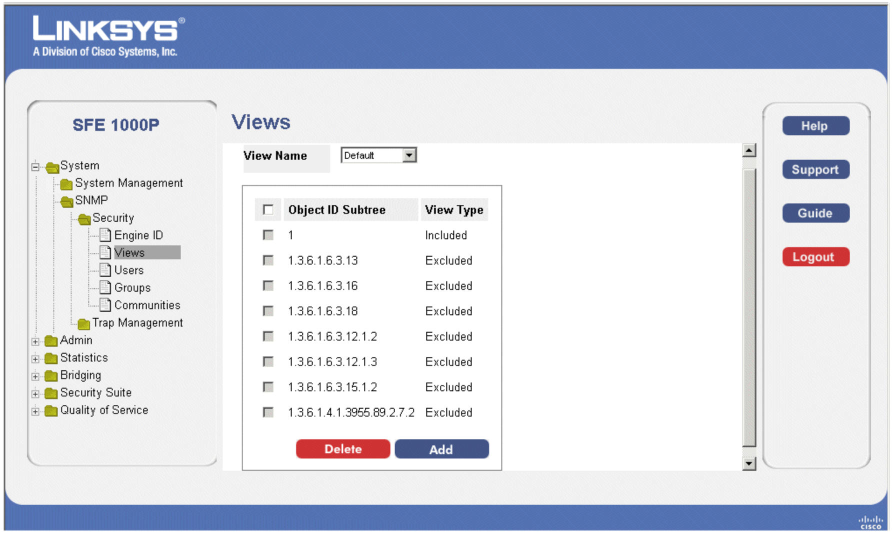
– *Checked* — Use the default Engine ID.

– *Unchecked* — Use a user-defined Engine ID.

## Defining SNMP Views

SNMP Views provide access or block access to device features or feature aspects. For example, a view can be defined that states that 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.

***SNMP Views Page***



Views

View Name: Default

| ☐ | Object ID Subtree | View Type |
|---|---|---|
| ☐ | 1 | Included |
| ☐ | 1.3.6.1.6.3.13 | Excluded |
| ☐ | 1.3.6.1.6.3.16 | Excluded |
| ☐ | 1.3.6.1.6.3.18 | Excluded |
| ☐ | 1.3.6.1.6.3.12.1.2 | Excluded |
| ☐ | 1.3.6.1.6.3.12.1.3 | Excluded |
| ☐ | 1.3.6.1.6.3.15.1.2 | Excluded |
| ☐ | 1.3.6.1.4.1.3955.89.2.7.2 | Excluded |

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.

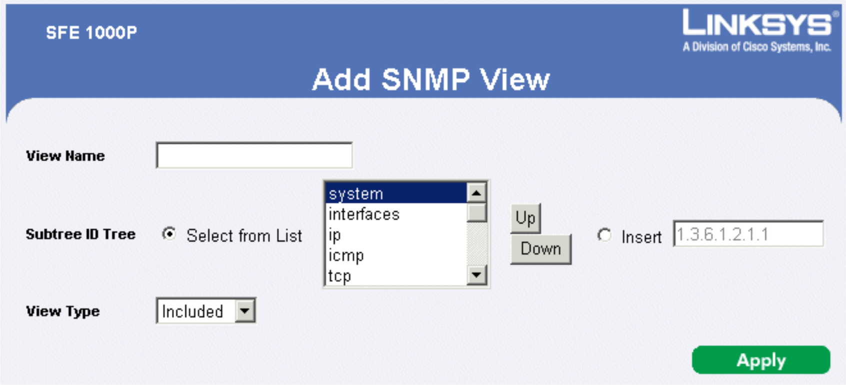
- **Object ID Subtree** — Indicates the device feature OID included or excluded in the selected SNMP view.

- **View Type** — Indicates if the defined OID branch will be included or excluded in the selected SNMP view.

## Add SNMP View

The *Add SNMP View Page* contains parameters for defining and configuring new SNMP views.

***Add SNMP View Page***



SFE 1000P

Add SNMP View

View Name

Subtree ID Tree ● Select from List ○ Insert 1.3.6.1.2.1.1

View Type Included

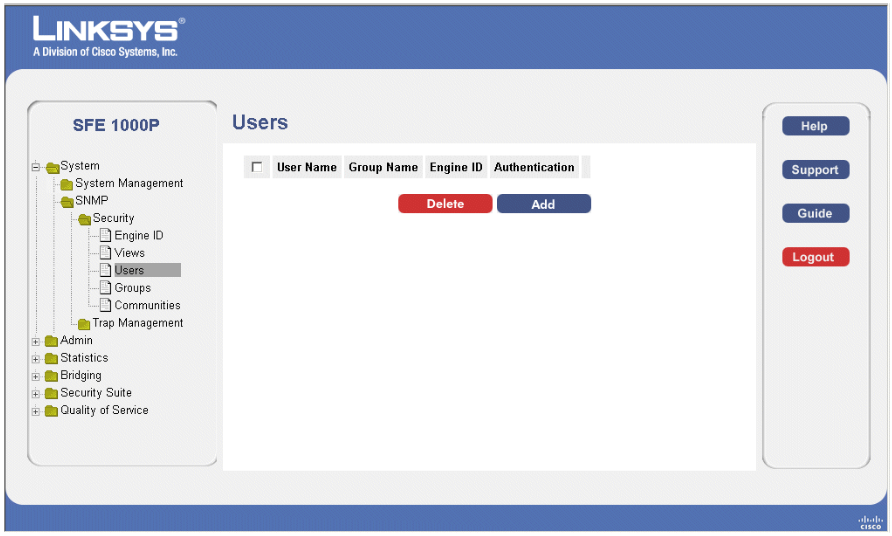
The *Add SNMP View Page* contains the following fields:

- **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.
- **Subtree ID Tree** — Indicates the device feature OID included or excluded in the selected SNMP view. The options to select the Subtree 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 in the *Select from List* field 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.

# Defining SNMP Users

The *SNMP Users 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 feature aspects.

***SNMP Users Page***



Users

| □ | User Name | Group Name | Engine ID | Authentication |
|---|---|---|---|---|

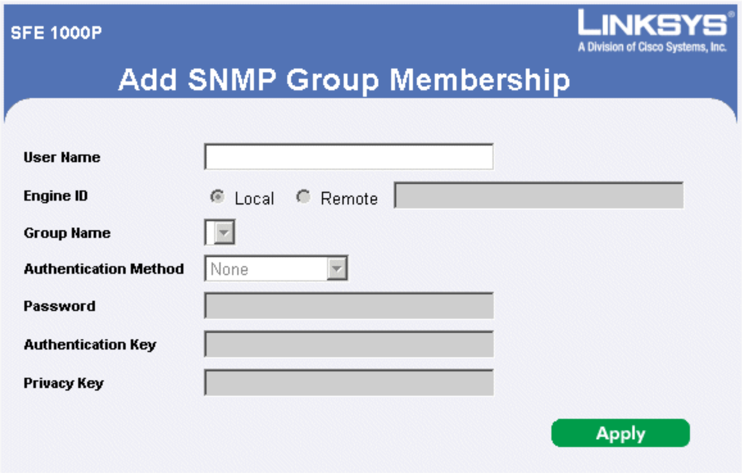
The *SNMP Users Page* contains the following fields.

- **User Name** — Displays the user-defined group 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 device engine ID.
- **Authentication** — Indicates the Authentication method used.

## Add SNMP Group Membership

The *Add SNMP Group Membership Page* provides information for assigning SNMP access control privileges to SNMP groups.

***Add SNMP Group Membership Page***



Add SNMP Group Membership

| | |
|---|---|
| User Name | |
| Engine ID | ● Local ○ Remote |
| Group Name | |
| Authentication Method | None |
| Password | |
| Authentication Key | |
| Privacy Key | |

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** — 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 the HMAC-MD5 algorithm.
  - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
  - *None* — No user authentication is used.

- **Password** — Define 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.

## Modifying SNMP Users

The *Edit SNMP User Page* provides information for assigning SNMP access control privileges to SNMP groups. 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 the HMAC-MD5 algorithm.

  - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.

  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.

  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.

  - *None* — No user authentication is used.

- **Password** — Define the local user password. Local user passwords can contain up to 159 characters. This field is available if the Authentication Method is a password.

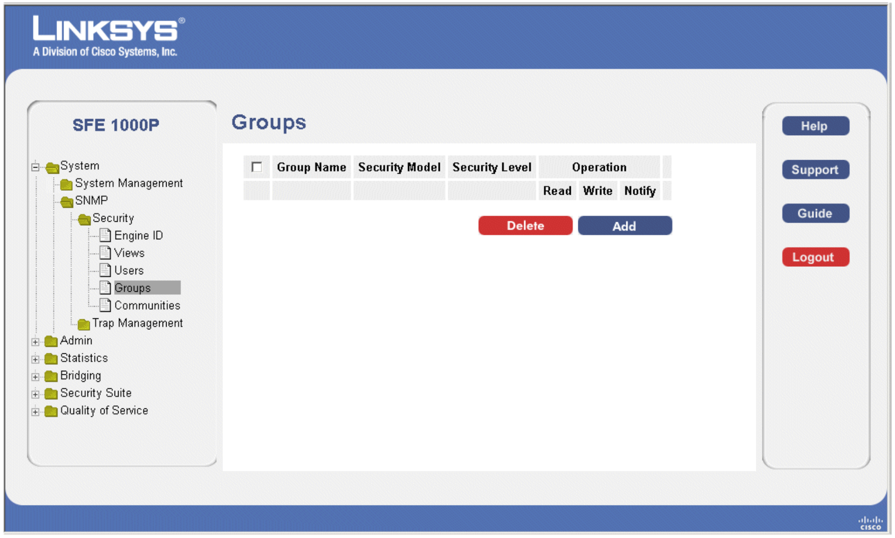
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each 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.

## Define SNMP Groups

The *SNMP Groups Profile 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.

***SNMP Groups Profile Page***



| □ | Group Name | Security Model | Security Level | Operation | | |
|---|---|---|---|---|---|---|
| | | | | Read | Write | Notify |

The *SNMP Groups Profile Page* contains the following fields:

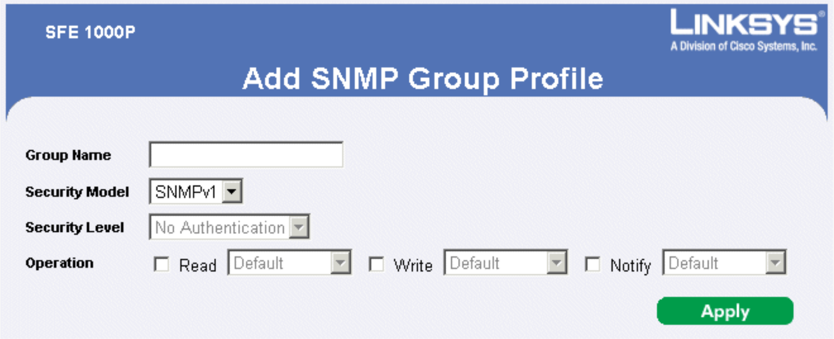
- **Group Name** — Displays the user-defined group to which access control rules are applied.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 is defined for the group.
  - *SNMPv3* — 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 rights. 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.

## Adding SNMP Group Profiles

The *Add SNMP Group Profile Page* allows network managers to define new SNMP Group profiles.

***Add SNMP Group Profile Page***



Group Name
Security Model: SNMPv1
Security Level: No Authentication
Operation: □ Read Default □ Write Default □ Notify Default

The *Add SNMP Group Profile Page* contains the following fields:

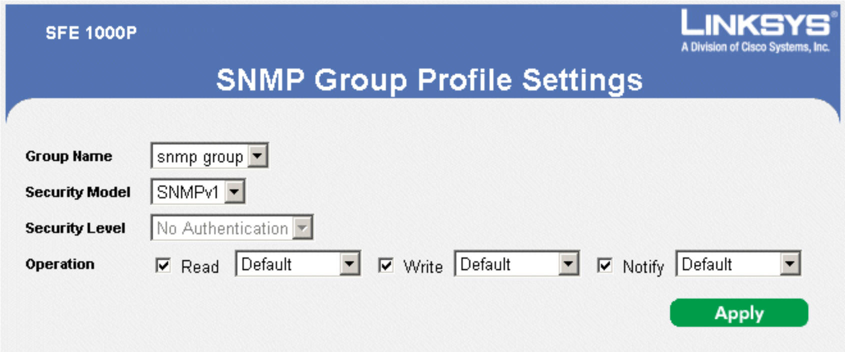
- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 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.

## Modifying SNMP Group Profile Settings

The *Edit SNMP Group Profile Settings Page* allows network managers to edit SNMP Group profiles.

***Edit SNMP Group Profile Page***



SNMP Group Profile Settings

|  |  |
|---|---|
| Group Name | snmp group |
| Security Model | SNMPv1 |
| Security Level | No Authentication |
| Operation | ☑ Read Default ☑ Write Default ☑ Notify Default |

The *Edit SNMP Group Profile Page* contains the following fields:

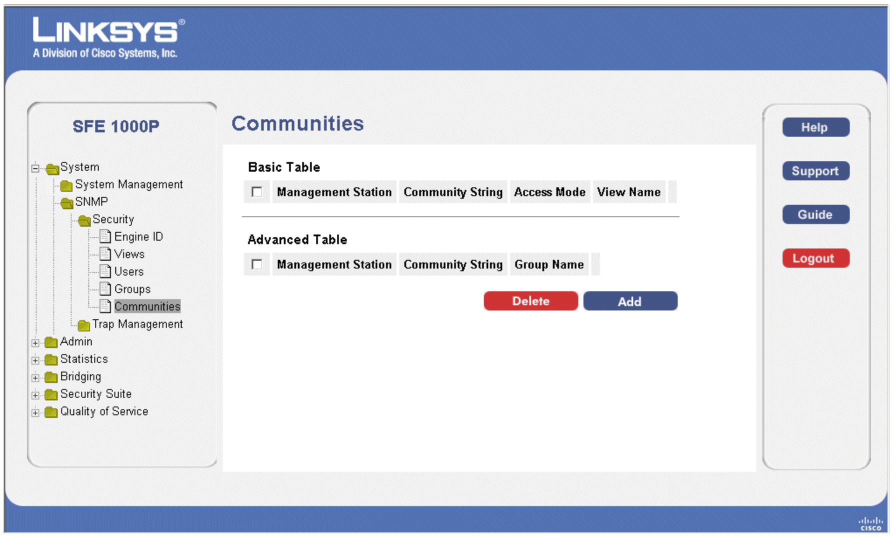
- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 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.

## 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.

***SNMP Communities Page***



Communities

Basic Table

| □ | Management Station | Community String | Access Mode | View Name |
|---|---|---|---|---|

Advanced Table

| □ | Management Station | Community String | Group Name |
|---|---|---|---|

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 user-defined SNMP view.

The SNMP Communities Advanced Table area contains the following fields:

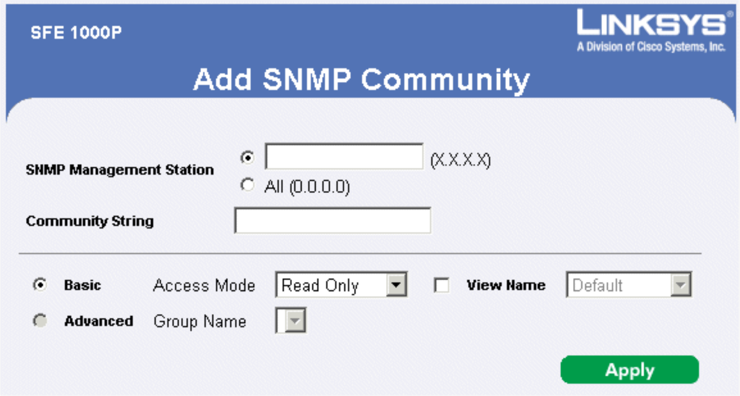
- **Management Station** — Displays the management station IP address for which the Advanced SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.

- **Group Name** — Displays advanced SNMP communities group name.

## Adding SNMP Communities

The *Add SNMP Community Page* allows network managers to define and configure new SNMP communities.

***Add SNMP Community Page***



SNMP Management Station ● ▭ (X.X.X.X) ○ All (0.0.0.0)

Community String ▭

● Basic Access Mode Read Only □ View Name Default

○ Advanced Group Name

The *Add SNMP Community Page* contains the following fields:

- **SNMP Management Station** — Defines the management station IP address for which the SNMP community is defined. There are two definition options:
  - Define the management station IP address.
  - **All**, which includes all management station IP addresses.
- **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.

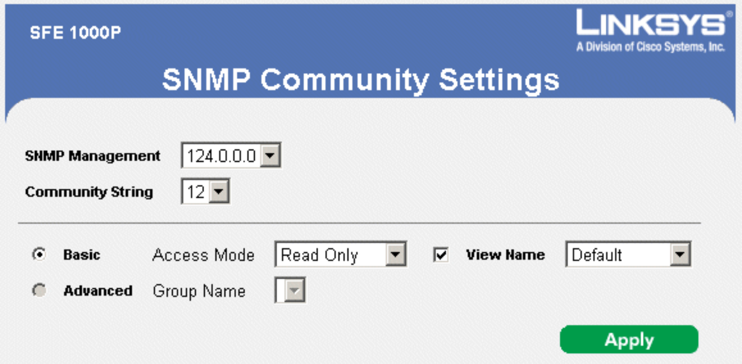
**Advanced** — Enables SNMP Advanced mode for a selected community and contains the following field:

- **Group Name** — Defines advanced SNMP communities group names.

## Modifying SNMP Community Settings

The *Edit SNMP Community Page* allows network managers to edit SNMP communities.

***Edit SNMP Community Page***



SNMP Management: 124.0.0.0

Community String: 12

● Basic — Access Mode: Read Only — ☑ View Name: Default

○ Advanced — Group Name:

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.

# Defining Trap Management

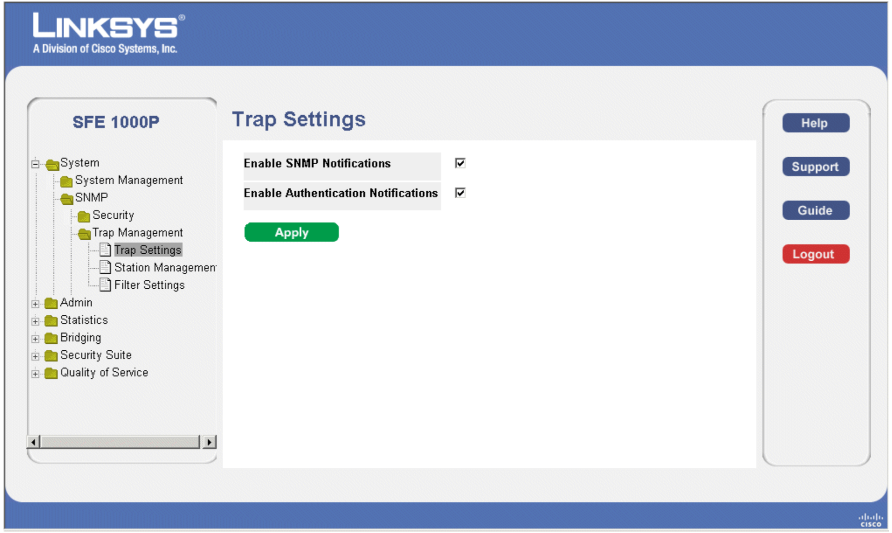
The Defining Trap Management section contains the following pages:

- Defining Trap Settings
- Configuring Station Management
- Defining SNMP Filter Settings

## Defining Trap Settings

The *Trap Settings Page* contains parameters for defining SNMP notification parameters.

***Trap Settings Page***



Trap Settings

Enable SNMP Notifications ☑

Enable Authentication Notifications ☑

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.

## Configuring Station Management

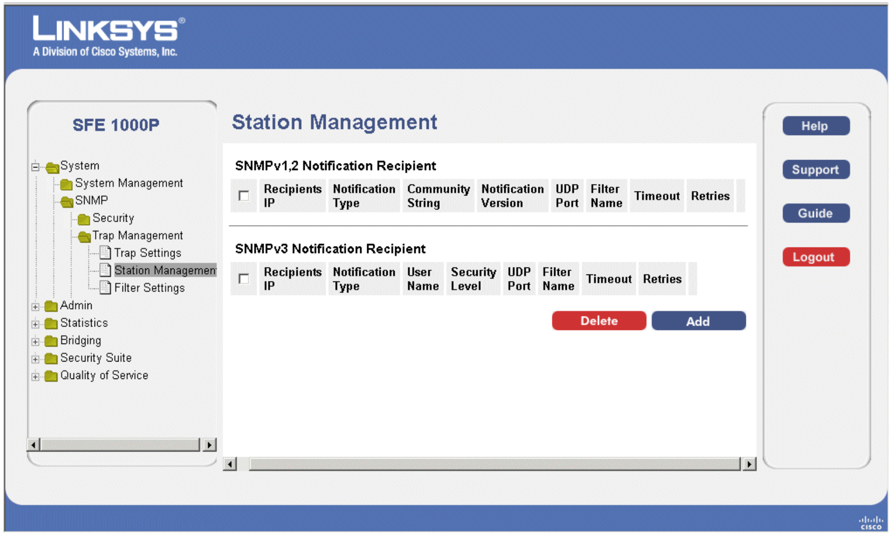
The *Station Management Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- 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 five management stations that receive authentication failure messages and other trap messages from the switch.

The *Station Management Page* contains two areas, the *SNMPv1,2 Notification Recipient* and the *SNMPv3 Notification Recipient* table.

***Station Management Page***



Station Management

SNMPv1,2 Notification Recipient

| □ | Recipients IP | Notification Type | Community String | Notification Version | UDP Port | Filter Name | Timeout | Retries |
|---|---|---|---|---|---|---|---|---|

SNMPv3 Notification Recipient

| □ | Recipients IP | Notification Type | User Name | Security Level | UDP Port | Filter Name | Timeout | Retries |
|---|---|---|---|---|---|---|---|---|

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.

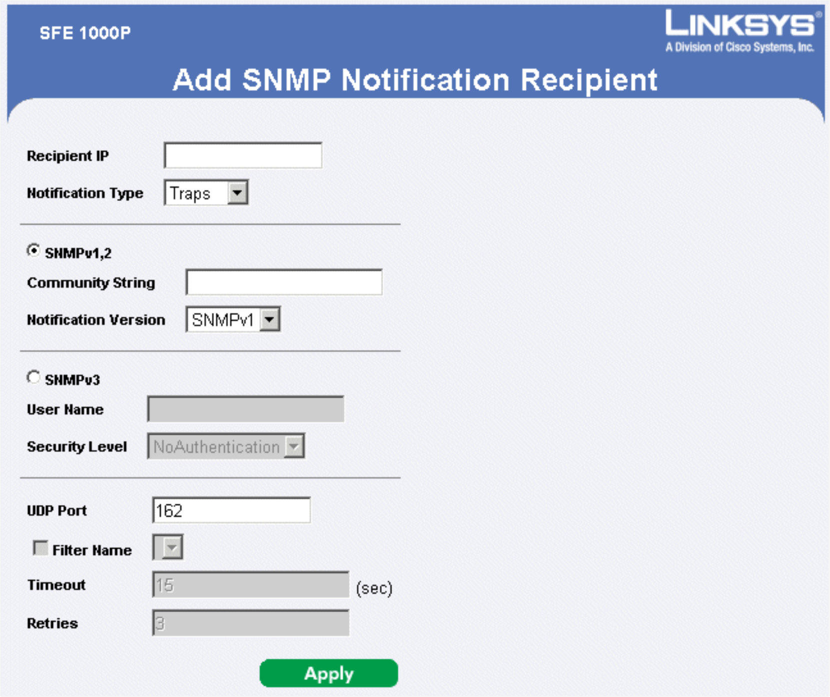
The *SNMPv3 Notification Recipient* table area contains the following fields:

- **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 Communities.
- **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** — 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.

## Adding a SNMP Notification Recipient

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.

***Add SNMP Notification Recipient Page***



Add SNMP Notification Recipient

Recipient IP

Notification Type: Traps

● SNMPv1,2

Community String

Notification Version: SNMPv1

○ SNMPv3

User Name

Security Level: NoAuthentication

UDP Port: 162

□ Filter Name

Timeout: 15 (sec)

Retries: 3

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:

- **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:
  - *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 SNMPv3is 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.

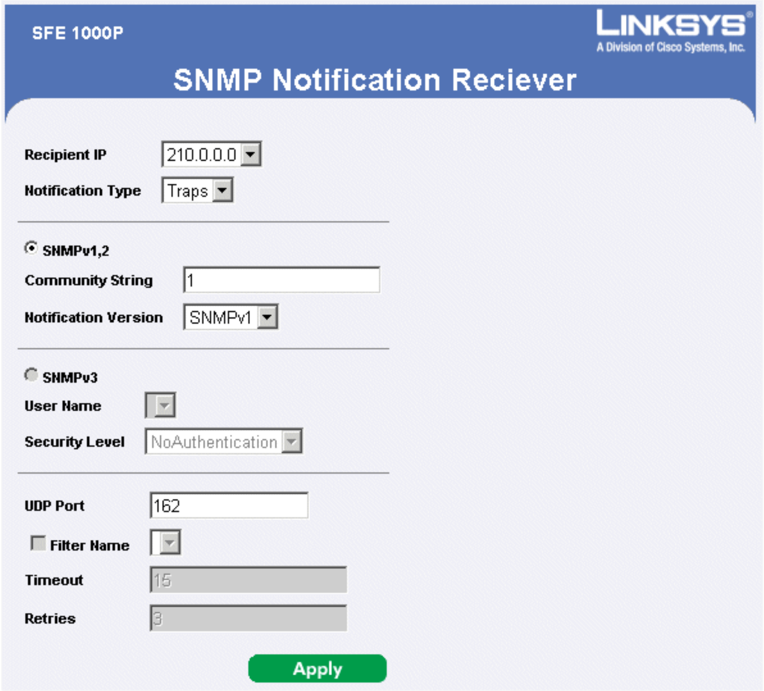
The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — 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.

## Modifying SNMP Notifications Settings

The *Edit SNMP Notification Page* allows system administrators to define notification settings. The *Edit SNMP Notification Page* is divided into four areas, Notification Recipient, SNMPv1,2 Notification Recipient, SNMPv3 Notification Recipient and UDP Port Notification Recipient.

***Edit SNMP Notification Page***



SNMP Notification Reciever

Recipient IP: 210.0.0.0
Notification Type: Traps

● SNMPv1,2
Community String: 1
Notification Version: SNMPv1

○ SNMPv3
User Name:
Security Level: NoAuthentication

UDP Port: 162
□ Filter Name:
Timeout: 15
Retries: 3

The *Edit SNMP Notification 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** — 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.

The SNMPv3 Notification Recipient area contains the following fields:

- **SNMPv3** — Enables SNMPv3 as the Notification version. If SNMPv3is 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.

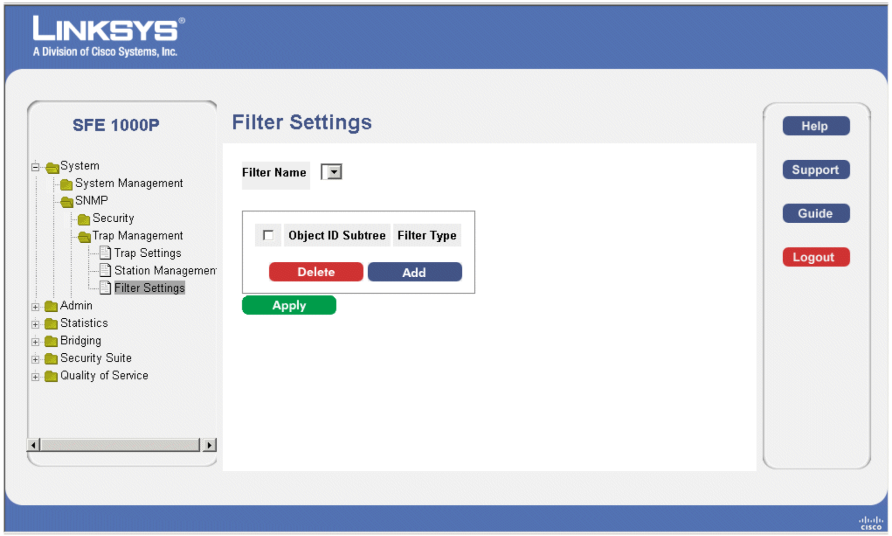
The UDP Port Notification Recipient area contains the following fields:

- **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.
- **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.

## 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.

***Filter Settings Page***



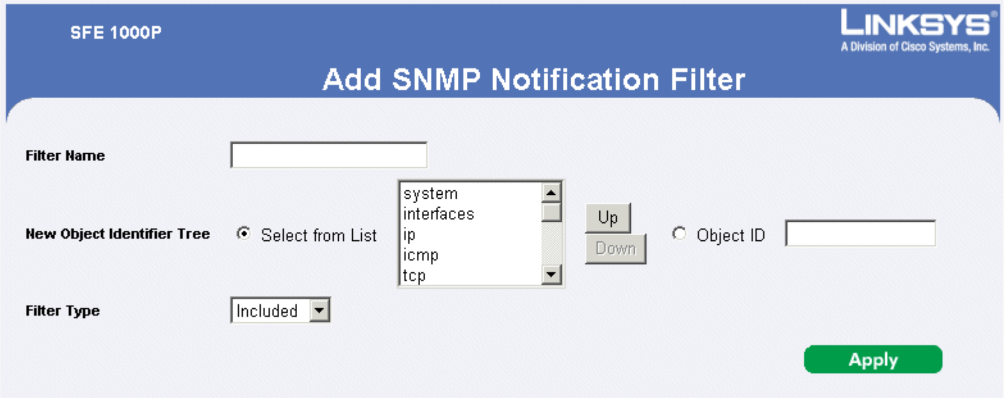
The *Filter Settings Page* contains the following fields:

- **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.

## Add SNMP Notification Filter

The Add SNMP Notification Filter Settings Page allows network managers to add filter notifications.

***Add SNMP Notification Filter Page***


SFE 1000P
LINKSYS®
A Division of Cisco Systems, Inc.
Add SNMP Notification Filter

Filter Name

New Object Identifier Tree ● Select from List

system
interfaces
ip
icmp
tcp

○ Object ID

Filter Type Included

The *Add SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **New Object Identifier 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. 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 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.

# 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 section:

- Defining General Settings
- Defining Advanced Mode
- Defining QoS Basic Mode

The section also contains the following pages:

- Configuring Policy Table
- Configuring Policy Table

# Defining General Settings

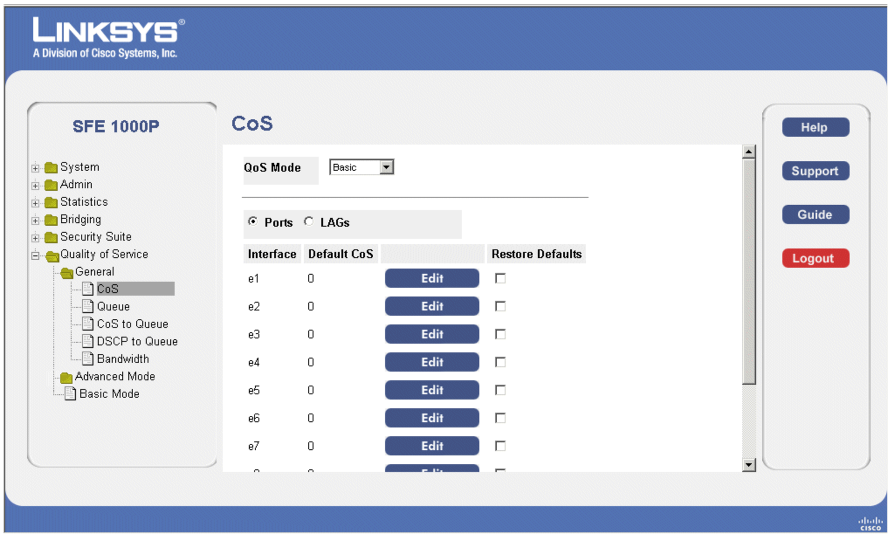
The QoS General Settings section contains the following pages:

- Defining CoS
- Defining 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.

***CoS Page***



CoS

QoS Mode: Basic

● Ports ○ LAGs

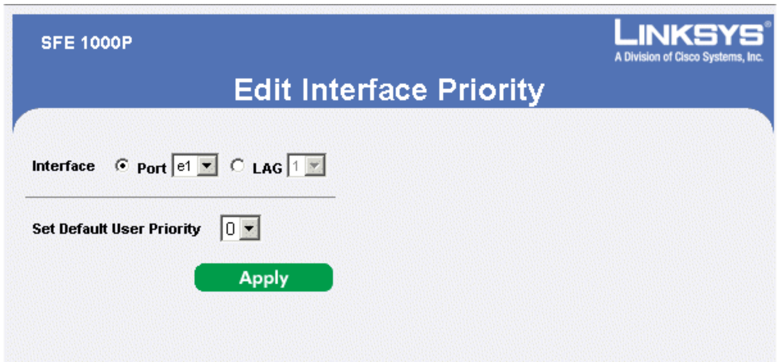
| Interface | Default CoS | | Restore Defaults |
|---|---|---|---|
| e1 | 0 | Edit | □ |
| e2 | 0 | Edit | □ |
| e3 | 0 | Edit | □ |
| e4 | 0 | Edit | □ |
| e5 | 0 | Edit | □ |
| e6 | 0 | Edit | □ |
| e7 | 0 | Edit | □ |

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.
  - *Basic* — Enables QoS on the device.
  - *Disable* — Disables QoS on the device.
- **Ports/LAGs** — Select whether to display the ports' or the LAGs' CoS configuration.
- **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

***Edit Interface Priority Page***



SFE 1000P

Edit Interface Priority

Interface ● Port e1 ○ LAG 1

Set Default User Priority 0

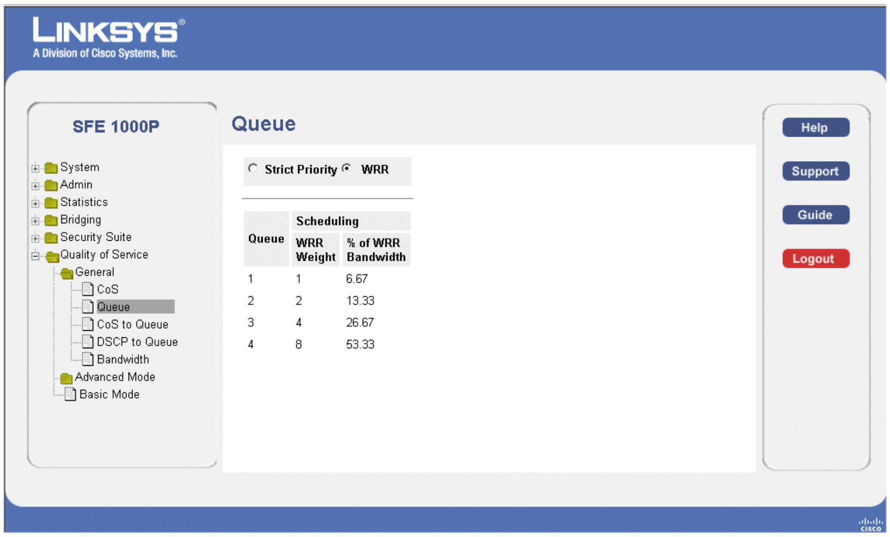
The *Edit Interface Priority Page* contains the following fields:

- **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.

## Defining Queue

The *Queue Page* contains fields for defining the QoS queue forwarding types.

***Queue Page***



Queue

○ Strict Priority ● WRR

| Queue | Scheduling | |
|---|---|---|
| | WRR Weight | % of WRR Bandwidth |
| 1 | 1 | 6.67 |
| 2 | 2 | 13.33 |
| 3 | 4 | 26.67 |
| 4 | 8 | 53.33 |

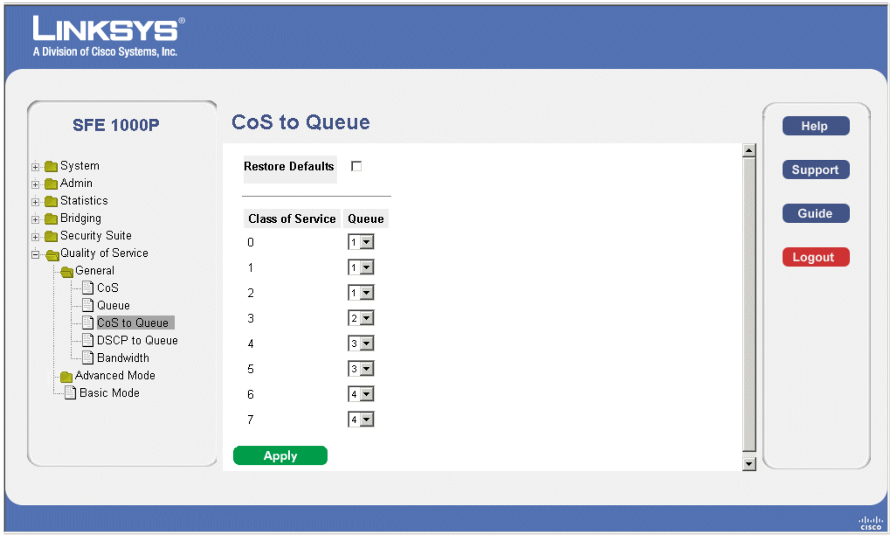
The *Queue Page* contains the following fields:

- Select whether traffic scheduling is based on either Strict Priority or WRR.
  - *Strict Priority* — Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
  - *WRR* — Indicates that traffic scheduling for the selected queue is based strictly on the WRR. If WRR is selected, the predetermined weights 8, 2, 4, and 1 are assigned to queues 4,3,2 and 1.
- **Queue** — Displays the queue for which the queue settings are displayed. The possible field range is 1 - 4.
- **WRR Weight** — WRR weight assigned to the queue.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the queue. These values are fixed and are not user defined.

## Mapping CoS to Queue

The *Cos to Queue Page* contains fields for classifying CoS settings to traffic queues.

***Cos to Queue Page***



CoS to Queue

Restore Defaults □

| Class of Service | Queue |
|---|---|
| 0 | 1 |
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 3 |
| 5 | 3 |
| 6 | 4 |
| 7 | 4 |

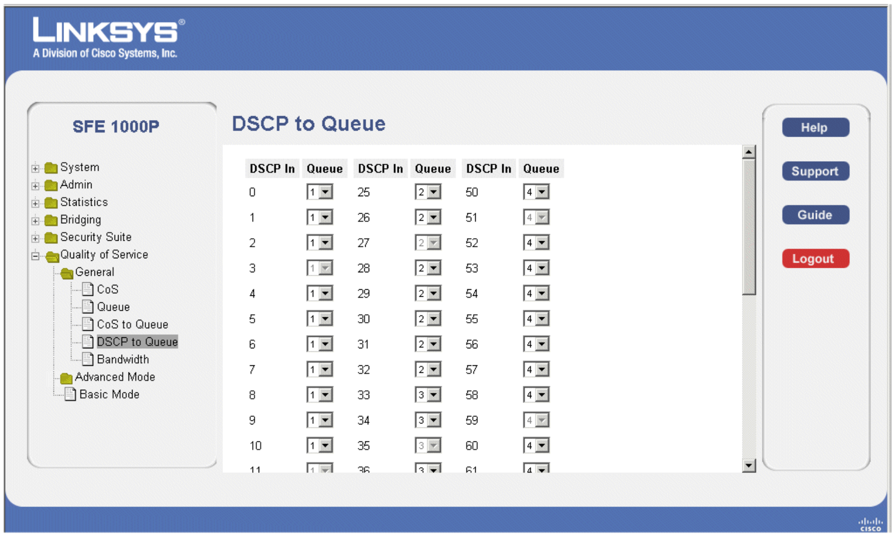
The *Cos to Queue Page* contains the following fields:

- **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.

## Mapping DSCP to Queue

The *DSCP to Queue Page* enables mapping DSCP values to specific queues.

***DSCP to Queue Page***



DSCP to Queue

| 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 | 2 | 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 |

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.

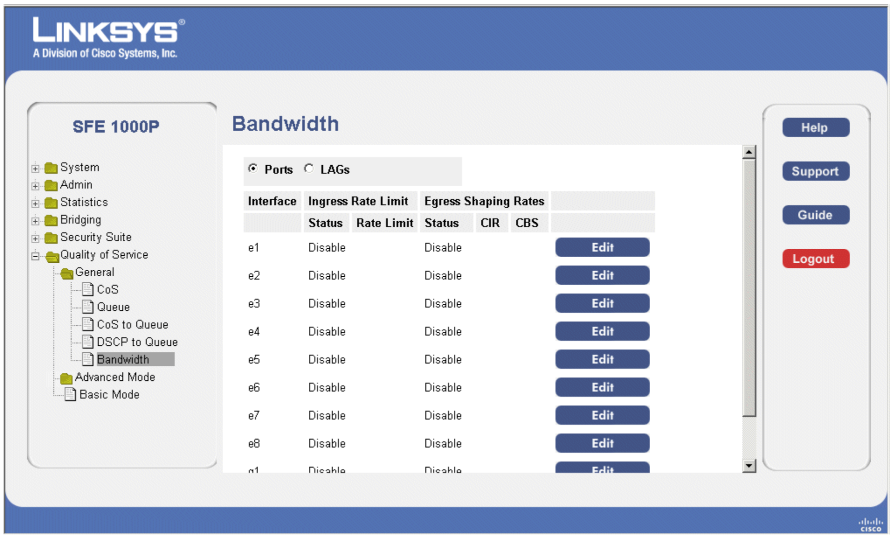
## Configuring Bandwidth

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.

***Bandwidth Page***



Bandwidth

● Ports ○ LAGs

| Interface | Ingress Rate Limit | | Egress Shaping Rates | | | |
|---|---|---|---|---|---|---|
| | Status | Rate Limit | Status | CIR | CBS | |
| e1 | Disable | | Disable | | | Edit |
| e2 | Disable | | Disable | | | Edit |
| e3 | Disable | | Disable | | | Edit |
| e4 | Disable | | Disable | | | Edit |
| e5 | Disable | | Disable | | | Edit |
| e6 | Disable | | Disable | | | Edit |
| e7 | Disable | | Disable | | | Edit |
| e8 | Disable | | Disable | | | Edit |
| g1 | Disable | | Disable | | | Edit |

The *Bandwidth Page* contains the following fields:

- **Ports/LAG** — Specifies whether the bandwidth settings are displayed for ports or for LAGs.
- **Interface** — Indicates the interface for which this bandwidth information is displayed.
- **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:

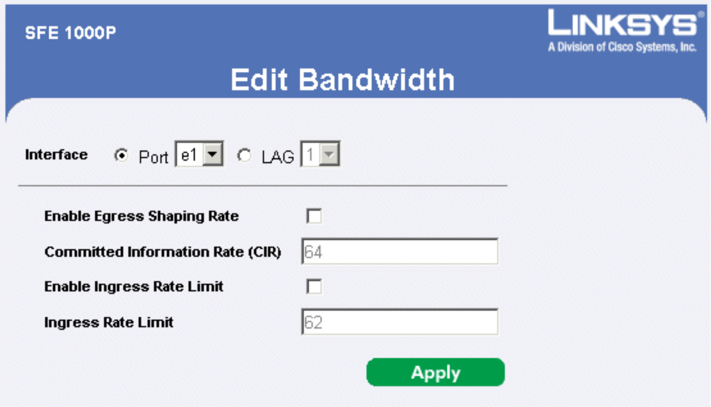
  For FE ports, the rate is 64 - 100,000 Kbps.
  For GE ports, the rate is 64 - 1,000,000 Kbps.

– *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

The *Edit Bandwidth Page* allows network managers to edit the bandwidth settings for specified egress and ingress interfaces.

***Edit Bandwidth Page***



Edit Bandwidth

Interface ● Port e1 ○ LAG 1

| | |
|---|---|
| Enable Egress Shaping Rate | □ |
| Committed Information Rate (CIR) | 64 |
| Enable Ingress Rate Limit | □ |
| Ingress Rate Limit | 62 |

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 Status** — 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 - 100,000 Kbps.
  - For GE ports, the rate is 64 - 1,000,000 Kbps.
- **Committed Burst Size (CbS)** — Defines CbS as the queue shaping type. CbS is supported only on GE interfaces. The possible field value is 4096 - 16,769,020 bytes.

- **Ingress Rate Limit Status** — 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.

## Defining Advanced 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.

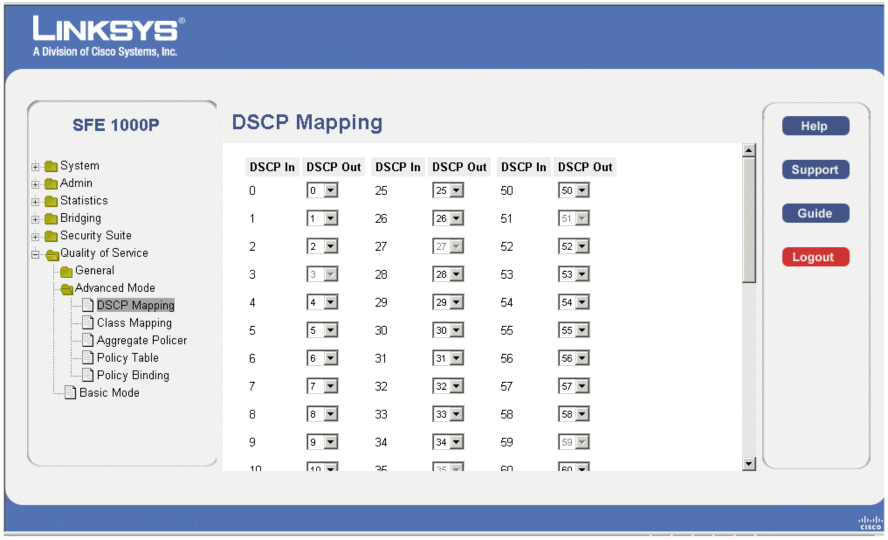
The *Advanced Mode* section contains the following pages:

- 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. This information is important when traffic exceeds user-defined limits.

***DSCP Mapping Page***



DSCP Mapping

| DSCP In | DSCP Out | DSCP In | DSCP Out | DSCP In | DSCP Out |
|---|---|---|---|---|---|
| 0 | 0 | 25 | 25 | 50 | 50 |
| 1 | 1 | 26 | 26 | 51 | 51 |
| 2 | 2 | 27 | 27 | 52 | 52 |
| 3 | 3 | 28 | 28 | 53 | 53 |
| 4 | 4 | 29 | 29 | 54 | 54 |
| 5 | 5 | 30 | 30 | 55 | 55 |
| 6 | 6 | 31 | 31 | 56 | 56 |
| 7 | 7 | 32 | 32 | 57 | 57 |
| 8 | 8 | 33 | 33 | 58 | 58 |
| 9 | 9 | 34 | 34 | 59 | 59 |
| 10 | 10 | 35 | 35 | 60 | 60 |

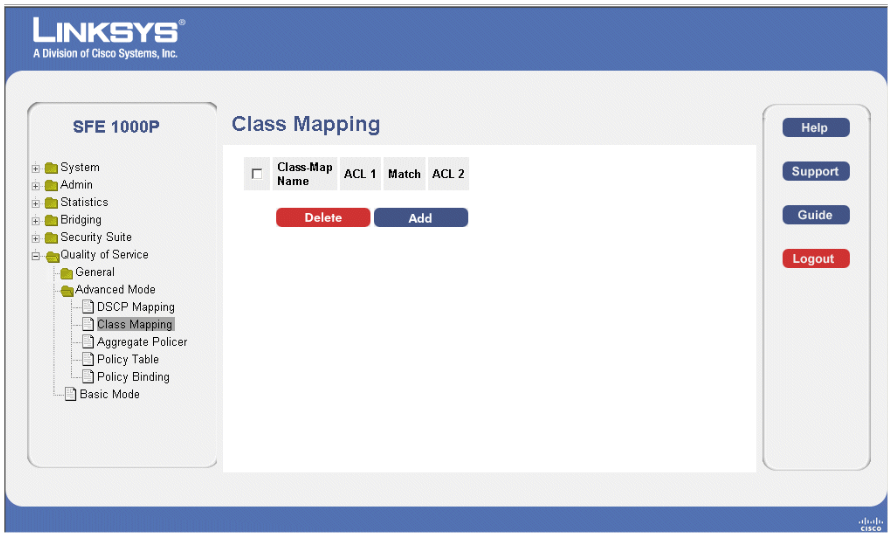
The *DSCP Mapping Page* contains the following fields:

- **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.

## 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.

***Class Mapping Page***

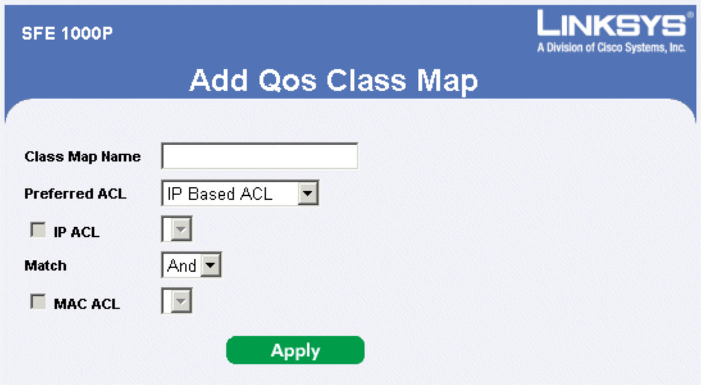


The *Class Mapping Page* contains the following fields:

- **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.

## Adding QoS Class Maps

*Add QoS Class Map Page*



SFE 1000P

Add Qos Class Map

Class Map Name

Preferred ACL: IP Based ACL

□ IP ACL

Match: And

□ MAC ACL

The *Add QoS Class Map Page* contains the following fields.

- **Class Map Name** — Defines a new Class Map name.
- **Preferred ACL** — Indicates 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.
- **IP ACL** — Matches packets to IP based ACLs first, then matches packets to MAC based 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.
- **MAC ACL** — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.

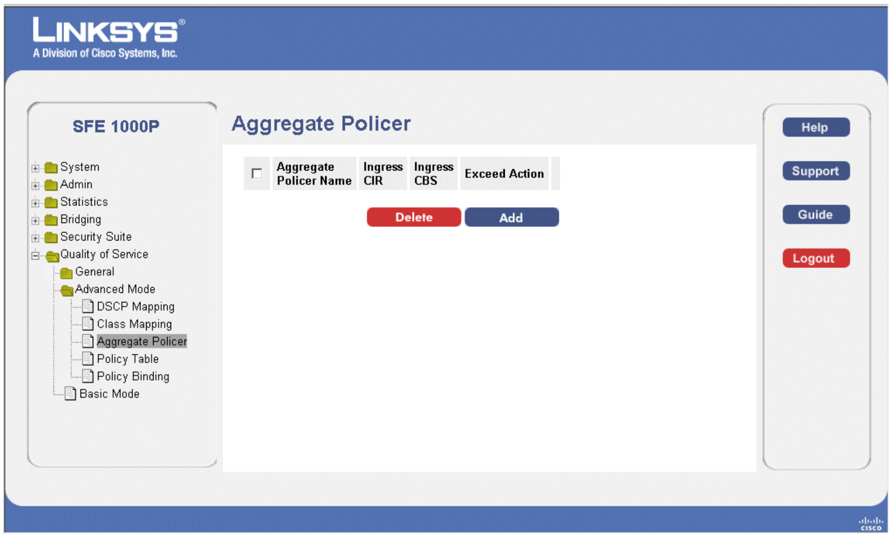
## Defining Aggregate Policer

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.

***Aggregate Policer Page***



Aggregate Policer

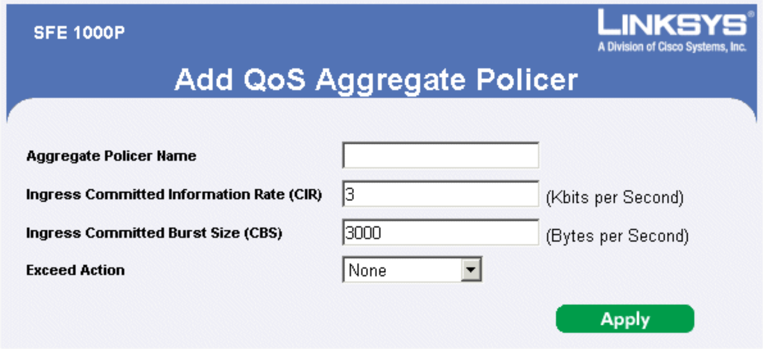
| □ | Aggregate Policer Name | Ingress CIR | Ingress CBS | Exceed Action |
|---|---|---|---|---|

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 CbS** — Defines the Committed Burst Size (CbS) 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.

## Adding QoS Aggregate Policer

***Add QoS Aggregate Policer Page***



Add QoS Aggregate Policer

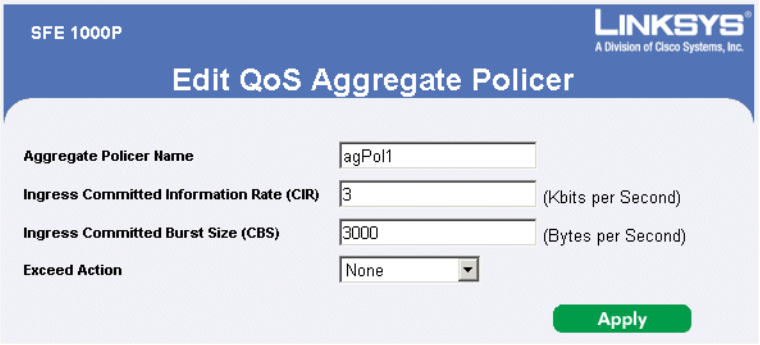
|  |  |  |
|---|---|---|
| Aggregate Policer Name |  |  |
| Ingress Committed Information Rate (CIR) | 3 | (Kbits per Second) |
| Ingress Committed Burst Size (CBS) | 3000 | (Bytes per Second) |
| Exceed Action | None |  |

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 (CBS)** — Defines the CBS 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.

## Modifying QoS Aggregate Policer

*Edit QoS Aggregate Policer Page*



SFE 1000P

Edit QoS Aggregate Policer

| | | |
|---|---|---|
| Aggregate Policer Name | agPol1 | |
| Ingress Committed Information Rate (CIR) | 3 | (Kbits per Second) |
| Ingress Committed Burst Size (CBS) | 3000 | (Bytes per Second) |
| Exceed Action | None | |

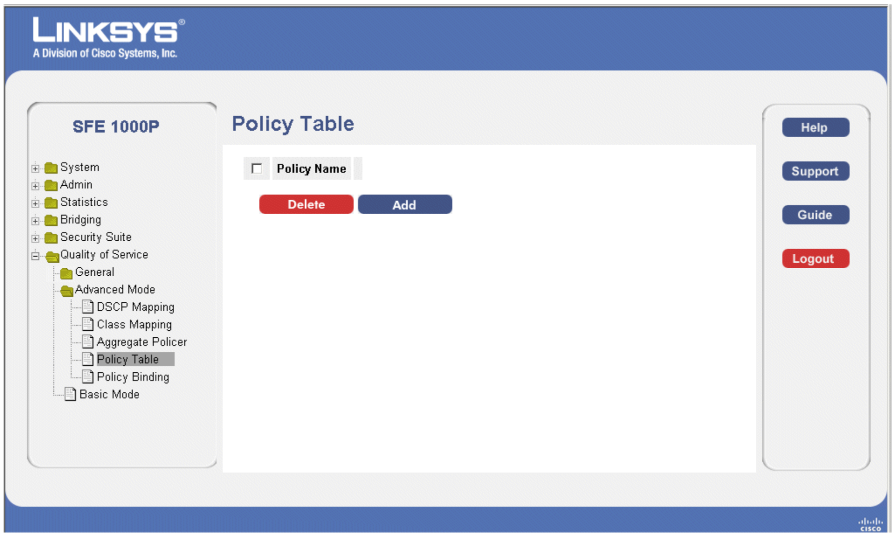
The *Edit QoS Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name**— Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in bits per second.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS 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.

## Configuring Policy Table

In the *Policy Table Page,* QoS policies are set up and assigned to interfaces.

***Policy Table Page***



Policy Table

☐ Policy Name

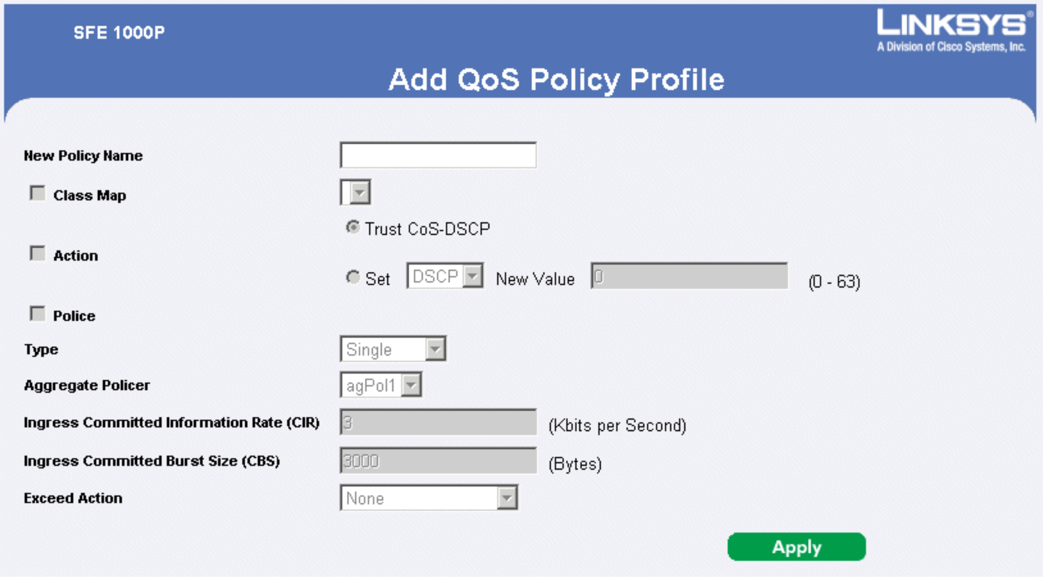
Delete Add

The *Policy Table Page* contains the following fields:

- **Policy Name**— Displays the user-defined policy name.

## Adding QoS Policy Profile

***Add QoS Policy Profile Page***



Add QoS Policy Profile

| | |
|---|---|
| New Policy Name | |
| ☐ Class Map | |
| ☐ Action | ● Trust CoS-DSCP<br>○ Set DSCP New Value 0 (0 - 63) |
| ☐ Police | |
| Type | Single |
| Aggregate Policer | agPol1 |
| Ingress Committed Information Rate (CIR) | 3 (Kbits per Second) |
| Ingress Committed Burst Size (CBS) | 3000 (Bytes) |
| Exceed Action | None |

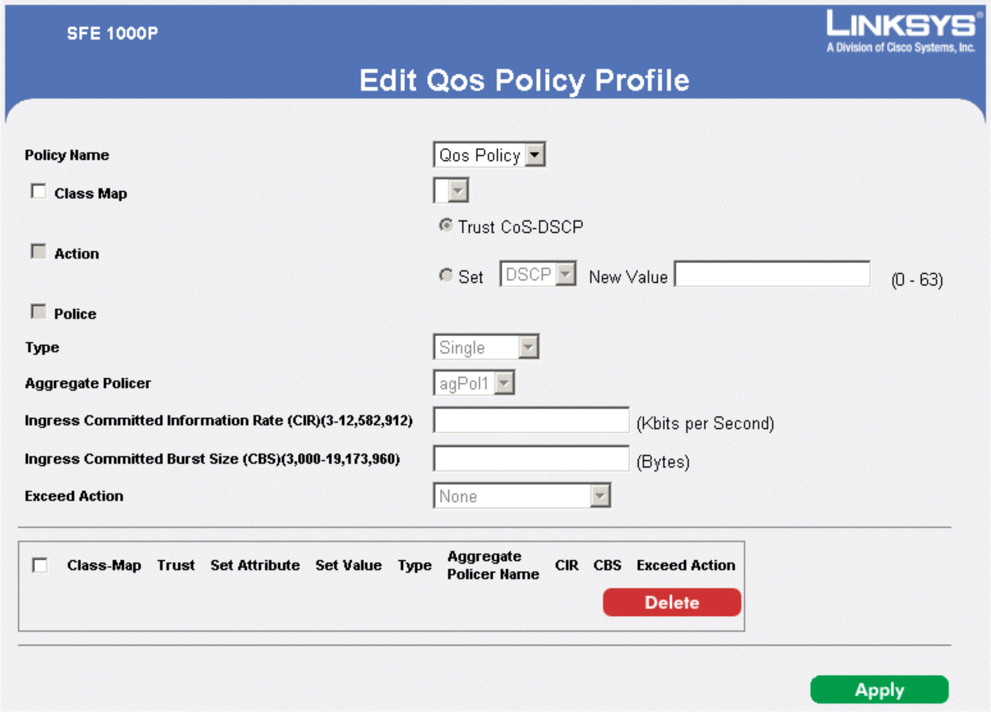
Apply

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 values are:
  - **Trust CoS-DSCP** — Enables CoS-DSCP Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.
  - **Set DSCP** — Defines the Trust configuration manually. In the **New Value** box, the possible values are 0-63.
- **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 (CbS)** — Defines the CbS 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.

## Modifying the QoS Policy Profile

*Edit QoS Policy Profile Page*



SFE 1000P

Edit Qos Policy Profile

Policy Name: Qos Policy

□ Class Map:

□ Action: ● Trust CoS-DSCP ○ Set DSCP New Value (0 - 63)

□ Police

Type: Single

Aggregate Policer: agPol1

Ingress Committed Information Rate (CIR)(3-12,582,912): (Kbits per Second)

Ingress Committed Burst Size (CBS)(3,000-19,173,960): (Bytes)

Exceed Action: None

| □ | Class-Map | Trust | Set Attribute | Set Value | Type | Aggregate Policer Name | CIR | CBS | Exceed Action |
|---|---|---|---|---|---|---|---|---|---|

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 values are:
  - **Trust CoS-DSCP** — Enables CoS-DSCP Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.
  - **Set DSCP** — Defines the Trust configuration manually. In the **New Value** box, the possible values are 0-63.
- **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.

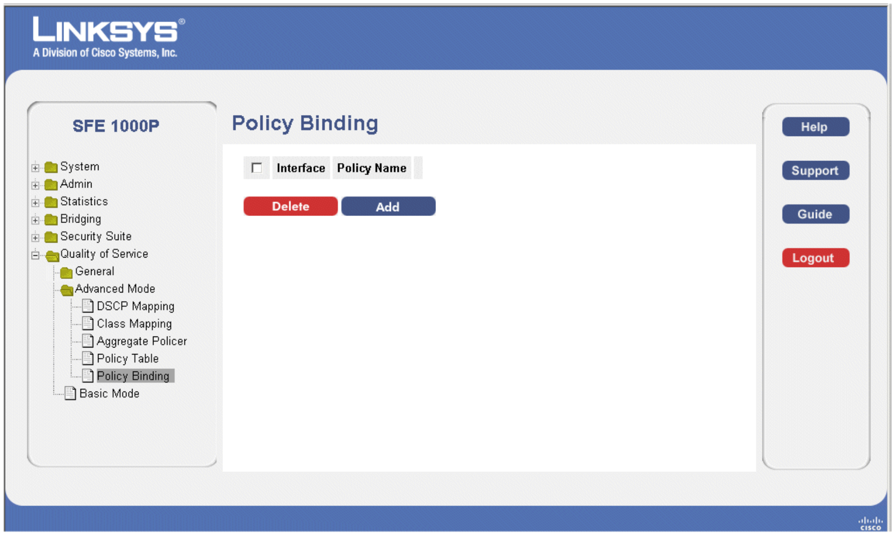
– *Single* — Configures the class to use manually configured information rates and exceed actions.

- **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 (CBS)** — Defines the CBS 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.
  - *Remark DSCP* —Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* —Forwards packets exceeding the defined CIR value.

## Defining Policy Binding

In the *Policy Binding Page*, QoS policies are associated with specific interfaces.

***Policy Binding Page***



Policy Binding

| ☐ | Interface | Policy Name |
|---|---|---|

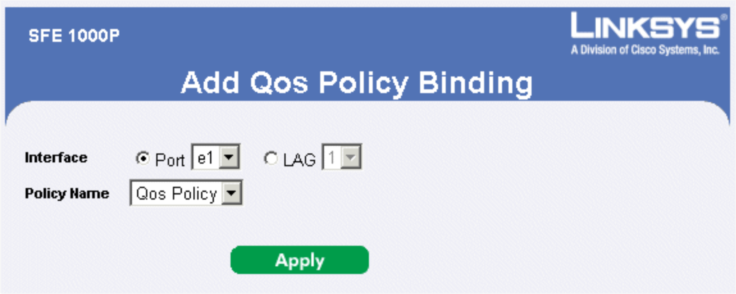
Delete Add

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.

## Adding QoS Policy Binding

*Add QoS Policy Binding Page*



SFE 1000P

Add Qos Policy Binding

Interface ● Port e1 ○ LAG 1

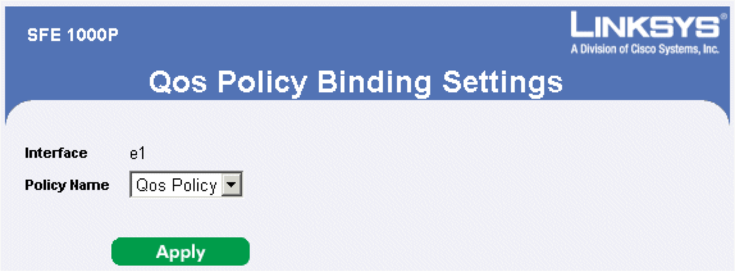
Policy Name Qos Policy

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.

## Modifying QoS Policy Binding Settings

*Edit QoS Policy Binding Page*



SFE 1000P

Qos Policy Binding Settings

Interface e1

Policy Name Qos Policy

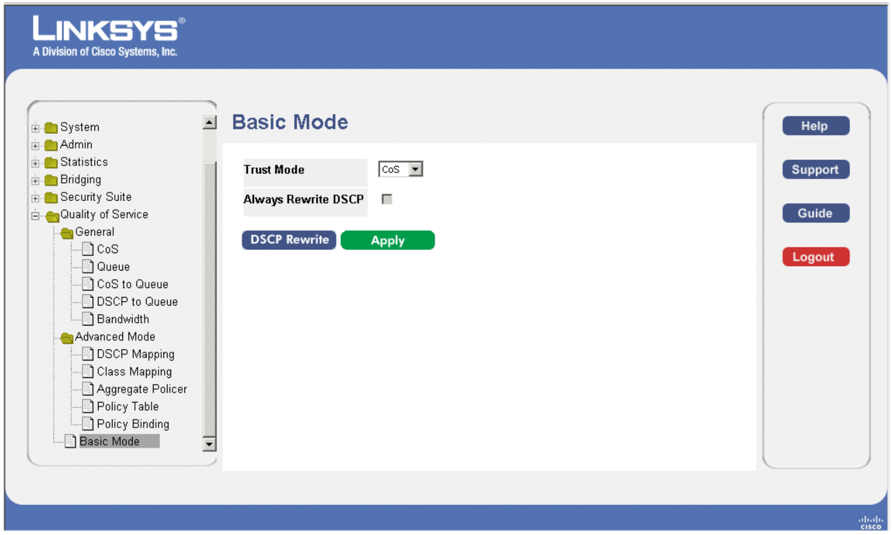
The *Edit QoS Policy Binding Page* contains the following fields.

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Displays the Policy name associated with the interface.

## 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.

***Basic Mode Page***



Basic Mode

Trust Mode: CoS

Always Rewrite DSCP: □

DSCP Rewrite | Apply

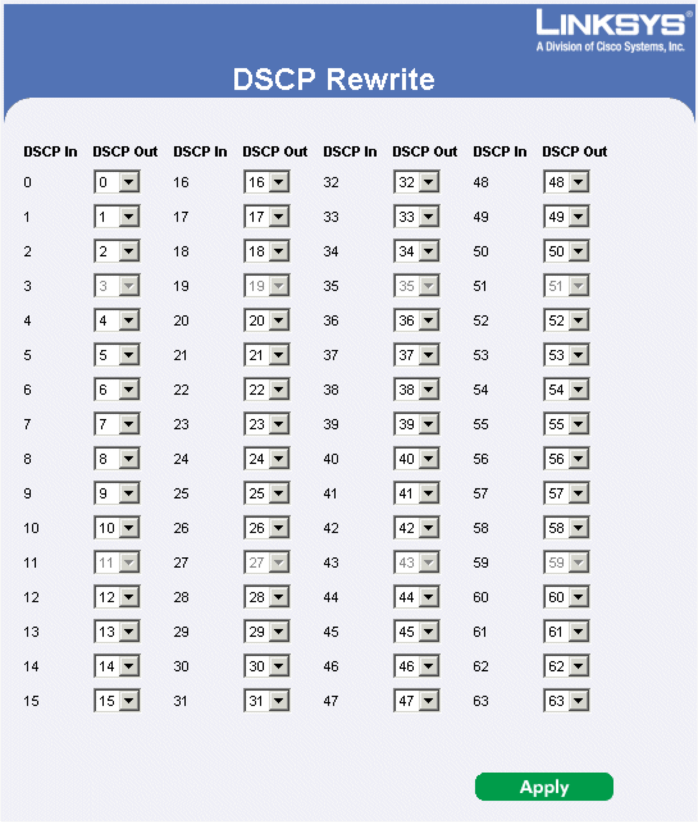
The *Basic Mode Page* contains the following fields:

- **Trust Mode** — Displays the trust mode. If a packet's CoS tag and DSCP tag, and TCP/UDP mapping 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.*

## Rewritting DSCP Values

In the *DSCP Mapping Page*, define the Differentiated Services Code Point (DSCP) tag to use in place of the incoming DSCP tags.

***DSCP Mapping Page***



| DSCP In | DSCP Out | DSCP In | DSCP Out | DSCP In | DSCP Out | DSCP In | DSCP Out |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 16 | 16 | 32 | 32 | 48 | 48 |
| 1 | 1 | 17 | 17 | 33 | 33 | 49 | 49 |
| 2 | 2 | 18 | 18 | 34 | 34 | 50 | 50 |
| 3 | 3 | 19 | 19 | 35 | 35 | 51 | 51 |
| 4 | 4 | 20 | 20 | 36 | 36 | 52 | 52 |
| 5 | 5 | 21 | 21 | 37 | 37 | 53 | 53 |
| 6 | 6 | 22 | 22 | 38 | 38 | 54 | 54 |
| 7 | 7 | 23 | 23 | 39 | 39 | 55 | 55 |
| 8 | 8 | 24 | 24 | 40 | 40 | 56 | 56 |
| 9 | 9 | 25 | 25 | 41 | 41 | 57 | 57 |
| 10 | 10 | 26 | 26 | 42 | 42 | 58 | 58 |
| 11 | 11 | 27 | 27 | 43 | 43 | 59 | 59 |
| 12 | 12 | 28 | 28 | 44 | 44 | 60 | 60 |
| 13 | 13 | 29 | 29 | 45 | 45 | 61 | 61 |
| 14 | 14 | 30 | 30 | 46 | 46 | 62 | 62 |
| 15 | 15 | 31 | 31 | 47 | 47 | 63 | 63 |

The *DSCP Mapping Page* allows the network administrator to define two DSCP tags:

- **DSCP In** — Indicates the DSCP value in the incoming packet.
- **DSCP Out** — Indicates the DSCP value in the outgoing packet that will correspond with the DSCP In value.

# Managing System Files

The Managing System Files section contains the following sections:

- File Management
- Logs
- Diagnostics

## File Management Overview

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. The file is checked for the right format, and that it is

This section contains information for defining File maintenance and includes both configuration file management as well as device access.

## File Management

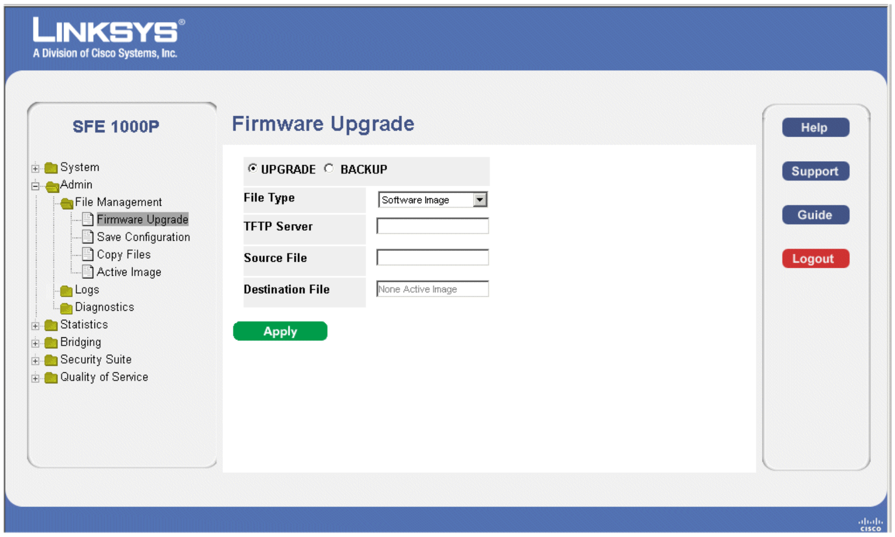
The File Management section contains the following pages:

- 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.

***Firmware Upgrade Page***



Firmware Upgrade

● UPGRADE ○ BACKUP

| | |
|---|---|
| File Type | Software Image |
| TFTP Server | |
| Source File | |
| Destination File | None Active Image |

The *Firmware Upgrade Page* contains the following fields:

- **Upgrade** — Specifies that the firmware download is a firmware upgrade.
- **Backup** — Specifies that the firmware download is a configuration backup.
- **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.
- **TFTP Server** — Specifies the TFTP Server IP Address from which files are downloaded.

- **Source File** — Specifies the file to be downloaded.
- **Destination File** — Specifies the name of the file after it is downloaded (Save As).

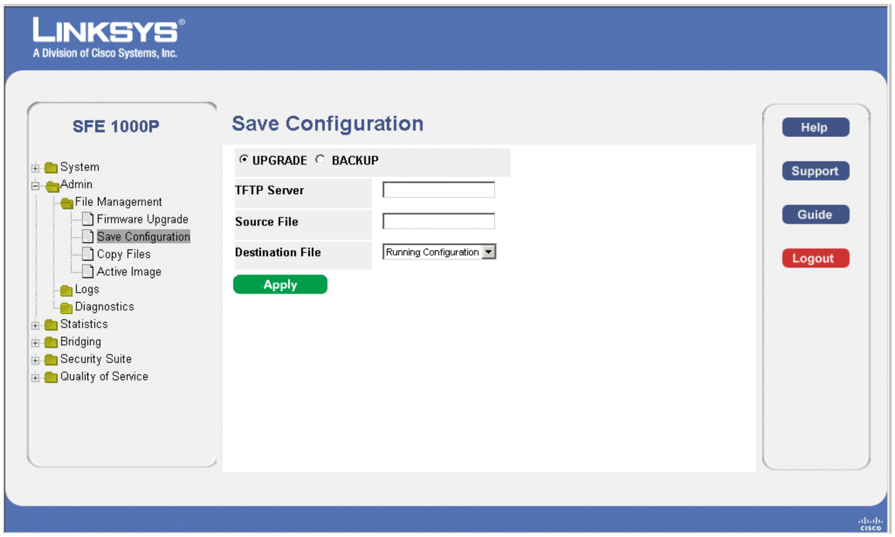
## Save Configuration

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.

***Save Configuration Page***



Save Configuration

● UPGRADE ○ BACKUP

| | |
|---|---|
| TFTP Server | |
| Source File | |
| Destination File | Running Configuration |

The *Save Configuration Page* contains the following fields:

- **Upgrade** — Specifies that the configuration file is associated with a firmware upgrade.
- **Backup** — Specifies that the configuration file contains the system backup configuration.

- **TFTP Server** — Specifies the TFTP Server IP Address for downloading or uploading the file.

- **Source File** — Name of the configuration file.

- **Destination File**— Specifies the type of configuration file to be created. The possible values are:

  – *Running* — Contains the configuration currently valid on the device.

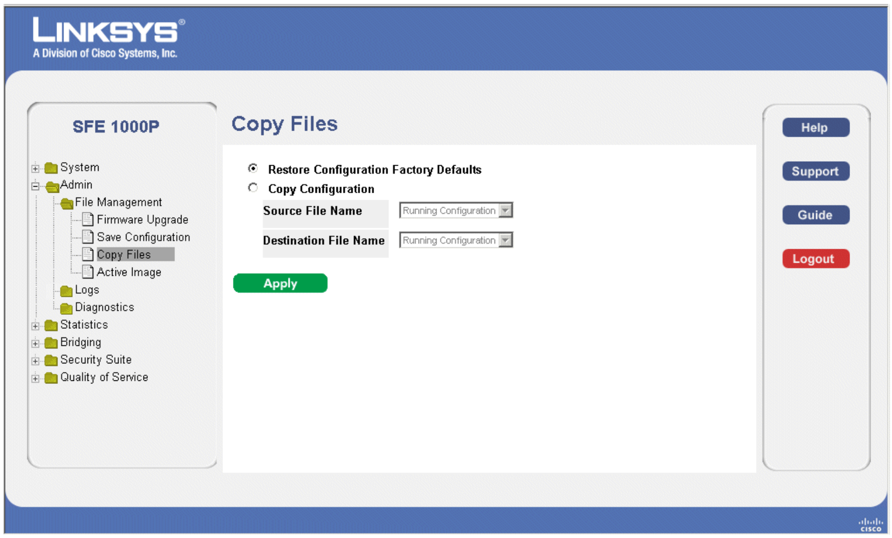
  – *Starting* — Contains the configuration which will be valid following system startup or reboot.

  – *Backup configurations* — Contains a copy of the system configuration for restoration following a shutdown or a fault.

## Copy Files

In the *Copy Files Page*, network administrators can copy configuration files from one device to another.

***Copy Files Page***



Copy Files

● Restore Configuration Factory Defaults

○ Copy Configuration

| | |
|---|---|
| Source File Name | Running Configuration |
| Destination File Name | Running Configuration |

The *Copy Files Page* contains the following fields:

- **Restore Configuration Factory Defaults** — Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When not selected, the device maintains the current Configuration file.

- **Copy Configuration** — Indicates the device configuration file to copy and the intended usage of the copied file (Running, Starting, or Backup).

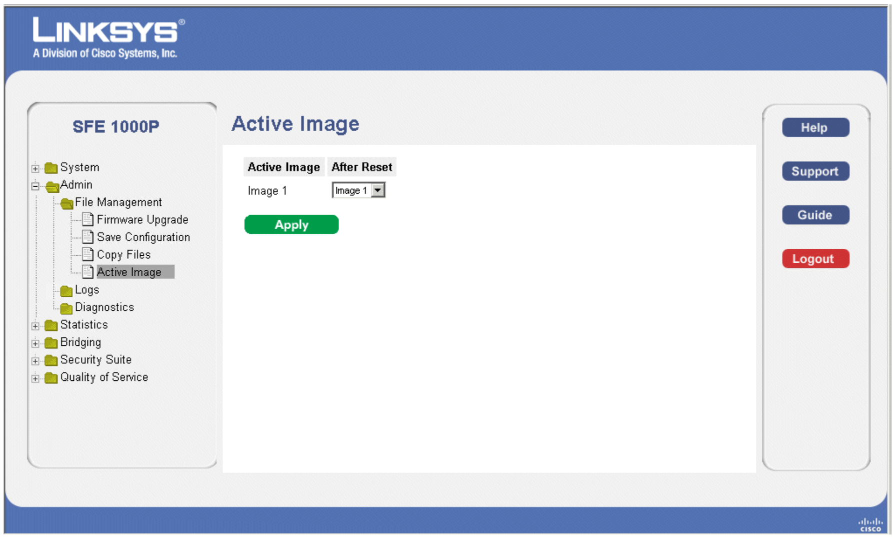
  – *Source File Name* — Indicates the type of configuration file to copy from the device.

  – *Destination File Name* — Defines the intended usage of the copied configuration file on the destination device.

## Active Image

The *Active Image Page* allows network managers to select the Image files.

***Active Image Page***



| Active Image | After Reset |
|---|---|
| Image 1 | Image 1 |

The *Active Image Page* contains the following fields:

- **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.

# 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 pages:

- Enabling System Logs
- Viewing the Device Memory Logs
- Viewing the Flash Logs
- Viewing Remote Logs

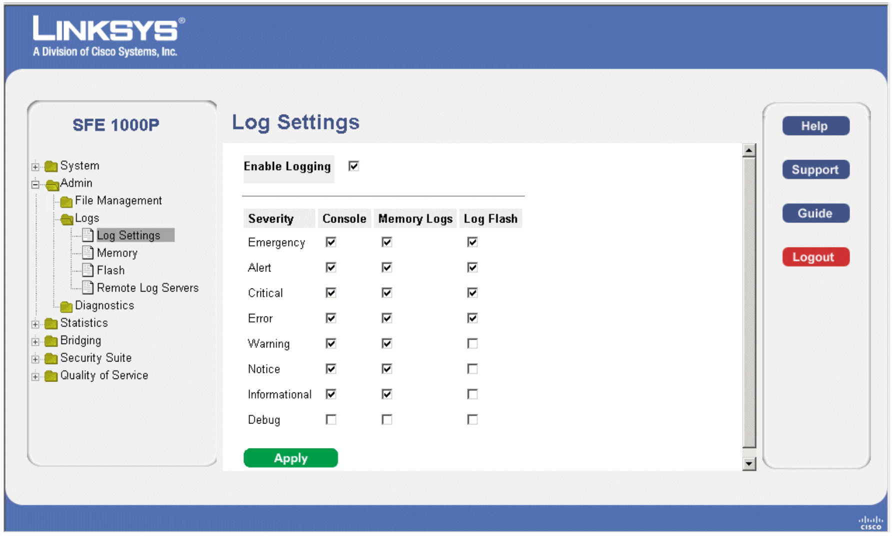
## Enabling System Logs

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.

*Log Settings Page*



Log Settings

Enable Logging ☑

| Severity | Console | Memory Logs | Log Flash |
|---|---|---|---|
| Emergency | ☑ | ☑ | ☑ |
| Alert | ☑ | ☑ | ☑ |
| Critical | ☑ | ☑ | ☑ |
| Error | ☑ | ☑ | ☑ |
| Warning | ☑ | ☑ | □ |
| Notice | ☑ | ☑ | □ |
| Informational | ☑ | ☑ | □ |
| Debug | □ | □ | □ |

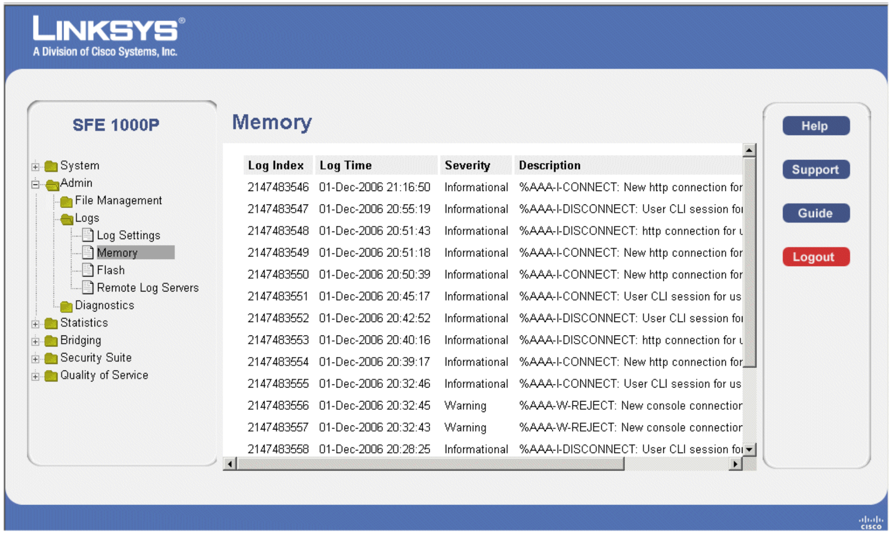
The *Log Settings Page* contains the following fields:

- **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.

## 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.

***Memory Page***



Memory

| Log Index | Log Time | Severity | Description |
|---|---|---|---|
| 2147483546 | 01-Dec-2006 21:16:50 | Informational | %AAA-I-CONNECT: New http connection for |
| 2147483547 | 01-Dec-2006 20:55:19 | Informational | %AAA-I-DISCONNECT: User CLI session fo |
| 2147483548 | 01-Dec-2006 20:51:43 | Informational | %AAA-I-DISCONNECT: http connection for u |
| 2147483549 | 01-Dec-2006 20:51:18 | Informational | %AAA-I-CONNECT: New http connection for |
| 2147483550 | 01-Dec-2006 20:50:39 | Informational | %AAA-I-CONNECT: New http connection for |
| 2147483551 | 01-Dec-2006 20:45:17 | Informational | %AAA-I-CONNECT: User CLI session for us |
| 2147483552 | 01-Dec-2006 20:42:52 | Informational | %AAA-I-DISCONNECT: User CLI session fo |
| 2147483553 | 01-Dec-2006 20:40:16 | Informational | %AAA-I-DISCONNECT: http connection for u |
| 2147483554 | 01-Dec-2006 20:39:17 | Informational | %AAA-I-CONNECT: New http connection for |
| 2147483555 | 01-Dec-2006 20:32:46 | Informational | %AAA-I-CONNECT: User CLI session for us |
| 2147483556 | 01-Dec-2006 20:32:45 | Warning | %AAA-W-REJECT: New console connectior |
| 2147483557 | 01-Dec-2006 20:32:43 | Warning | %AAA-W-REJECT: New console connectior |
| 2147483558 | 01-Dec-2006 20:28:25 | Informational | %AAA-I-DISCONNECT: User CLI session fo |

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.

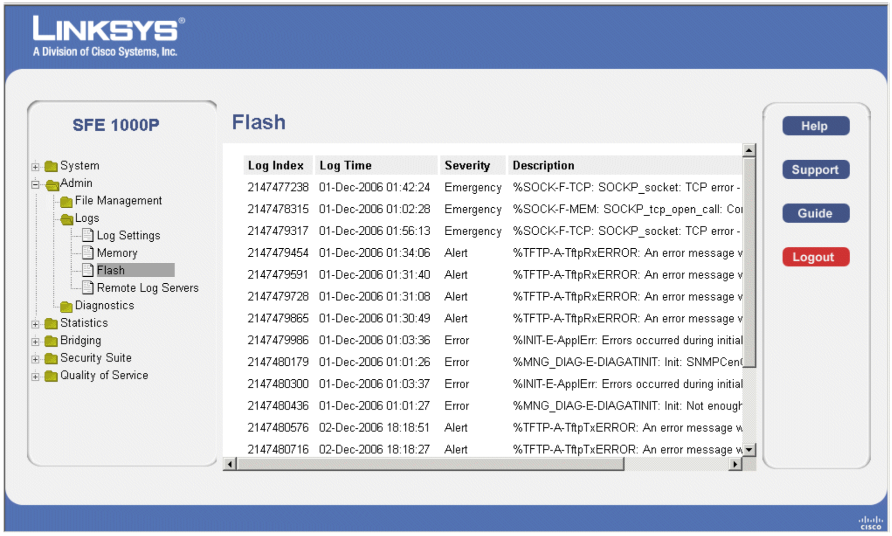
## Clearing Message Logs

To clear the *Memory Page,* 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.

***Flash Page***



Flash

| Log Index | Log Time | Severity | Description |
|---|---|---|---|
| 2147477238 | 01-Dec-2006 01:42:24 | Emergency | %SOCK-F-TCP: SOCKP_socket: TCP error - |
| 2147478315 | 01-Dec-2006 01:02:28 | Emergency | %SOCK-F-MEM: SOCKP_tcp_open_call: Co |
| 2147479317 | 01-Dec-2006 01:56:13 | Emergency | %SOCK-F-TCP: SOCKP_socket: TCP error - |
| 2147479454 | 01-Dec-2006 01:34:06 | Alert | %TFTP-A-TftpRxERROR: An error message v |
| 2147479591 | 01-Dec-2006 01:31:40 | Alert | %TFTP-A-TftpRxERROR: An error message v |
| 2147479728 | 01-Dec-2006 01:31:08 | Alert | %TFTP-A-TftpRxERROR: An error message v |
| 2147479865 | 01-Dec-2006 01:30:49 | Alert | %TFTP-A-TftpRxERROR: An error message v |
| 2147479986 | 01-Dec-2006 01:03:36 | Error | %INIT-E-ApplErr: Errors occurred during initial |
| 2147480179 | 01-Dec-2006 01:01:26 | Error | %MNG_DIAG-E-DIAGATINIT: Init: SNMPCen |
| 2147480300 | 01-Dec-2006 01:03:37 | Error | %INIT-E-ApplErr: Errors occurred during initial |
| 2147480436 | 01-Dec-2006 01:01:27 | Error | %MNG_DIAG-E-DIAGATINIT: Init: Not enough |
| 2147480576 | 02-Dec-2006 18:18:51 | Alert | %TFTP-A-TftpTxERROR: An error message w |
| 2147480716 | 02-Dec-2006 18:18:27 | Alert | %TFTP-A-TftpTxERROR: An error message w |

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 Message Logs

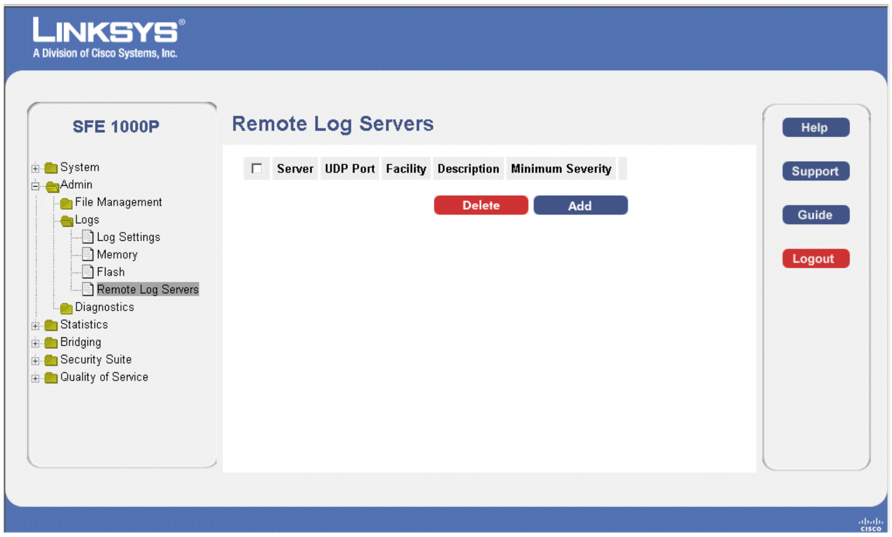
Message Logs can be cleared from the *FLASH Log Page*.

To clear the *Flash Page,* click the **Clear Logs** button**.** 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.

***Remote Log Servers Page***



Remote Log Servers

| □ | Server | UDP Port | Facility | Description | Minimum Severity |
|---|---|---|---|---|---|

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.

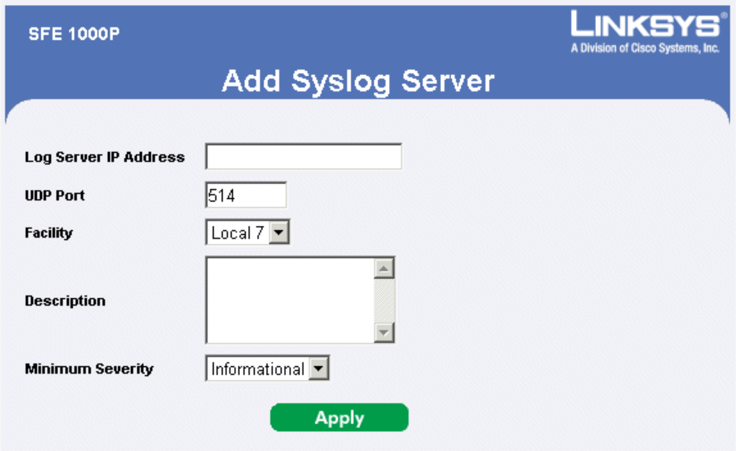
  – *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.

- *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.

## Adding a System Log Server

The *Add Syslog Server Page* contains fields for defining new Remote Log Servers.

***Add Syslog Server Page***



Log Server IP Address

UDP Port 514

Facility Local 7

Description

Minimum Severity Informational

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

- **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.

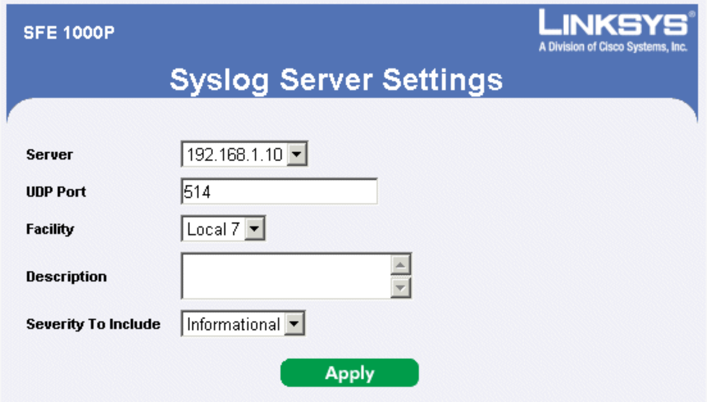
  The following are the available log severity levels:

  - *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.
  - *Notice* — The system is functioning properly, but system notice has occurred.
  - *Informational* — Provides device information.
  - *Debug* — Provides debugging messages.

## Modify Syslog Server Settings

The *Edit Syslog Server Page* contains fields for modifying Remote Log Server settings.

***Edit Syslog Server Page***



SFE 1000P

LINKSYS® A Division of Cisco Systems, Inc.

Syslog Server Settings

| | |
|---|---|
| Server | 192.168.1.10 |
| UDP Port | 514 |
| Facility | Local 7 |
| Description | |
| Severity To Include | Informational |

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.
- *Notice* — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

# 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.

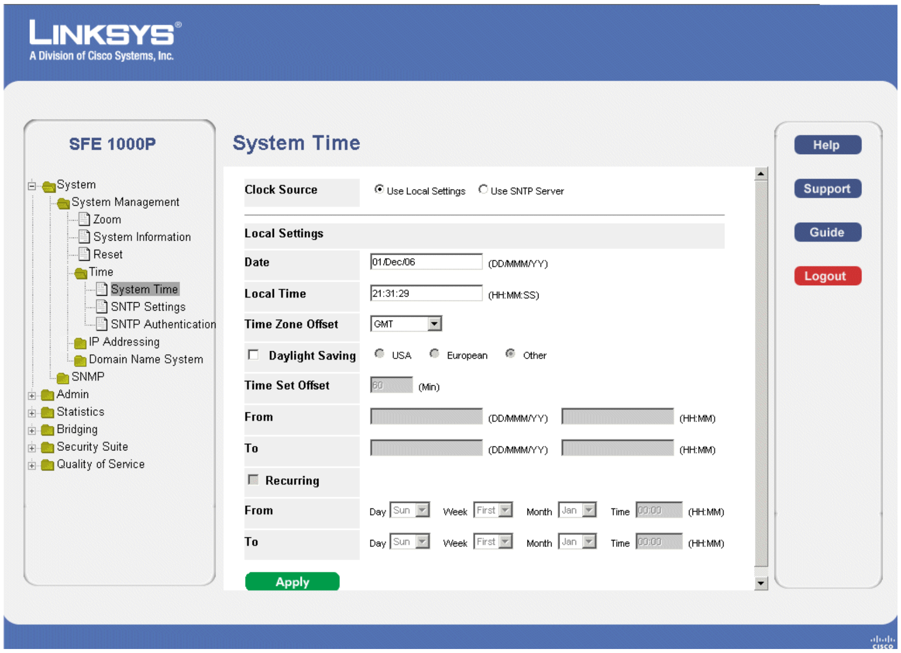
This section provides information for configuring the system time, and includes the following topics: including:

- 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.

***System Time Page***



System Time

| | |
|---|---|
| Clock Source | ● Use Local Settings ○ Use SNTP Server |
| Local Settings | |
| Date | 01/Dec/06 (DD/MMM/YY) |
| Local Time | 21:31:29 (HH:MM:SS) |
| Time Zone Offset | GMT |
| □ Daylight Saving | ○ USA ○ European ● Other |
| Time Set Offset | 60 (Min) |
| From | (DD/MMM/YY) (HH:MM) |
| To | (DD/MMM/YY) (HH:MM) |
| □ Recurring | |
| From | Day Sun Week First Month Jan Time 00:00 (HH:MM) |
| To | Day Sun Week First Month Jan Time 00:00 (HH:MM) |

The *System Time Page* contains the following fields:

- **Clock Source —** Indicates the source used to set the system clock. The possible field values:
  – *SNTP* — Sets the system time via an SNTP server.

   - *Local Settings* — The system time is set on the local device. This is the default value.

- **Date —** Indicates the system date. The field format is Day:Month:Year, for example, 04 May 2050.

- **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* — The device switches to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.

   - *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 (1-1440) —** 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 Day:Month:Year 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. The possible field values are:

   - *Date* — The date at which DST begins. The possible field range is 1-31.

   - *Month* — The month of the year in which DST begins. The possible field range is Jan-Dec.

   - *Year* — The year in which the configured DST begins.

   - *Time* — The time at which DST begins. The field format is Hour:Minute, for example, 05:30.

- **To —** Indicates the time that DST ends in countries other than USA or Europe in the Day:Month:Year 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. The possible field values are:

   - *Date* — The date at which DST ends. The possible field range is 1-31.

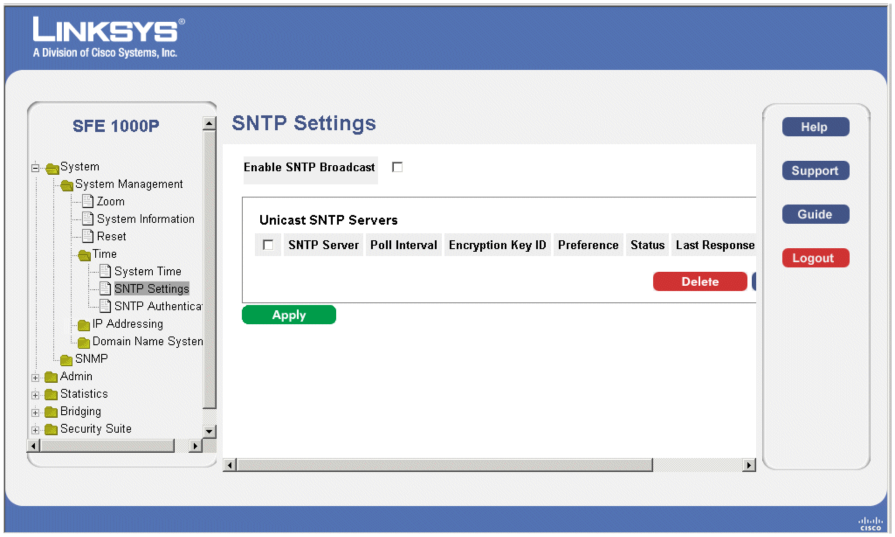
  - *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
  - *Year*— The year in which the configured DST ends.
  - *Time* — The time at which DST starts. The field format is Hour:Minute, for example, 05:30.

- **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.

## 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.

***SNTP Settings Page***



SNTP Settings

Enable SNTP Broadcast □

Unicast SNTP Servers

| □ | SNTP Server | Poll Interval | Encryption Key ID | Preference | Status | Last Response |
|---|---|---|---|---|---|---|

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 looking for an interface.
- **Status** — The operating SNTP server status. The possible field values are:

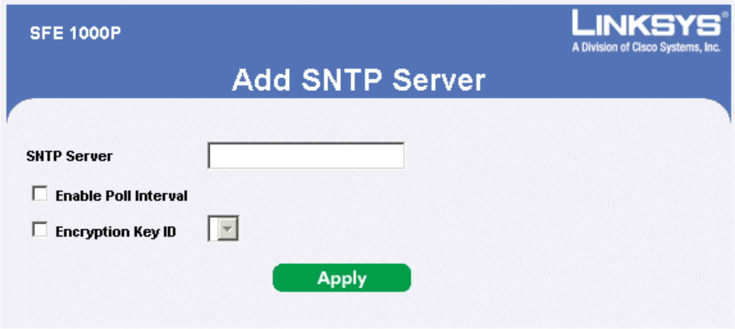
- *Up* — The SNTP server is currently operating normally.
- *Down* — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.

- **Last Response** — Indicates the last time a response was received from the SNTP server.
- **Offset** — Indicates the Timestamp difference between the device local clock and the acquired time from the SNTP server.
- **Delay** — Indicates the amount of time it takes to reach the SNTP server.

## Add SNTP Server

The *Add SNTP Server Page* provides parameters for adding an SNTP server.

***Add SNTP Server Page***



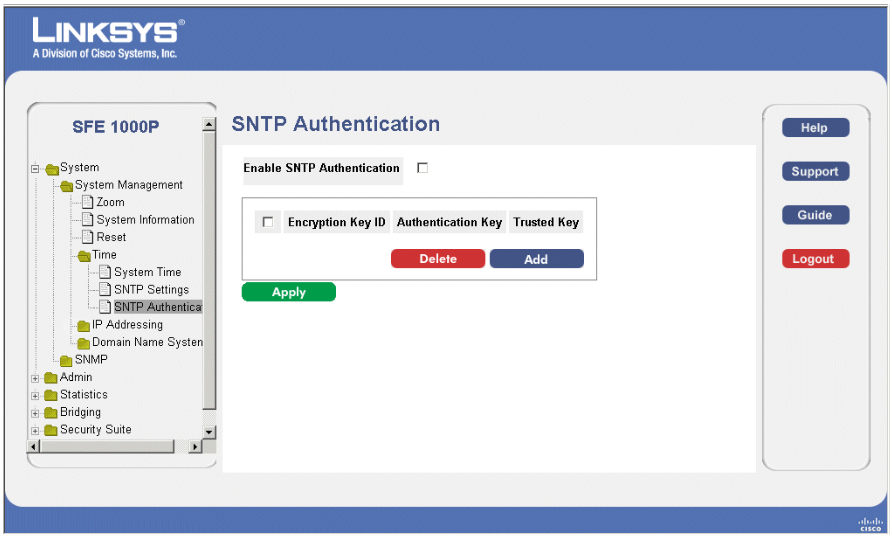
The *Add SNTP Server Page* contains the following fields:

- **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.

## Defining SNTP Authentication

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

***SNTP Authentication Page***

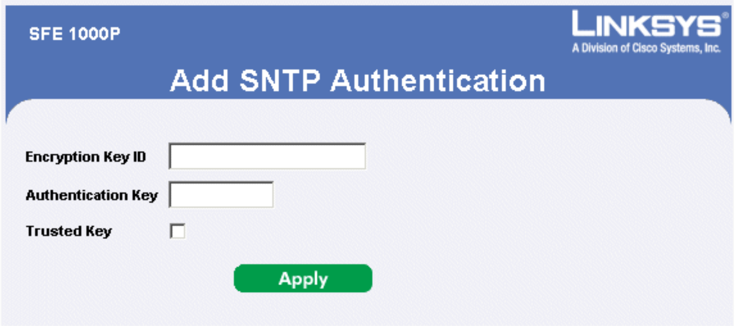


The *SNTP Authentication Page* contains the following fields:

- **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.

## Add SNTP Authentication

*Add SNTP Authentication Page*



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.

# 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

## Viewing Ethernet Statistics

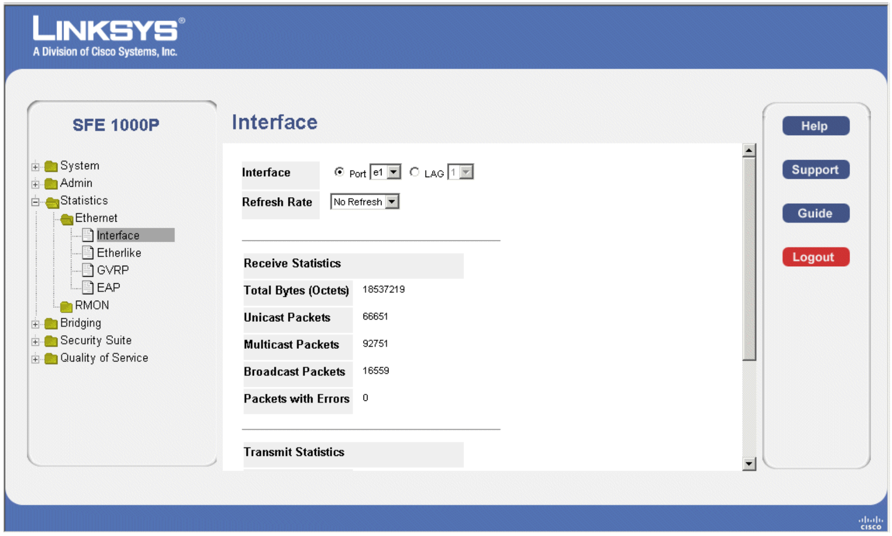
The Ethernet section contains the following pages:

- Defining Ethernet Interface
- Viewing Etherlike Statistics
- Viewing GVRP Statistics
- Viewing EAP Statistics

### Defining Ethernet Interface

The *Interface Page* contains statistics for both received and transmitted packets. The *Interface Page* is divided into three areas, General Information, Receive Statistics and Transmit Statistics.

***Interface Page***



Interface

| | |
|---|---|
| Interface | ● Port e1 ○ LAG 1 |
| Refresh Rate | No Refresh |

| Receive Statistics | |
|---|---|
| Total Bytes (Octets) | 18537219 |
| Unicast Packets | 66651 |
| Multicast Packets | 92751 |
| Broadcast Packets | 16559 |
| Packets with Errors | 0 |

Transmit Statistics

The *Interface Page* contains the following fields:

The General Information area 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.
  - *No Refresh* — Indicates that the Ethernet statistics are not refreshed.

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.

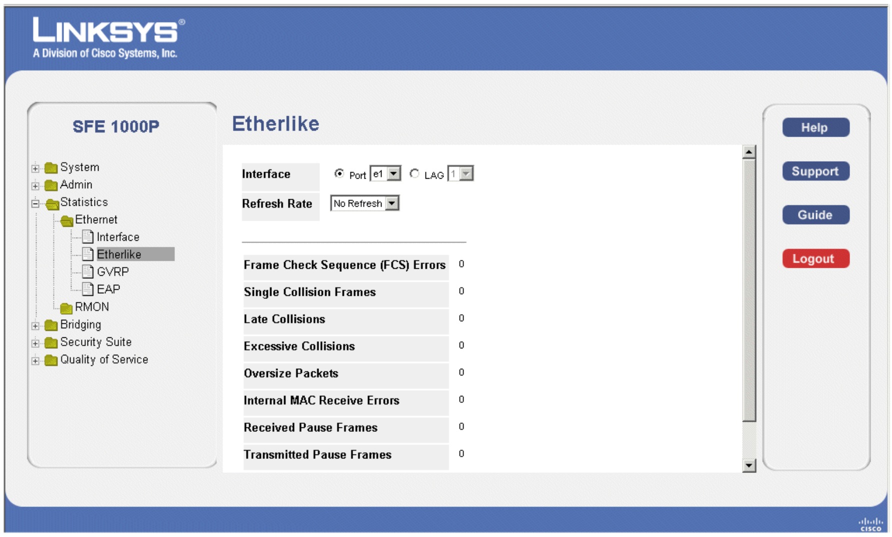
## Resetting Interface Statistics Counters

To clear the statistics counters, click the **Clear Counters** button.

## Viewing Etherlike Statistics

The *Etherlike Page* contains interface statistics.

***Etherlike Page***



Etherlike

Interface ● Port e1 ○ LAG 1

Refresh Rate No Refresh

| | |
|---|---|
| Frame Check Sequence (FCS) Errors | 0 |
| Single Collision Frames | 0 |
| Late Collisions | 0 |
| Excessive Collisions | 0 |
| Oversize Packets | 0 |
| Internal MAC Receive Errors | 0 |
| Received Pause Frames | 0 |
| Transmitted Pause Frames | 0 |

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.
  - *No Refresh* — Indicates that the Etherlike statistics are not refreshed.
- **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.

- **Excessive Collisions** — Displays the number of excessive collisions 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.

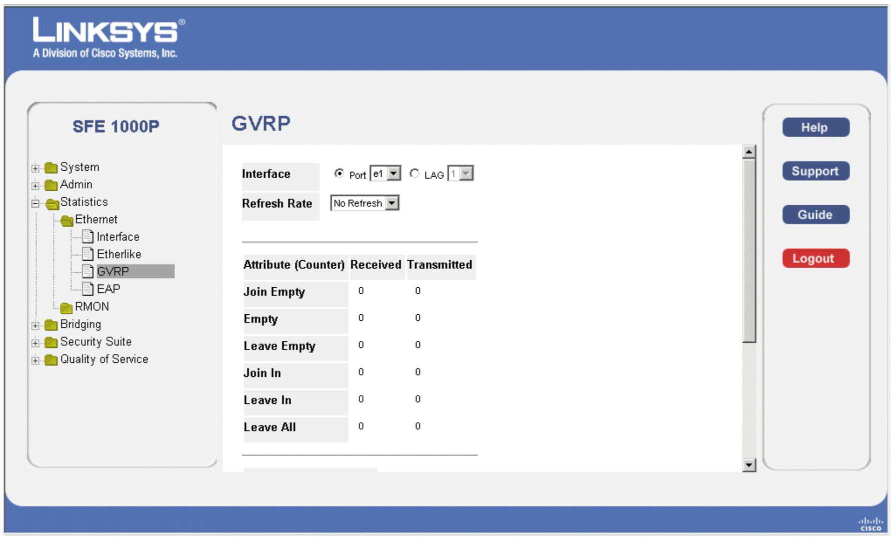
## Resetting Etherlike Statistics Counters

To clear the statistics counters, click the **Clear Counters** button.

# Viewing GVRP Statistics

The *GVRP Page* contains statistics for GVRP communication on the device.

***GVRP Page***



GVRP

Interface ● Port e1 ○ LAG 1

Refresh Rate No Refresh

| Attribute (Counter) | Received | Transmitted |
|---|---|---|
| Join Empty | 0 | 0 |
| Empty | 0 | 0 |
| Leave Empty | 0 | 0 |
| Join In | 0 | 0 |
| Leave In | 0 | 0 |
| Leave All | 0 | 0 |

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.
  - *No Refresh* — Indicates that the GVRP statistics are not refreshed.

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 Events** — Displays the device GVRP Invalid Events statistics.

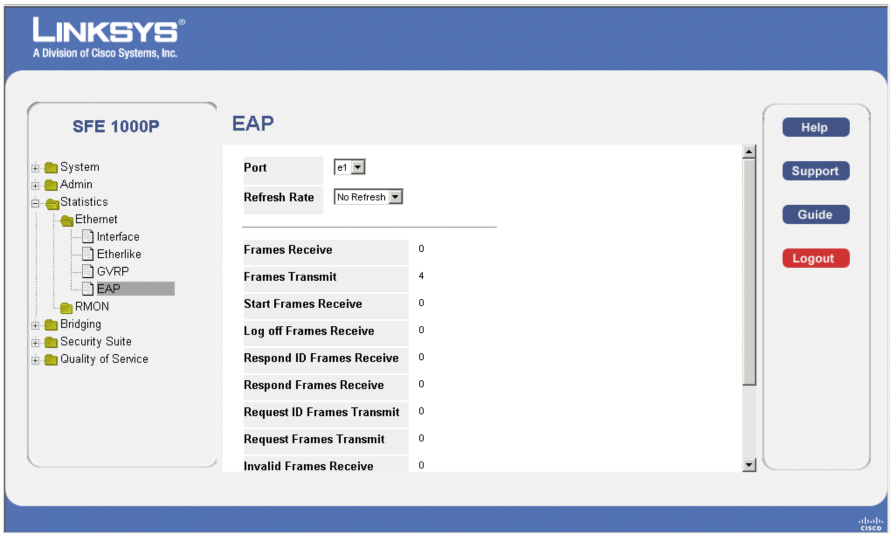
## Resetting GVRP Statistics Counters

To clear the statistics counters, click the **Clear Counters** button.

## Viewing EAP Statistics

The *EAP Page* contains information about EAP packets received on a specific port.

***EAP Page***



EAP

| | |
|---|---|
| Port | e1 |
| Refresh Rate | No Refresh |

| | |
|---|---|
| Frames Receive | 0 |
| Frames Transmit | 4 |
| 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 |

The EAP Page page contains the following fields:

- **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.
  - *No Refresh* — Indicates that the EAP statistics are not refreshed.
- **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 Respond 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

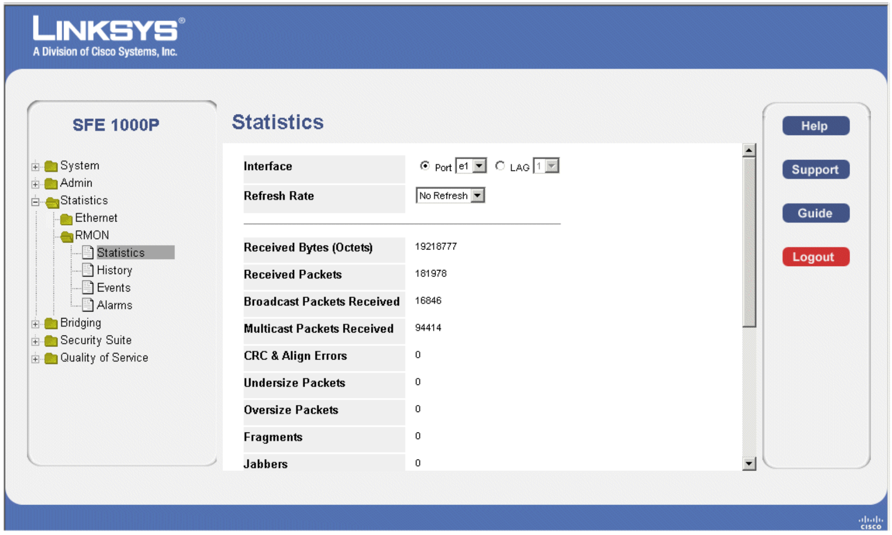
The RMON section contains the following pages:

- Viewing RMON Statistics
- Configuring RMON History
- Configuring RMON Events
- 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.

***RMON Statistics Page***



Statistics

| | |
|---|---|
| Interface | ● Port e1 ○ LAG 1 |
| Refresh Rate | No Refresh |
| Received Bytes (Octets) | 19218777 |
| Received Packets | 181978 |
| Broadcast Packets Received | 16846 |
| Multicast Packets Received | 94414 |
| CRC & Align Errors | 0 |
| Undersize Packets | 0 |
| Oversize Packets | 0 |
| Fragments | 0 |
| Jabbers | 0 |

The *RMON Statistics 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 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.

– *No Refresh* — Indicates that the RMON statistics are not refreshed.

- **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, 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.

## Resetting RMON Statistics Counters

To clear the statistics counters, click the **Clear Counters** button.

# Configuring RMON History

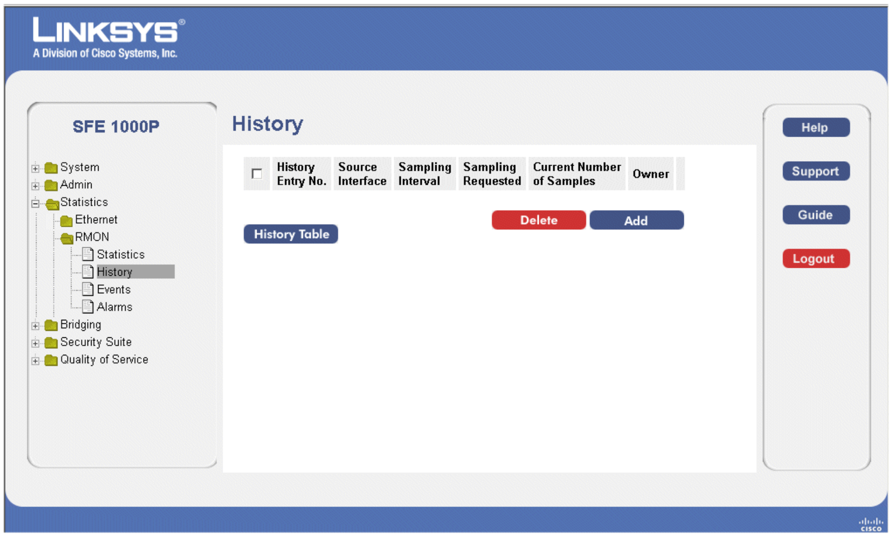
This section contains the following topics:

- 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.

***RMON History Control Page***



| ☐ | History Entry No. | Source Interface | Sampling Interval | Sampling Requested | Current Number of Samples | Owner |
|---|---|---|---|---|---|---|

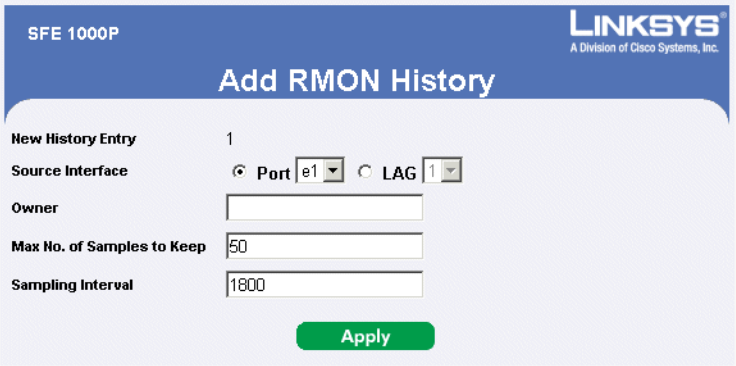
The *RMON History Control Page* contains the following fields:

- **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:
  - *Port* — Specifies the port from which the RMON information was taken.
  - *LAG* — 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.

## Add RMON History

***Add RMON History Page***



Add RMON History

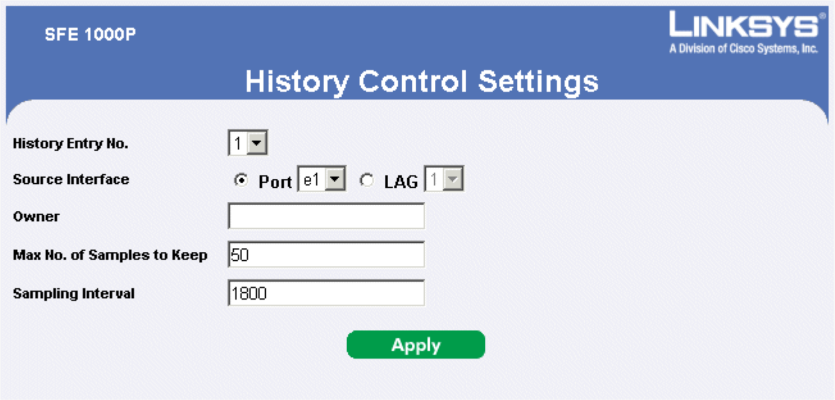
| | |
|---|---|
| New History Entry | 1 |
| Source Interface | ● Port e1 ○ LAG 1 |
| Owner | |
| Max No. of Samples to Keep | 50 |
| Sampling Interval | 1800 |

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).

## Modify History Control Settings

*Edit RMON History Page*



History Entry No. 1

Source Interface ● Port e1 ○ LAG 1

Owner

Max No. of Samples to Keep 50

Sampling Interval 1800

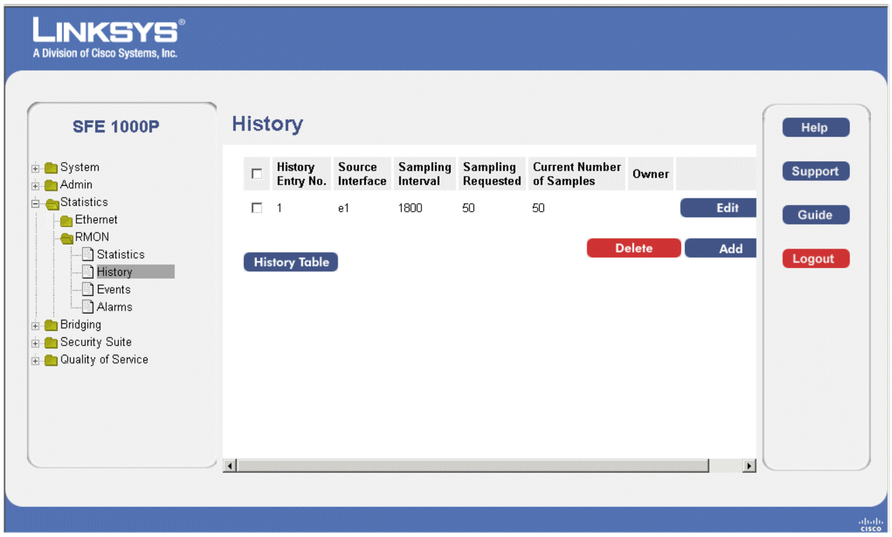
The *Edit RMON History Page* contains the following fields:

- **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).

## 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.

***RMON History Table Page***



History

| □ | History Entry No. | Source Interface | Sampling Interval | Sampling Requested | Current Number of Samples | Owner |
|---|---|---|---|---|---|---|
| □ | 1 | e1 | 1800 | 50 | 50 | |

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.

## Configuring RMON Events

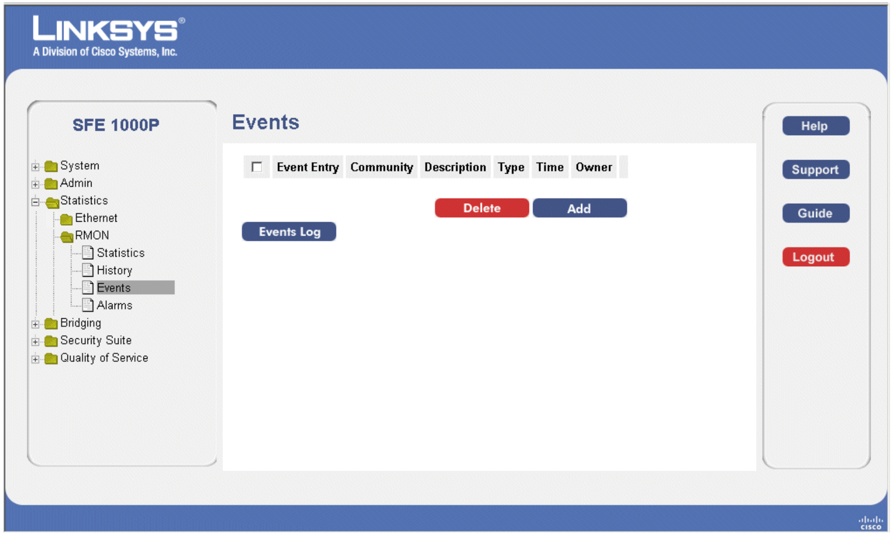
This section includes the following topics:

- Defining RMON Events Control
- Viewing the RMON Events Logs

### Defining RMON Events Control

The *RMON Events Page* contains fields for defining RMON events.

***RMON Events Page***



Events

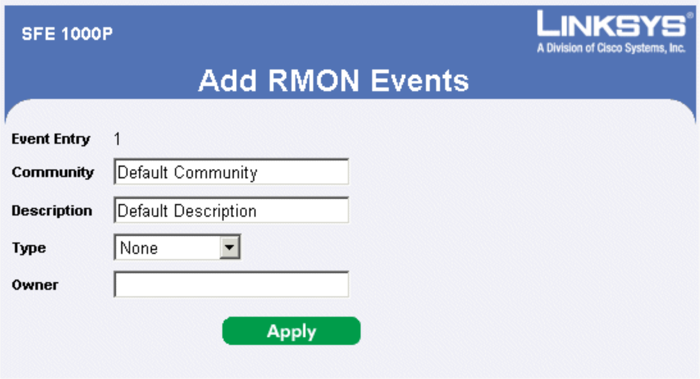
| □ | Event Entry | Community | Description | Type | Time | Owner |
|---|---|---|---|---|---|---|

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.

## Add RMON Events

***Add RMON Events Page***



SFE 1000P

LINKSYS® A Division of Cisco Systems, Inc.

Add RMON Events

Event Entry 1

Community Default Community

Description Default Description

Type None

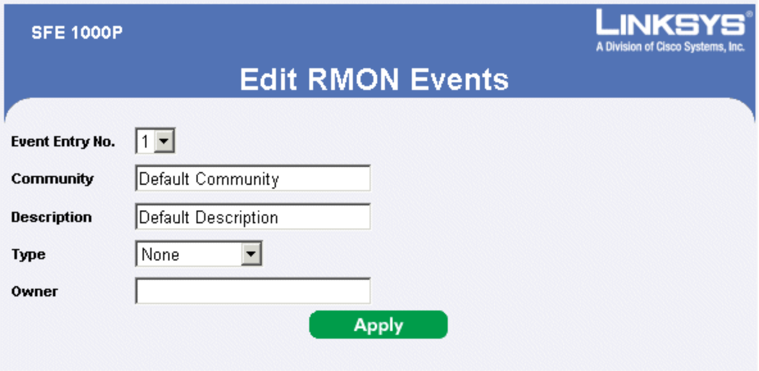
Owner

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.

## Modify Event Control Settings

***Edit RMON Events Page***



|  |  |
|---|---|
| Event Entry No. | 1 |
| Community | Default Community |
| Description | Default Description |
| Type | None |
| Owner |  |

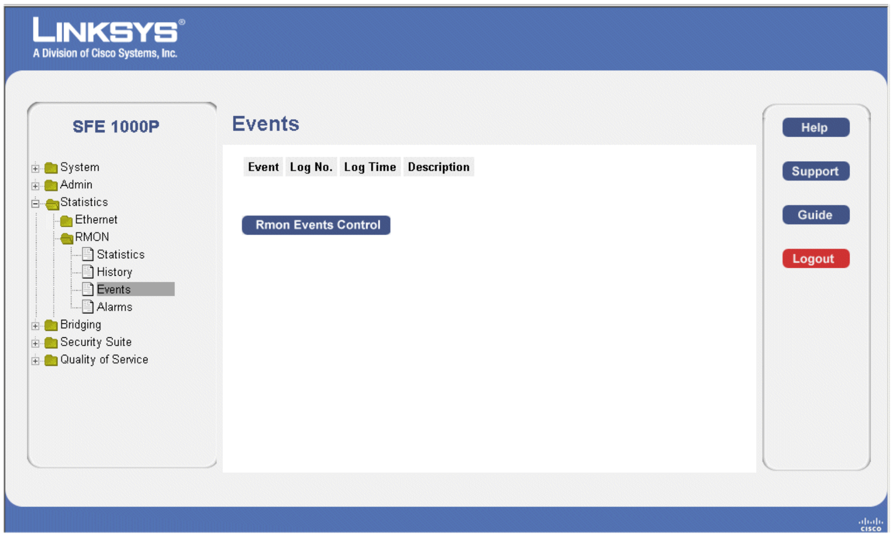
The *Edit RMON Events Page* contains the following fields:

- **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.

## Viewing the RMON Events Logs

The RMON *Events Log Page* contains a list of RMON events.

***Events Log Page***



Events

| Event | Log No. | Log Time | Description |
|---|---|---|---|

The *Events Log Page* contains the following fields:

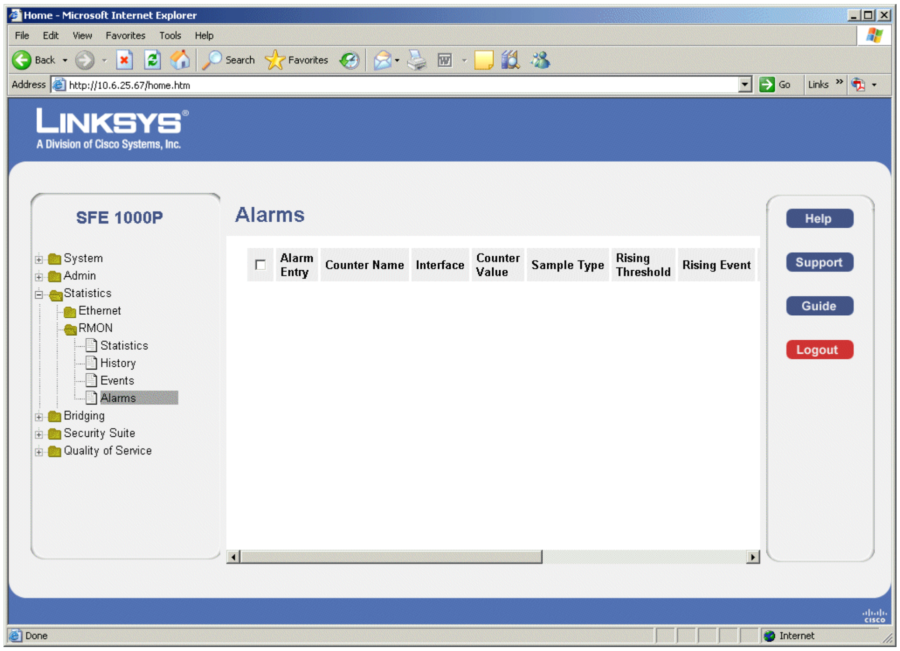
- **Event** — Displays the RMON Events Log entry number.
- **Log No.—** Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

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.

***RMON Alarms Page***



| □ | Alarm Entry | Counter Name | Interface | Counter Value | Sample Type | Rising Threshold | Rising Event |
|---|---|---|---|---|---|---|---|

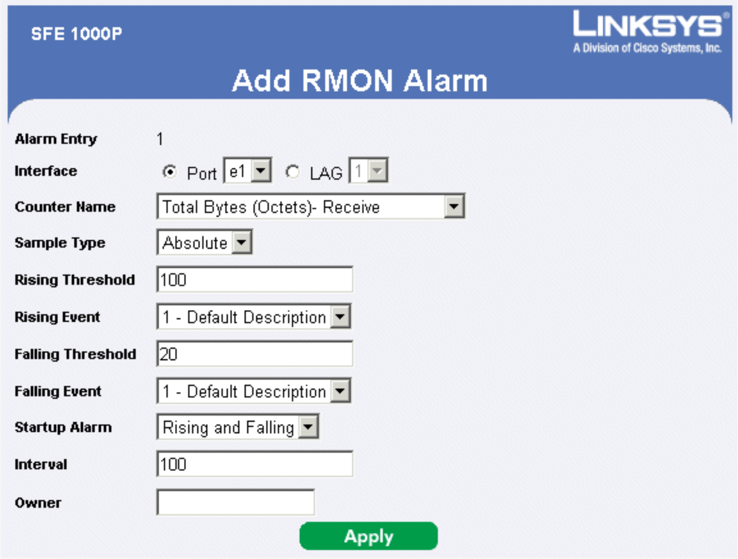
The *RMON Alarms Page* contains the following fields:

- **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.

## Add RMON Alarm

*Add RMON Alarm Page*



SFE 1000P

Add RMON Alarm

| | |
|---|---|
| Alarm Entry | 1 |
| Interface | ● Port e1 ○ LAG 1 |
| Counter Name | Total Bytes (Octets)- Receive |
| 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 | 100 |
| Owner | |

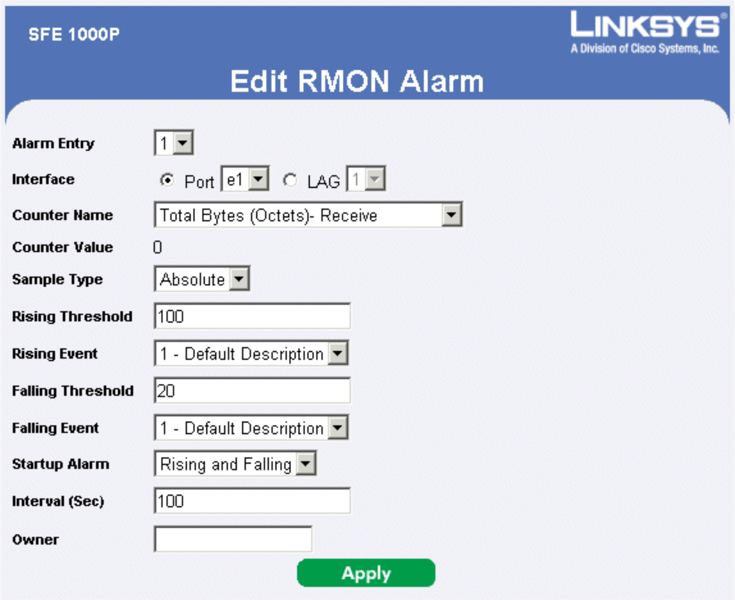
The *Add RMON Alarm Page* contains the following fields:

- **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.
  - *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** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

## Modify RMON Alarm Settings

*Edit RMON Alarms Page*



SFE 1000P

Edit RMON Alarm

| | |
|---|---|
| Alarm Entry | 1 |
| Interface | ● Port e1 ○ 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 | |

The *Edit RMON Alarms 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.
  - *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** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm

# Managing Device Diagnostics

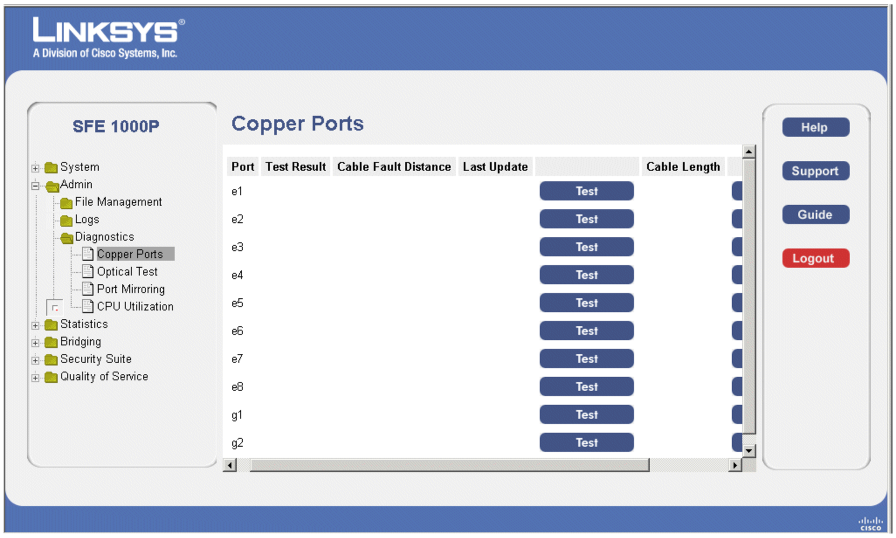
This section contains information for configuring port mirroring, running cable tests, and viewing device operational information, and includes the following topics:

- Viewing Integrated Cable Tests
- Performing Optical Tests
- Configuring Port Mirroring
- Defining 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.

***Copper Ports Page***



Copper Ports

| Port | Test Result | Cable Fault Distance | Last Update | | Cable Length |
|---|---|---|---|---|---|
| e1 | | | | Test | |
| e2 | | | | Test | |
| e3 | | | | Test | |
| e4 | | | | Test | |
| e5 | | | | Test | |
| e6 | | | | Test | |
| e7 | | | | Test | |
| e8 | | | | Test | |
| g1 | | | | Test | |
| g2 | | | | Test | |

The *Copper Ports Page* contains the following fields:

- **Port** — Specifies the port to which the tested 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.

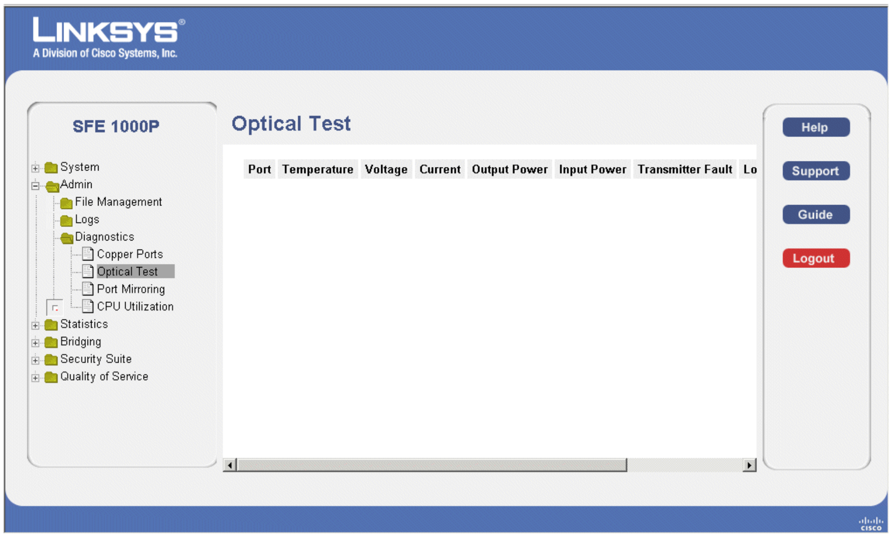
- *Open Cable* — Indicates that a cable is connected on only one side.
- *Short Cable* — Indicates that a short has occurred in the cable.

- **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.

## 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. During the port test, the port moves to a down state.

***Optical Test Page***



Optical Test

| Port | Temperature | Voltage | Current | Output Power | Input Power | Transmitter Fault | Lo |
|---|---|---|---|---|---|---|---|

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.

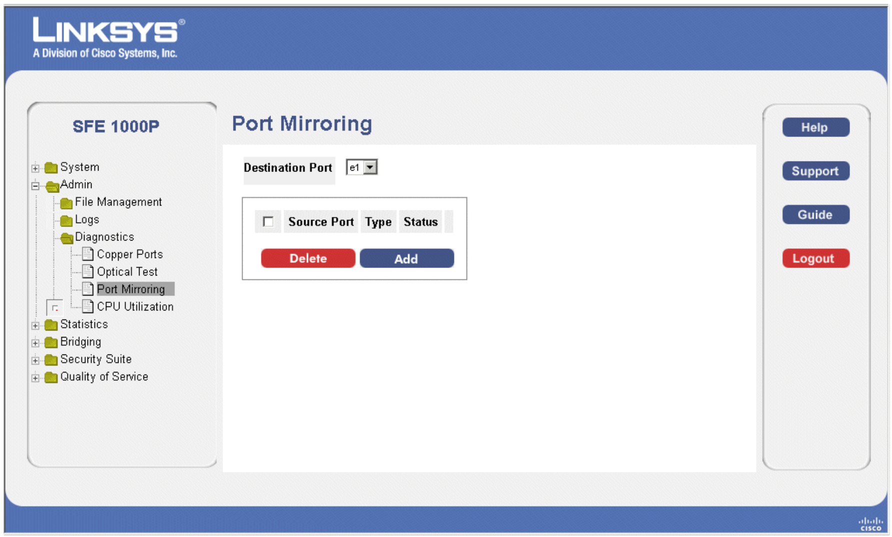
- **Data Ready** — Indicates the data status.

## 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.

***Port Mirroring Page***



Port Mirroring

Destination Port e1

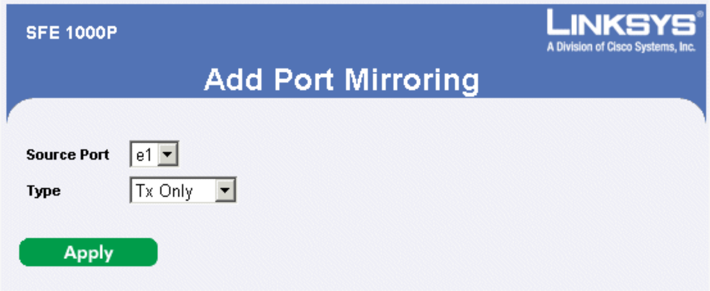
| □ | Source Port | Type | Status |
|---|---|---|---|

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 on receiving ports.
  - *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.

## Adding Port Mirroring Session

***Add Port Mirroring Page***



SFE 1000P

Add Port Mirroring

Source Port: e1

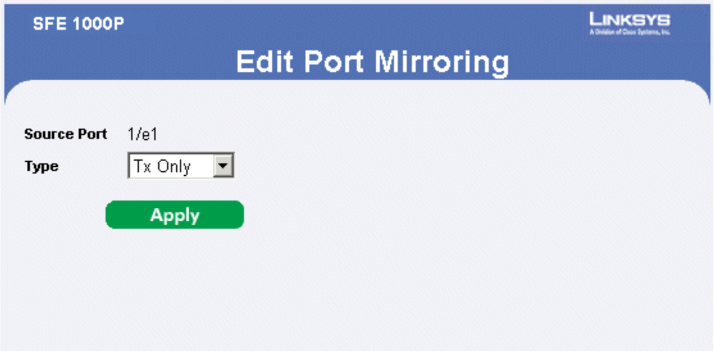
Type: Tx Only

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.

## Modifying Port Mirroring

***Edit Port Mirroring Page***



SFE 1000P

Edit Port Mirroring

Source Port: 1/e1

Type: Tx Only

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

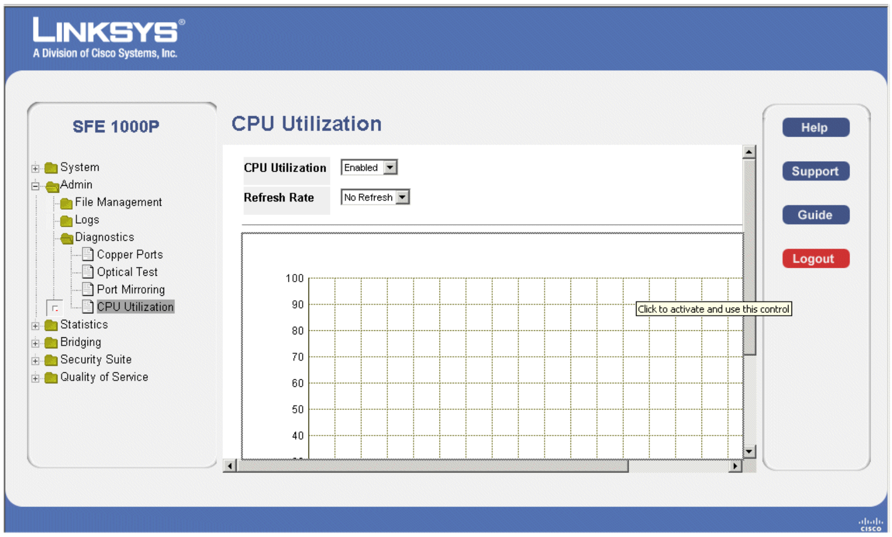
- **Source Port** — Defines the port from which traffic is to be analyzed.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *RxOnly* — Defines the port mirroring on receiving ports. This is the default value.
  - *TxOnly* — Defines the port mirroring on transmitting ports.

– *Tx and Rx*— Defines the port mirroring on both receiving and transmitting ports.

## Defining CPU Utilization

The *CPU Utilization Page* contains information about the system's CPU utilization.

***CPU Utilization Page***



CPU Utilization

CPU Utilization: Enabled

Refresh Rate: No Refresh

Click to activate and use this control

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.
- **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 second intervals, that usage samples are taken.

A Division of Cisco Systems, Inc.

March2008Rev1.0-CH