



SFE1000P 8-port 10/100 Ethernet Switch with PoE Administration Guide March 2008



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

ılıılı cısco. © Copyright 2008, Cisco Systems, Inc.

Specifications are subject to change without notice.

Linksys, the Cisco Systems logo, the Linksys Logo, and the Linksys One logo are registered trademarks of Cisco Systems, Inc. All other trademarks mentioned in this document are the property of their respective owners.

Document Revision History

Revision	Date	Description
1.0	March 2008	Initial release

Chapter 1: Preface	•••	•••	•	•	•	•	•	•	1 1 1 1
Chapter 2: Getting Started Starting the Application Understanding the Interface Device Representation Using the Linksys Management Buttons Using Screen and Table Options Adding Device Information Modifying Device Information Deleting Device Information Resetting the Device Logging Off The Device			•			•		•	3 35 67 77 88 99
Chapter 3: Managing Device Information Understanding the Device Zoom View Defining General System Information Resetting the Device			•	•	•	•	•	•	10 10 11 11
Chapter 4: Managing Power-over-Ethernet Defining PoE Settings	Devices	. .	•	•	•	•	•	•	13 13
Chapter 5: Configuring Device Security Passwords Management Modifying the Local User Settings Defining Authentication Defining Authentication Profiles Modify the Authentication Profile Mapping Authentication Profiles Defining TACACS+ Modifying TACACS+ Settings Defining RADIUS Modifying RADIUS Server Settings Defining Access Method Defining Access Profiles Defining Profile Rules Modifying Profile Rules Defining Traffic Control Defining Storm Control Modifying Storm Control Defining Port Security Modifying Port Security					•	•	•	•	15 17 17 18 19 20 22 22 24 24 24 24 24 24 26 28 29 29 30 30 31

Defining 802.1x Defining Port Authentication Modifying 8021X Security Defining Multiple Hosts Modifying Multiple Host Settings Defining Authenticated Host Defining Access Control Defining MAC Based ACL Adding Rule to MAC Based ACL Defining IP Based ACL Defining IP Based ACL Adding an IP Based Rule Defining ACL Binding Modifying ACL Binding Defining DoS Prevention Global Settings Defining Martian Addresses	32 33 34 35 35 36 36 36 37 38 38 40 40 41 41 42 42
Chapter 6: Configuring Device Interfaces	.44
Defining Port Settings Modifying Port Settings	44 44
Defining LAG Management	45
Defining LAG Settings	47
Contiguring LACP Modify LACP Parameter Settings	49 50
Chapter 7: Configuring VLANs	.51
Defining VLAN Properties	52
Moditying VLANs Defining VLAN Membership	53 53
Modifying VLAN Membership	54
Defining Interface Settings Modifying VLAN Interface Settings	54 55
Configuring GVRP Settings	55
Defining VLAN Protocol Group	57
Modifying Protocol Groups Defining VIAN Protocol Port	58 58
Charter 9. Configuring ID Information	40
Domain Name System	. 60
Defining DNS Server	60
Configuring Layer 2IP Addresses	62 63
Configuring IP Addressing Defining IP Interfaces	63 63

Enabling ARP Modifying ARP Settings	64 65
Chapter 9: Defining Address Tables	. 66 66 67
Chapter 10: Configuring Multicast Forwarding	. 69 70 70 72 72 73
Chapter 11: Configuring Spanning Tree	. 74 75 76 77 78 79 79 80 81 82 83
Chapter 12: Configuring SNMP	. 85 86 87 88 89 90 91 92 93 93 93 93 96 96
Chapter 13: Configuring Quality of Service	. 98 99 100 3

Def	Modifying Interface Priorities Defining Queue Mapping CoS to Queue Mapping DSCP to Queue Configuring Bandwidth ining Advanced Mode Configuring DSCP Mapping Defining Class Mapping Defining Class Mapping Defining Aggregate Policer Modifying QoS Aggregate Policer Configuring Policy Table Modifying the QoS Policy Profile Defining Policy Binding Modifying QoS Policy Binding Settings Defining QoS Basic Mode											100 101 102 103 104 105 106 107 108 107 108 109 110 111 112 112
Chapter File	• 14: Managing System Files . Management Overview File Management Firmware Upgrade Save Configuration Copy Files Active Image	•	•	•	•	•	• •	•	•	•	•	114 115 115 116 117 118
Chapter	• 15: Managing System Logs Enabling System Logs Viewing the Device Memory Logs Clearing Message Logs Viewing the Flash Logs Clearing Message Logs Viewing Remote Logs Modify Syslog Server Settings	•	•	•	•	•		•	•	•	•	<pre>119 119 121 121 122 122 123 124</pre>
Chapter	16: Configuring System Time . Defining System Time Defining SNTP Settings Defining SNTP Authentication	•	•	•	•	•	•••	•	•	•	•	125 125 126 127
Chapter Vie	17: Viewing Statistics wing Ethernet Statistics Defining Ethernet Interface Resetting Interface Statistics Counters Viewing Etherlike Statistics Resetting Etherlike Statistics Counters Viewing GVRP Statistics Resetting GVRP Statistics Counters	•	•	•	•	•	• •	•	•	•	•	128 128 129 129 129 129 130 130

Viewing EAP Statistics13Managing RMON Statistics13Viewing RMON Statistics13Resetting RMON Statistics Counters13Configuring RMON History13Defining RMON History Control13Modify History Control Settings13Viewing the RMON History Table13Configuring RMON Events13Defining RMON Events13Defining RMON Events13Defining RMON Events Control13Defining RMON Events Logs13Defining RMON Alarms13Modify Event Alarms13Defining RMON Alarms13	31 32 32 33 33 33 34 35 35 35 37 37
Chapter 18: Managing Device Diagnostics 14 Viewing Integrated Cable Tests 14 Performing Optical Tests 14 Configuring Port Mirroring 14 Modifying Port Mirroring 14 Defining CPU Utilization 14	40 41 42 43 43
Appendix A: Console Interface Configuration 14 Overview 12 Configuring the HyperTerminal Application 12 Connecting to the SFE1000P through a Telnet Session 12	44 44 47
Appendix B: Contacts	18 48 48
Appendix C: Warranty Information14LIMITED WARRANTY14Exclusions and Limitations14Obtaining Warranty Service15Technical Support15	19 49 49 50 51
Appendix D: Regulatory Information 15 Federal Communications Commission Interference Statement 15 Industry Canada Statement 15 Règlement d'Industry Canada 15 EC Declaration of Conformity (Europe) 15 User Information for Consumer Products Covered by EU Directive 2002/96/EC on 15 Waste Electric and Electronic Equipment (WEEE) 15	52 52 53 53
Appendix E: Environmental Specifications	51

Contents

Appendix F: Safety Information	. 162
Meaning of the Warning Symbol	162
General Safety Information	162
Appendix G: Software License Agreement	. 164
Software in Linksys Products:	164
Software Licenses:	164
Schedule 1 Linksys Software License Agreement	164
Schedule 2	166
Schedule 3	171

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 administration of the SFE1000P, explains how to install 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,"provides information for defining 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," provides information for defining 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 how to configure 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.
- Appendix B, "Contacts," is a listing of support resources and contact information for such.
- Appendix C, "Warranty Information," is the Linksys warranty.

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

The following diagram illustrates how the SFE1000P fits into your network.



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.

To open the User Interface:

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

2

SFE1000P Gigabit Ethernet Switch Administration Guide

Enter Network Password Page

LINKSYS [®] A Division of Cisco Systems, Inc.	
	Password
	Login Clear
	-thats 6960

- 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.
- 4. Click Login The Embedded Web System Home Page opens:



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.

SFE1000P Gigabit Ethernet Switch Administration Guide

2

Embedded Web System Home Page

SFE 1000P 200m System System Management System Information Reset Time P Admin Statistics Bridging Security Suite Quality of Service Image: Comparison of Service	LINKSYS [®] A Division of Cisco Systems, Inc.		
System System Information Reset Domain Name System SNMP Admin Statistics Sindinging Security Suite Quality of Service	SFE 1000P	Zoom	Help
	System System Management Com System Information Reset Time Domain Name System SNMP Admin Statistics Bridging Security Suite Guality of Service	LINKERYS SFE1000P 8-Port 10/100 +2Port Gigabit Switch with WebView and Power over Ethernet Uncourt Pet Uncourt Pet Uncourt Ogabit Net PRR 1 2 3 4 5 5 7 8 01	Support Guide
		4	

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.
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.

SFE1000P Gigabit Ethernet Switch Administration Guide



LINKSYS USER INTERTACE COMPONENT	Linksv	s User	Interface	Com	ponent
----------------------------------	--------	--------	-----------	-----	--------

A Division of Cisco Systems, Inc.	Zoom ³	Help
System System Management System Information Reset Domain Name System SNMP Admin Statistics Bridging Calify of Service	LINKEYS SFE1000P 8-Port 10100 +2-Port Gigabit Switch with WebView and Power over Ethernet UNKACT PIE LINKACT Gigabit LINKACT Gigabit LINKACT Gigabit LINKACT Gigabit t 3 3 6 7 8 CT minicOBC 022-minicOBC 022-mini	Support Guide Logout 4
		-ili-ili- cisco

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

Linksys	SFI	SFE1000P 8-Port 10/100 +2Port Gigabit Sw		Switch wi	h with WebView and Power over Ethernet			Ethernet				
		LINK/ACT	-	_	PeE	LINK/ACT	-	_	PoE I	UNKIACT Gigabit LIK	KIACT Gigabit	
	• •	10000										սիսիս
Ra	INT PWR		2							G1 miniGBIC	G2miniGBIC	cisco

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:

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 settlings of a selected port to the default settings
Test	Test	Performs cable tests immediately.

Device Management Buttons

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. To add information to tables or EWS pages:

- 1. Open an EWS page.
- 2. Click the Add button. An add page opens, for example, the Add SNTP Server Page:

Add SNTP Server

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add SNTP Server	
SNTP Server		
🗌 Enable Poll Interval		
Encryption Key ID		
	Apply	

- 3. Define the fields.
- 4. Click Apply. The configuration information is saved, and the device is updated.

Modifying Device Information

- 1. Open the EWS page.
- 2. Select a table entry.
- 3. Click the Edit Button. A Modify page opens, for example, the Interface Priority Page opens:

- 1. . .

EC	iit I	ntert	ace	Priori	fy

•-

SFE 1000P	LINKSYS [®] A Division of Cisco Systems, Inc.
Edit Interface Priority	
Interface 💿 Port e1 💌 C LAG 1 💌	
Set Default User Priority	
Apply	

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

Deleting Device Information

- 1. Open the EWS page.
- 2. Select a table row.
- 3. Check the Remove checkbox.

4. Click the Delete button. The information is deleted, and the device is updated.

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:

1. Click **System > General > Reset**. The *Reset* page opens.

	Reset Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System Management System Information Reset IP Addressing Domain Name System SNMP Admin Statistics Bridging Security Suite Quality of Service	Reset Reset the device by selecting 'Reset'. Reset	Help Support Guide Logout

- 2. Click the **Reset** button. The device is reset, and a prompt for a user name and password is displayed.
- 3. Enter a user name and password to reconnect to the Web Interface, if the device is not part of a full Linksys One system. If the device is part of a Linksys One system, login is automatically done from the Service Router.

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. To open the Zoom Page:

Click the System > System Management > Zoom. The Zoom Page opens:

SFE 1000P	Zoom LINKSYS SELCOOP 8-Port 10/100 12Port Gigabil Switch with WebView and Power over Ethernet LINKKSY Mar Park 2 3 4 5 6 7 8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	er Guide an mindetter cisco Help Suppo Guide Logou
	4	

Zoom Page

The Zoom Page contains the following port indicators:

• Green - Indicates the port is currently operating.

3

Defining General System Information

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

1. Click the System > System Management > System Information. The System Information Page opens:



SFE 1000P	System Inform	nation Help
🗄 💼 System	Model Name	SFE1000P - 8-port Fast Ethernet Switch with 2 Giga Combo ports, We Support
System Management	System Name	
System Information	System Location	Guide
	System Contact	
	System Object ID	1.3.6.1.4.1.3955.7.4.1000.1
SNMP	System Up Time	O days, 1 hours, 43 minutes, 31 seconds
Admin	Base MAC Address	00:24:c6:26:49:00
E Bridging	Hardware Version	00.00.01
a en Security Suite	Software Version	1.0.0.13
	Boot Version	1.0.0.3
	Apply	

2. Enter information into the appropriate fields and press Apply.

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.

To reset the device:

1. Click System > General > Reset. The Reset page opens.

SFE1000P Gigabit Ethernet Switch Administration Guide



Reset Page

LINKSYS A Division of Cisco Systems, Inc.		
SFE 1000P	Reset	Help
System System Management Doom System Information Preset SNMP Admin Statistics Statistics Statistics Construction Statistics Construction Statistics Construction Statistics Construction Statistics Construction Statistics Construction Statistics	Reset the device by selecting 'Reset'.	Support Guide Logout

- 2. Click the **Reset** button.
- 3. Enter a user name and password to reconnect to the Web Interface. If the device is part of a Linksys One system, login is automatically done from the Service Router.



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

Defining PoE Settings

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%.

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

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

SFE1000P Gigabit Ethernet Switch Administration Guide



PoE Settings Page

SFE 1000P	PoE	Settings					Help
System Admin	Port	Admin Status	Priority	Power Alloction (watts)	Power Consumption (miliwatts)		Support
Bridging	e1	Enable	Low	15400	0	Edit	Guide
Address Tables	e2	Enable	Low	15400	0	Edit	
-en Port Management	e3	Enable	Low	15400	0	Edit	Logout
LAG Management	e4	Enable	Low	15400	0	Edit	
LACP	e5	Enable	Low	15400	0	Edit	
PoE Settings	e6	Enable	Low	15400	0	Edit	
Spanning Tree	e7	Enable	Low	15400	0	Edit	
em Multicast Security Suite Quality of Service	e8	Enable	Low	15400	0	Edit	

2. Click the **Edit** button. The *Edit PoE* opens:

	Edit PoE	Ī	
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Po	1	
Port		e2 💌	
Enable	PoE	V	
Power	Priority Level	Low -	
Power	Consumption	0	
Overlo	ad Counter	0	
Short	Counter	0	
Denied	l Counter	0	
Absen	t Counter	0	
Invalid	Signature Counter	0	
Power	Allocation	15400	
	Apply		

- 3. Define the relevant fields.
- 4. Click Apply. The PoE Settings are defined, and the device is updated.

5

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.

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

SFE1000P Gigabit Ethernet Switch Administration Guide



User Authentication Page.

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	User Authentication	Help
Admin Statistics Bridging Security Suite Passwords Management User Authentication	ews Edit Delete Add	Guide
Authentication Access Method Traffic Control 802.1X Access Control		
Quality of Service		
		ahaha

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

Add Local User Page

SFE 2000P		LINKSYS® A Division of Cisco Systems, Inc.
A	dd Local User	
User Name		
Password		
Confirm Password		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The local user settings are modified.

Modifying the Local User Settings

- Click Security Suite > Passwords Management > User Authentication. The User Authentication Page Opens:
- 2. Click the Edit Button. The Edit Local User Page opens:

Edit Local User Page

SFE 2000P		LINKSYS [®] A Division of Cisco Systems, Inc.
Edi	t Local User	
User Name	ews 🔻	1
Password	•••••	•
Confirm Password	•••••	•
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The local user settings are modified, and the device is updated.

Defining Authentication

The Authentication section contains the following pages:

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

5

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.

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

SFE 1000P System Admin Statistics Bridging Security Suite Passwords Management Authentication Profiles Adthol Trafile Control B02.1X Access Method Trafile Control B02.1X Access Control B02.1X B	SFE 1000P System Admin Statistics Bridging Security Suite Passwords Management Authentication Profiles Taffic Control Bo2 1X Access Method Taffic Control Bo2 1X Access Control DoS Prevention Dass Prevention Conside Feasion	
System Admin Admin Statistics Bridging Security Suite Passwords Management Authentication - Profile Name Methods Console Default Local Edit Network Default Local Edit Network Default Local Edit Delete Add Delete Add Console Default Local Edit Delete Add	 System Admin Statistics Brdging Security Suite Passwords Management Authentication Profile Mame Methods Console Default Local Edit Network Default Local Edit Delete Add 	
Statistics Bridging Security Suite Passwords Management Authentication Profiles Mapping Profiles Authentication Profiles Access Method B02.1X Access Control Do S Prevention Quality of Service	Statistics Statistics Statistics Security Suite Console Default Local Console Default L	ort
Security Suite Passwords Management Authentication Profiles Access Method Trafic Control B02.1X Access Control Dos Prevention Ouslify of Service	Security Suite Passwords Management Authentication Profiles Delete Add Delete Add Correct Society Delete Add Correct Society Delete Correct C	e
Autrentication Profiles Autrentication Mapping Profiles Characters Method Traffic Control 002.1X Access Control Dos Prevention Quality of Service V	Authentication Profiles Mapping Profiles Access Method Traffic Control BS Prevention Construct BS Prevention Cons	ut
Imapping Tollies Traffic Control B02.1X Access Control Dos Prevention Ousling of Service ▼	Access Method Trafic Control DoS Prevention Ore Service	
Access Method Trafic Control B02.1X Access Control Dos Prevention Quality of Service ✓	ADUS ACcess Method Control Bos Prevention Dos Prevention	
Access Control Dos Prevention Quality of Service	Craffic Control B02.1X Access Control DoS Prevention Order of Service	
Access Control	Access Control	
Quality of Service	DoS Prevention	

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

Add Authentication Profile Page

SFE 1000P		A Division of Cisco Systems, Inc.
Ac	ld Authentication	Profile
Profile Name		
Authentication Metho	d	
ptional Methods	Selected Methods	
RADIUS	2	
TACACS+	3	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The settings are modified, and the device is updated.

5

Modify the Authentication Profile

- 1. Click Security Suite > Authentication > Profiles. The Profiles Page opens:
- 2. Click the Edit Button. The Edit Authentication Profile Page opens:

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Authentication Profile	•
Profile Name	Console Default 💌	
	Method Selected Methods	
RADIUS TACACS+ None		
,	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The authentication profile is defined, and the device is updated.

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.

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

SFE1000P Gigabit Ethernet Switch Administration Guide



Mapping Profiles Page

LINKSYS [®] A Division of Cisco Systems, Inc.				
SFE 1000P	Console C Telnet N Secure Telnet (SSH) N Secure HTTP Optional Methods CALACS+ D None D HTTP Optional Methods HTTP Optional Methods RADAS TACACS+ D None D Apply	es console Default ietwork Default iet	-	Help Support Guide Logout
				սիս

- 2. Define the relevant fields.
- 3. Click Apply. Mapping Profiles is defined, and the device is updated.

Defining TACACS+

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

- Authentication Provides authentication during login and via user names and userdefined 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.

To define TACACS+:

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

TACACS+ Page

SFE 1000P	TACACS+			Help
System Admin Statistics Bridging Security Suite Passwords Management	Default Parameters Source IP Address Key String Timeout for Reply	0000 5 C	Sec)	Suppor Guide Logout
Authentication Profiles Mapping Profiles TACACS+ RADIUS Access Method	□ Host IP Address Priority	Source Authentication IP Address Port	Timeout Single for Reply Connection Delete	Status Add
Access Control DoS Prevention Quality of Service	Apply			

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

Add TACACS+ Server Page

SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	Add TACAC	S+ Ser	ver
Host IP Address			
Priority			
Source IP Address		(x.x.x)	🗖 Use Default
Key String			🗖 Use Default
Authentication Port	49		
Timeout for Reply		(sec)	🗖 Use Default
Single Connection			
			Apply

- 3. Add a TACACS+ server.
- 4. Click Apply. The TACACS+ server is added, and the device is updated.

Modifying TACACS+ Settings

- 1. Click Security Management > Security Suite > Authentication. The TACACS+ Page opens:
- 2. Click the Edit Button. The TACACS+ Page opens:

	TACACS+	- Page		
SFE 1000P				LINKSYS [®] A Division of Cisco Systems, Inc.
	TACAC	S+		
Host IP Address	10.6.250.67 💌			
Priority	20			
Source IP Address	Default	(X.X.X)	🗹 Use I	Default
Key String	Default		🗹 Use I	Default
Authentication Port	49			
Timeout for Reply	Default	(sec)	🗹 Use I	Default
Status	Not Connected			
Single Connection				
			Appl	у

- 3. Define the relevant fields.
- 4. Click Apply. The TACACS+ settings are modified, and the device is updated.

Defining RADIUS

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

To define RADIUS:

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

SFE1000P Gigabit Ethernet Switch Administration Guide



RADIUS Page

LINKSYS [®] A Division of Cisco Systems, Inc.								
SFE 1000P	RADIUS						ſ	Help
System Admin Statistics Bridging Security Suite	Default Parameters Default Retries Default Timeout for Reply	3	(Sec)					Support Guide
Passwords Management Authentication Profiles Mapping Profiles TACACS+ RADUS Anagement Mathed	Default Dead Time Default Key String Source IP Address	0	(Min)					Logout
Traffic Control ■ 802.1X ■ Access Control ■ DoS Prevention ■ Quality of Service	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Key Time String Delete	Source IP Address	Us Ty Add	

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

Add Radius Server Page

SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	Add RADI	US 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		
			Apply

- 3. Define the relevant fields.
- 4. Click Apply. The Radius Server is added, and the device is updated.

5

Modifying RADIUS Server Settings

- 1. Click Security Suite > Authentication > RADIUS. The RADIUS Page opens:
- 2. Click the Edit button. The Edit RADIUS Settings Page opens:

Edit RADIUS Settings Page					
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.		
	RADIUS Serv	er Setting	s		
IP Address	192.1.1.120 💌				
Priority	0				
Authentication Port	1812				
Number of Retries	Default	I	🔽 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				
			Apply		

- 3. Define the relevant fields.
- 4. Click Apply. The RADIUS Server settings are modified, and the device is updated.

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

SFE1000P Gigabit Ethernet Switch Administration Guide

- Secure HTTP (HTTPS)
- SNMP

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

To define access profiles:

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

SFE 1000P	Acc	ess Profiles		Help
System Admin Statistics Bridging Security Suite Authentication Access Method Access Method Access Method Traffic Control B02.1X Access Control DoS Prevention Quality of Service		Access Profile Name None Console Only Delete	Current Active Access Profile © Add	Support Guide Logout

Access Profiles Page

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

SFE1000P Gigabit Ethernet Switch Administration Guide



Add Access Profile Page

SFE 1000P		LINKSYS [®] A Division of Clisco Systems, Inc.
	Add Access Profile	
Access Profile Name		
Rule Priority		
Management Method	All	
🗆 Interface	C Port e1 🔽 C LAG 1 🔽 C VLAN 10 🔽	
Source IP Address	Network Mask Prefix Length	
Action	Permit 💌	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The access profile is added, and the device is updated.

Defining Profile Rules

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

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

To define profile rules:

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

Profile Rules Page

SFE 1000P	Pro	ofil	e Rul	es						ſ	Help
System Admin	Acces	ıs Pr	ofile Nam	e Console	Only 💌						Support
Statistics Bridging Security Suite		#	Priority	Interface	Management Method	Source IP Address	Prefix Length	Action			Guide
Passwords Management	-	1	1		All		/32	Deny	Edit		Logout
Access Method							(Delete	A	dd	
Traffic Control											
Access Control											
Quality of Service											

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

Add Profile Rule Page

SFE 1000P	A Di	INKSYS [®] ision of Cisco Systems, Inc.
	Add Profile Rule	
Access Profile Name		
Priority Management Method		
Interface		
Source IP Address	CNetwork Mask	
Action	Permit 💌	Apply

- 3. Define the relevant fields.
- 4. Click Apply. The profile rule settings are added, and the device is updated.

5

Modifying Profile Rules

- 1. Click Security Suite > Access Method > Profile Rules. The Profile Rules Page opens:
- 2. Click the Edit button. The Edit Profile Rule Page opens:

	Edit Profile Rule Page
SFE 1000P	LINKSYS A Division of Gisco Systems, Inc
	Edit Profile Rule
Access Profile Name	AP1
Priority	
Management Method	All
Interface	
Source IP Address	CNetwork Mask
Action	Permit
	Apply

- 3. Define the relevant fields.
- 4. Click Apply. The profile rules are defined, and the device is updated.
5

Defining Traffic Control

The Traffic Control section contains the following pages:

- **Defining Storm Control** ٠
- 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.

To define storm control:

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

SFE 1000P	Sto	rm	Control			Hel
System Admin	Сор	y from	Entry Number	To Entry Numbe	er(s)	(Exam Supp
Statistics	_	Internet				Gui
Security Suite	#	Port	Enable Broadcast Control	Broadcast Rate Threshold	Broadcast Mode	
Passwords Management	1	e1	Enabled	200	Broadcast Only	
Authentication	2	e2	Enabled	200	Broadcast Only	
- Control	3	e3	Enabled	200	Broadcast Only	
Storm Control	4	e4	Enabled	200	Broadcast Only	
- en 802.1X	5	e5	Enabled	200	Broadcast Only	
Access Control DoS Prevention	6	еб	Enabled	200	Broadcast Only	
Quality of Service	7	e7	Enabled	200	Broadcast Only	
	8	e8	Enabled	200	Broadcast Only	
			21100100	200		

1 0

- 2. Define the relevant fields.
- 3. Click Apply. Storm control is enabled, and the device is updated.

Modifying Storm Control

- 1. Click Security Suite > Traffic Control > Storm Control. The Storm Control Page opens:
- 2. Click the Edit Button. The Edit Storm Control Page opens:

	Edit Storm Control Page	
SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Storm Control	
Port	e1 💌	
Enable Broadcast Control		
Broadcast Mode	Broadcast Only	
Broadcast Rate Threshold	200	
	Apply	

- 3. Modify the relevant fields.
- 4. Click Apply. Storm control is modified, and the device is updated.

Defining Port Security

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

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

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



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

Perform the following to define port security:

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

LINKSYS® Division of Cisco Systems, Inc.									
SFE 1000P	Port Se	curity						Help	5
System	Ports	C LAGs						Supp	ort
Statistics Bridging	Interface	Interface Status	Learning Mode	Max Entries	Action	Тгар	Trap Frequency (Sec)	Guid	e
Passwords Management	e1	Unlocked	Classic Lock	1		Disable	10	Logo	ut
Authentication	e2	Unlocked	Classic Lock	1		Disable	10		
Traffic Control	e3	Unlocked	Classic Lock	1		Disable	10		
Storm Control	e4	Unlocked	Classic Lock	1		Disable	10		
- <mark>6</mark> 802.1X	e5	Unlocked	Classic Lock	1		Disable	10		
Access Control DoS Prevention	e6	Unlocked	Classic Lock	1		Disable	10		
Quality of Service	e7	Unlocked	Classic Lock	1		Disable	10		
	e8	Unlocked	Classic Lock	1		Disable	10		
	•								

- 2. Define the relevant fields.
- 3. Click Apply. Port security is defined, and the device is updated.

Modifying Port Security

- 1. Click Security Suite > Traffic Control > Port Security. The Port Security Page opens:
- 2. Click the Edit Button. The Edit Port Security Page opens:

Edit Port Security Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Port Security	
Interface	• Port e1 - C LAG 1-	
Lock Interface		
Learning Mode	Classic Lock 💌	
Max Entries	1	
Action on Violation	Discard	
Enable Trap	Γ	
Trap Frequency	10	
	Apply	

- 3. Modify the relevant fields.
- 4. Click **Apply**. Port security is modified, and the device is updated.

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

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



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

	802.1X Pro	operties Page	
System Admin SFE 1000P System Admin Statistics Site Bridging Security Suite Security Suite Admentation Advectority Suite Advectority Suite Access Method Traffic Control	BO2.1X Pro Properties Port Based Authentication State Authentication Method Guest VLAN Guest VLAN ID Apply	Deater	Help Support Guide Logout
02.1X Properties Port Authentication Multiple Host Access Control DoS Prevention Ouality of Service			ehole
			cisco

- 2. Define the relevant fields.
- 3. Click Apply. The 802.1X properties are defined, and the device is updated.

Defining Port Authentication

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

SFE 1000P	Por	t Au	the	nticatior	ı			ſ	Help
System	Сор	y from E	ntry N	umber		To Entry Number	(s)	(Example: 1,3,	Suppor
Statistics Bridging Security Suite	#	Port N	lser lame	Current Port Control	Guest VLAN	Periodic Reauthentication	Reauthentication Period	Authentica State	Guide
Passwords Management Authentication	1	e1		Authorized	Disable	Disable	3600	Force Auth	Logout
Access Method	2	e2		*	Disable	Disable	3600	Initialize	
-en Iraffic Control -en 802.1X	з	e3		*	Disable	Disable	3600	Initialize	
Properties	4	e4		Authorized	Disable	Disable	3600	Force Auth	
- Multiple Host	5	e5		•	Disable	Disable	3600	Initialize	
Authenticated Host	6	e6		Authorized	Disable	Disable	3600	Force Auth	
DoS Prevention	7	e7		•	Disable	Disable	3600	Initialize	

802 1X Port Authentication Page

- 2. Define the relevant fields.
- 3. Click Apply. The port authentication settings are modified, and the device is updated.

5

Modifying 8021X Security

- 1. Click Security Suite > 802.1X > Properties. The 802.1X Properties Page opens:
- 2. Click the Edit button. The Port Authentication Settings Page opens:

Port Aut	hentication Settings Page	;
SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
Port Author	entication 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	
	Apply	

- 3. Modify the relevant fields.
- 4. Click Apply. The port authentication settings are defined, and the device is updated.

Defining Multiple Hosts

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

1. Click Security Suite > 802.1X > Multiple Host. The 802.1X Multiple Host Page opens:

SFE 1000P	Mu	ltiple Hos	t					Hel
💼 System 💼 Admin	Po	rt Multiple Hosts	Action on Violation	Traps	Trap Frequency	Status	Number of Violations	Supp
Statistics	e1	Single	Discard	Disable	10	Not in auto mode	0	Guid
Bridging	e2	Single	Discard	Disable	10	Not in auto mode*	0	
Passwords Management	e3	Single	Discard	Disable	10	Not in auto mode*	0	
Access Method	e4	Single	Discard	Disable	10	Not in auto mode	0	
-en Iraffic Control	e5	Single	Discard	Disable	10	Not in auto mode*	0	
Properties	e6	Single	Discard	Disable	10	Not in auto mode	0	ā
Multiple Host	e7	Single	Discard	Disable	10	Not in auto mode*	0	
Authenticated Host	e8	Single	Discard	Disable	10	Not in auto mode*	0	
DoS Prevention	e1	Single	Discard	Disable	10	Not in auto mode*	0	

802.1X Multiple Host Page

- 2. Define the relevant fields.
- 3. Click Apply. The host settings are modified, and the device is updated.

Modifying Multiple Host Settings

- 1. Click Security Suite > 802.1X > Multiple Host. The 802.1X Properties Page opens:
- 2. Click the Edit button. The Edit Multiple Host Page opens:

Edit Multiple Host Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Multiple Hosts	
Port	e3 💌	
Enable Multiple Hosts		
Action on Violation	Discard 🔽	
Enable Traps		
Trap Frequency	10	
	Apply	

- 3. Modify the relevant fields.
- 4. Click Apply. The multiple host settings are defined, and the device is updated.

5

Defining Authenticated Host

The Authenticated Host Page contains a list of authenticated users.

1. Click Security Suite > 802.1X > Authenticated Host. The Authenticated Host Page opens:

INKSYS ® Division of Cisco Systems, Inc.						
SFE 1000P	Authent	icat	ed Host			Help
En System	User Name	Port	Session Time	Authentication Method	MAC Address	Suppd
Admin 🔤		e1	248	Remote	00000000000	
Statistics		e2	0	Remote	00000000000	Guide
Bridging Security Suite		еЗ	0	Remote	00000000000	- Culture
Passwords Management		e4	- 248	Remote	00000000000	Logou
Authentication		e5	0	Remote		Logoa
Access Method		e6	248	Remote		
Traffic Control		.7	240	Remote	000000000000	
Pronerties		-9	0	Remote	00000000000	
Port Authentication		~1	0	Remote	00000000000	
- Multiple Host		gi	0	Remote	00000000000	
Authenticated Host		g∠	U	Remote	0000000000	
- Access Control						
Quality of Service						

- 2. Define the relevant fields.
- 3. Click Apply. The authenticated host settings are defined, and the device is updated.

Defining Access Control

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

The Access Control section contains the following pages:

- Defining MAC Based ACL ٠
- 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.

To define the MAC Based ACL:

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

INKSYS [®] Ision of Cisco Systems, Inc.								
SFE 1000P	MAC Base	d ACL						Help
System Admin Statistics Bridging Security Suite Passwords Management Authentication	ACL Name	Source MAC Address Mask	Destination MAC Address Mask	VLAN ID	CoS	Cos Mask	Eth	Guide Logout
Access Method Traffic Control 802.1X Access Control MAC Based ACL ACL Binding DoS Prevention						Delete Ri	ule ACL	
Quality of Service	4				1			

2. Click the Add ACL button. The Add MAC Based ACL Page opens:

Add MAC Based ACL Page

SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	Add MA	C Based ACL	
ACL Name			
New Rule Priority			
Source MAC Address	0	Wild Card Mask	C Any
Dest. MAC Address	0	Wild Card Mask	C Any
VLAN ID		I	
CoS			
CoS Mask			
Ether Type			
Action	Permit		
			Apply

- 3. Define the relevant fields.
- 4. Click Apply. The MAC Based ACL is defined, and the device is updated.

5

Adding Rule to MAC Based ACL

- 1. Select an existing ACL.
- 2. Click the Add Rule button. The Add MAC Based Rule Page opens:

	Add MAC Bus	a Role i age	
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	Add MAC	Based Rule	
ACL Name New Rule Priority Source MAC Address Dest. MAC Address VLAN ID CoS CoS Mask Ether Type Action	New ACL	Wild Card Mask	C Any C Any
			Apply

Add MAC Based Rule Page

- 3. Define the relevant fields.
- 4. Click Apply. The ACL Rule is defined, and the device is updated.

Defining IP Based ACL

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

SFE1000P Gigabit Ethernet Switch Administration Guide



Chapter

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

IP Based ACL Page

SFE 1000P	IP Ba	ased A	ACL								ſ	Help
System Admin Statistics Bridging Security Suite	ACL N	ame 🔽] nt the flag	types i	n the fo	llowing	order:	Urg, Ack, Ps	h, Rst, S	Syn, Fin. Set	is rep	Support Guide
-en Passwords Management		Rule Priority	Protocol	Flag	ICMP Type	ICMP Code	IGMP Type	Source		Destination		Logout
Access Method Traffic Control PD2 1V		Thomy		500	Type	Couc	1340	IP Address	Mask	IP Address	Mas	
Access Control											_	
CL Binding DoS Prevention Quality of Service												
	•										- FI	

2. Click the Add Button. The Add IP Based ACL Page opens:

Add IP Based ACL Page

SFE 1000P	
	Add IP Based ACL
ACL Name	
New Rule Priority 🗖	
Protocol	C Select from List CMP
Source Port	C C Any
Destination Port	C C Any
TCP Flags	🗖 Urg Set 🔽 Ack Set 🔽 Psh Set 🔽 Rst Set 🔽 Syn Set 🔽 Fin
ісмр 🗐	C Select from List Echo-Reply 🔽 C ICMP Type 🛛 C Any
ICMP Code	
IGMP 🗖	Select from List DVMRP GIGMP Type 19 CAny
Source IP Address	C C Any Wild Card Mask C C Any
Dest. IP Address	C C Any Wild Card Mask C C Any
Match DSCP	e
Match IP Precedence	e
Action	Permit 💌
Apply	

- 3. Define the relevant fields,
- 4. Click Apply. The IP Based ACL is defined, and the device is updated.

Adding an IP Based Rule

- 1. Click Security Suite > Access Control > IP Based ACL. The IP Based ACL Page opens:
- 2. Click the Add ACL Rule button. The Add IP Based Rule Page opens:

	5
SFE 1000P	LINKSYS" A Division of Cisco Systems, Inc.
	Add IP Based Rule
ACL Name	ip1
New Rule Priority	
Protocol	Select from List ICMP Protocol ID 1
Source Port	C Any
Destination Port	C Any
TCP Flags	🗖 Urg Set 🔽 Ack Set 🔽 Psh Set 🔽 Rst Set 💟 Syn Set 💟
ісмр 🗖	Select from List Echo-Reply
ICMP Code 🗖	
IGMP 🗖	Select from List DVMRP GIGMP Type 19 CAny
Source IP Address	C C Any Wild Card Mask C C Any
Dest. IP Address	C C Any Wild Card Mask C C Any
Match DSCP	©
Match IP Precedence	с
Action	Permit
Apply	

Add IP Based Rule Page

- 3. Select either Match DSCP or Match IP.
- 4. Click Apply. The IP based rule settings are modified, and the device is updated.

Defining ACL Binding

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



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

_INKSYS ® Division of Cisco Systems, Inc.				
SFE 1000P	ACL I	Binding		Help
💼 System 🎦 Admin	Copy fr	om Entry Number	To Entry Number(s)	(Example: 1,3,5 Support
 Statistics Bridging Security Suite 	• Por	ts ⊂ LAGs		Guide
Passwords Management	□ #	Interface ACL Name		Logout
Authentication Access Method	□ 1	e1	Edit	
- Traffic Control	□ 2	e2	Edit	
Access Control	□ 3	e3	Edit	
MAC Based ACL	□ 4	e4	Edit	
ACL Binding	D 5	e5	Edit	
end DoS Prevention DoS Prevention	□ 6	e6	Edit	
	7	e7	Edit	
	•			

- 2. Define the relevant fields.
- 3. Click **Apply**. The ACL binding settings are modified, and the device is updated.

Modifying ACL Binding

- 1. Click Security Suite > Access Control > ACL Binding. The ACL Binding Page opens:
- 2. Click the Edit button. The Edit ACL Binding Page opens:

Edit ACL Binding Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Edit ACL Binding	
Interface	• Port 2 C LAG 1	
Select ACL	None	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. ACL binding is defined, and the device is updated.

Defining DoS Prevention

The DoS Prevention section contains the following pages:

- Global Settings
- Defining Martian Addresses



Global Settings

1. Click Security Suite > Dos Prevention > Global Settings. The Global Settings Page opens:

|--|

LINKSYS [®] A Division of Cisco Systems, Inc.				
SFE 1000P	Global Settings		ſ	Help
System Statistics Statistics Statistics Security Suite Passwords Management Access Method Traffic Control Os Prevention Os Prevention Matian Addresses Ouality of Senice	Security Suite Status Denial of Service Protection Stacheldraht Distribution Invasor Trojan Back Orifice Trojan Apply	Disabled		Support Guide Logout

- 2. Define the relevant fields.
- 3. Click Apply. The Dos prevention global settings are defined, and the device is updated.

Defining Martian Addresses

 Click Security Suite > Dos Prevention > Martian Addresses. The Martian Addresses Page opens:

Iresses	Help
Mask Delete Add	Support Guide Logout
	Iresses Mask Delete Add

2. Click the Add button. The Add Martian Addresses Page opens:

Add Martian Addresses Page

SFE 1000P		LINKSYS A Division of Cisco Systems, Inc.
	Add Martian Addresse	s
Include Reserved Martian Addresses		
IP Address	C Select from Known Martian Addresses 10.0.0.0/8 💆 🤄 Ne	w IP Address
• Mask		
C Prefix Length		
		Apply

- 3. Define the relevant fields.
- 4. Click Apply. The martian addresses are added, and the device is updated.

6

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.

To define port settings:

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

LINKSYS® Division of Cisco Systems, Inc.											
SFE 1000P	Pol	rt Setti	ngs							ſ	Help
💼 System 🎦 Admin	Cop	y From En	ry Number	Τα	Entry N	umber(s)			(Example: 1,3,5-8)		Support
Estatistics →Bridging → Address Tables	#	Interface	Port Type	Port Status	Port Speed	Duplex Mode	PVE	LAG			Guide
Port Management	1	e1	100M-copper	Up	100M	Full			Edit		Logout
	2	e2	100M-copper	Down					Edit		
	3	e3	100M-copper	Down					Edit		
PoE Settings	4	e4	100M-copper	Down					Edit		
-en Spanning Tree	5	e5	100M-copper	Down					Edit		
Le Multicast	6	e6	100M-copper	Down					Edit		
Quality of Service	7	e7	100M-copper	Down					Edit		
	8	8	100M.conner	Down					Edit	1	

- 2. Define the relevant fields.
- 3. Click Apply. Port Settings are defined, and the device is updated.

Modifying Port Settings

- 1. Click Bridging > Port Management > Port Settings. The Port Settings Page opens:
- 2. Click the Edit button. The Edit Port Settings Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



SFE 1000P	LINKSYS® A Division of Cisco Systems, Inc.
	Edit Port
Port	e1 💌
Description	
Port Type	100M-copper
Admin Status	Up
Current Port Status	Up
Reactivate Suspended Port	Г
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	

Edit Port Settings Page

- 3. Define the relevant fields.
- 4. Click Apply. The Port Settings are modified, and the device is updated.

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.

6

SFE1000P Gigabit Ethernet Switch Administration Guide

- 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.

To define LAG management:

1. Click Bridging > Port Management > LAG Management. The LAG Management Page opens:

SFE 1000P	LAG	Management		Help
💼 System	LAG	Name Link State	Member	Support
💼 Admin	LAG 1	Link Not Presen	Edit	
Statistics	LAG 2	Link Not Procom	Edit	Guide
Address Tables	LAG 2	LINK NOL PRESEN	Edil	
en Port Management	LAG 3	Link Not Presen	Edit	Logout
Port Settings	LAG 4	Link Not Presen	Edit	
LAG Management	LAG 5	Link Not Presen	Edit	
	LAG 6	Link Not Presen	Edit	
	LAG 7	Link Not Presen	Edit	
Spanning Tree	LAG 8	Link Not Presen	Edit	
Security Suite	Bold	- Active		
Quality of Service	Grayed	- Passive		

- 2. Define the relevant fields.
- 3. Click Apply. LAG Management is defined, and the device is updated.

LAG Management Page

Modifying LAG Membership

- 1. Click Bridging > Port Management > LAG Management. The LAG Management Page opens:
- 2. Click the Edit button. The Edit LAG Membership Page opens:

Eall LAG Membership Fage	
SFE 1000P	LINKSYS [®] A Division of Cisco Systems, Inc.
Edit LAG Membership	
LAG 1 💌	
LAG Name	
LACP	
Port List Lag Members	

Edit LAG Membership Page

- 3. Define the relevant fields.
- 4. To assign ports to a LAG, click the port numbers in the Port List and then click the Right Arrow button. The port number then appears in the LAG Members list.

Conversely, to remove a port from a LAG, click the port number in the LAG Members list and then click the Left Arrow button.

5. Click Apply. The LAG membership is defined, and the device is updated.

Defining LAG Settings

Link Aggregated Groups optimize port usage by linking a group of ports together to form a single aggregated group. Link aggregated groups multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

The LAG Settings Page contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and eight LAGs per system.

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

SFE 1000P	LAG	Settings	\$						Help
System Admin	Copy Fr	om Entry Nun	nber 🗌		To E	Entry Number(s)	(Example: 1	Suppor
Bridging Address Tables	LAG	Description	Туре	Status	Speed	Auto Negotiation	Flow Control	VE	Guide
-en Port Management Port Settings	LAG 1		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	Logout
LAG Management	LAG 2		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
LACP	LAG 3		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
PoE Settings	LAG 4		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
Spanning Tree	LAG 5		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
em Multicast Security Suite	LAG 6		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
Quality of Service	LAG 7		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	
	LAG 8		Unknown	Unknown	Unknown	Unknown	Unknown	Edit	

LAG Settings Page

2. Click the Edit button. The LAG Configuration Settings opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



LAG Configuration Settings	LAG	Configu	vration	Settings
----------------------------	-----	---------	---------	----------

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	LAG Configuration Settings	
	Ī	
LAG	1 -	
Description		
LAG Type		
Admin Status	Up 🔽	
Current LAG Status		
Reactivate Suspended LAG	F	
Operational Status	Active	
Admin Auto Negotiation	Enable 🔽	
Current Auto Negotiation		
Admin Advertisement	🗹 Max Capability 📕 10 Full 📕 100 Full 📕 1000 Full	
Current Advertisement	Unknown	
Neighbor Advertisement	Unknown	
Admin Speed	10M 🗾	
Current LAG Speed		
Admin Flow Control	Disable 💌	
Current Flow Control		
PVE	None 💌	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The LAG configuration settings are modified, and the device is updated.

Configuring LACP

Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

Aggregated Links can be manually setup or automatically established by enabling Link Aggregation Control Protocol (LACP) on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.



To define LACP:

1. Click Bridging > Port Managing > LACP. The LACP Page opens:

INKSYS [®] Ision of Cisco Systems, Inc.						
SFE 1000P	LAC	Р			ſ	Help
System Admin	LACP	System Priorit	y 1		-	Support
Statistics Bridging	Port	Port Priority	LACP Timeout			Guide
Address Tables	e1	1	Long	Edit		-
Port Settings	e2	1	Long	Edit		Logout
LAG Management	e3	1	Long	Edit		
	e4	1	Long	Edit		
VLAN Management	e5	1	Long	Edit		
Spanning Tree	e6	1	Long	Edit		
Security Suite	e7	1	Long	Edit		
Quality of Service	e8	1	Long	Edit		
	- n1	1	Long	Edit	-	

LACP Page

- 2. Define the relevant fields.
- 3. Click **Apply**. The LACP settings are modified, and the device is updated.

Modify LACP Parameter Settings

- 1. Click Bridging > Port Managing > LACP. The LACP Page opens:
- 2. Click the Edit button. The Edit LACP Page opens:

Edit LACP Page							
SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.					
L	ACP Parameters Settings						
Port	e3 🗸						
LACP Port Priority	1						
LACP Timeout	Long 💌						
	Apply						

- 3. Define the relevant fields.
- 4. Click Apply. The LACP Parameters settings are defined, and the device is updated.



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.

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

Properties Page

SFE 1000P	Pro	ope	rties					Help
System		Г	VIAN	Type	Authentication]	Support
Statistics		-	ID Nar	ne				Guide
Address Tables			10	Static	Enabled	Edit		
Port Management		Π	100	Default	Enabled	Edit		Logout
Membership					Delete	Add		
GVRP Setting							_	
Protocol Group								
E Spanning Tree								
Le Multicast								
Quality of Service	-							

2. Click the Add button. The Add VLAN Page opens:

Add VLAN Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add VLAN	
VLAN ID		
VLAN Name		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The add VLAN settings are modified, and the device is updated.

Modifying VLANs

- 1. Click Bridging > VLAN Management > Properties. The Properties Page opens.
- 2. Click Edit. The Edit VLAN Page opens:

	Edi	t VLAN Page	
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
Au	thenticatio	on VLAN Settir	igs
VLAN ID	10		1
VLAN Name			
Disable Authenticati	on 🗖		
		Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The VLAN Settings are defined, and the device is updated.

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.

1. Click Bridging > VLAN Management > Membership. The VLAN Membership Page opens:

LINKSYS® A Division of Cisco Systems, Inc.		
SFE 1000P	Membership	Help
a- <mark>en</mark> System a- <mark>en</mark> Admin a- <mark>en</mark> Statistics a-en <mark>en</mark> Bridging	VLAN ID TOO Y VLAN Name VLAN Type Defaut	Support
Address Tables Port Management VLAN Management OTProperties	ି Ports ି LAGs	Logout
	Interface Interface Status	
- GVRP Settings	e1 Untagged Edit	
Protocol Group	e2 Untagged Edit	
Spanning Tree	e3 Untagged Edit	
Multicast	e4 Untagged Edit	
Security Suite	e5 Untagged Edit	
	e Untergrad Edit	_

1 ·

- 2. Define the relevant fields.
- 3. Click **Apply**. VLAN membership is defined, and the device is updated.

Modifying VLAN Membership

- 1. Click Bridging > VLAN Management > Membership. The VLAN Membership Page opens:
- 2. Click the Edit button. The Edit VLAN Membership Page opens:

Ea	lit	VLAN	Meml	bersl	hip	Page
----	-----	------	------	-------	-----	------

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit VLAN Membership	
VLAN ID	100	
VLAN Name		
Interface	e4	
Interface Status	Untagged 🗾	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. VLAN Membership is modified, and the device is updated.

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.

 Click Bridging > VLAN Management > Interface Setting. The VLAN Interface Setting Page opens:

LINKSYS [®] Division of Cisco Systems, Inc.							
	Interfec	e Cattin					
SFE 1000P	mena	e Setti	iy				lelp
System	Ports	C LAGs				Î Su	pport
	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering		uide
Address Tables	e1	Trunk	100	Admit All	Enable	Edit	
- Ent Management	e2	Trunk	100	Admit All	Enable	Edit	gout
Properties	e3	Trunk	100	Admit All	Enable	Edit	
- Interface Setting	e4	Trunk	100	Admit All	Enable	Edit	
GVRP Settings	e5	Trunk	100	Admit All	Enable	Edit	
Protocol Port	еб	Trunk	100	Admit All	Enable	Edit	
- en Spanning Tree	e7	Trunk	100	Admit All	Enable	Edit	
Security Suite	e8	Trunk	100	Admit All	Enable	Edit	
Guailty of SerVice	g1	Trunk	100	Admit All	Enable	Edit	

2. Define the relevant fields.

3. Click **Apply**. The VLAN Interface Settings are defined, and the device is updated.

Modifying VLAN Interface Settings

- 1. Click **Bridging** > **VLAN Management** > **Interface Setting**. The VLAN *Interface Setting Page* opens:
- 2. Click the Edit button. The Edit Ports Page opens:

		Edit Ports Page	
	SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
		Edit Ports	
1	Interface	e4 v	
1	VLAN Mode	Trunk	
1	PVID	100	
	Frame Type	Admit All	
I	Ingress Filtering	Enable 💌	
		Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The VLAN Interface settings are modified, and the device is updated.

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.



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

To define GVRP:

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

GVRP Settings Page

SEE 1000P	GV	RP Se	ttinas				Holp	
System	GVI	RP Global S	Status Disable					
Admin							ouppo	
Bidaina							Guide	
Address Tables	Cop	y From En	ry Number	To Entry N	umber(s)	(Example: 1,3,5	-8)	_
Port Management	-						Logou	
VLAN Management	۰	Ports C I	.AGs					
) Membership) Interface Setting	#	Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration			
GVRP Settings	1	e1	Disabled	Enabled	Enabled	Edit		
Protocol Group	2	e2	Disabled	Enabled	Enabled	Edit		
Protocol Port	3	e3	Disabled	Enabled	Enabled	Edit		
Spanning Tree			N: 11 1	Enabled	Enchlad	Ealit		
Spanning Tree Multicast	4	e4	Disabled	Lilabieu	Lilableu	Euli		

- 2. Define the relevant fields.
- 3. Click Apply. The GVRP Settings are defined, and the device is updated.

Modifying GVRP Settings

- 1. Click Bridging > VLAN Management > GVRP Settings. The GVRP Settings Page opens:
- 2. Click the Edit button. The Edit GVRP Page opens:

	Edit GVRP Page	
SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit GVRP	
Interface	Port e2 C LAG 1	
GVRP State	Disable 💌	
Dynamic VLAN Creation	Enable 💌	
GVRP Registration	Enable 💌	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. GVRP settings are modified, and the device is updated.

7

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.

1. Click Bridging > VLAN Management > Protocol Group. The Protocol Group Page opens:

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Protocol Group Protocol Value Group ID (Hex) Delete Add	Help Support Guide Logout
Multicast Security Suite Quality of Service	_	

2. Click the Add Button. The Add Protocol Group Page opens:

Add Protocol Group Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add Protocol Group	
Protocol Value	 Protocol Value IP _ ▲ C Ethernet-Based Protocol Value 	(Hex Format)
Group ID (1-2147483647)	1	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The Protocol Group is added, and the device is updated.

Modifying Protocol Groups

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

- 1. Click Bridging > VLAN Management > Protocol Group. The Protocol Group Page opens:
- 2. Click the Edit Button. The Protocol Group Settings Page opens:

Protocol Group Settings Page				
SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.		
	Protocol Group Settings			
Protocol Value Group ID (Hex)	0800			
•	Apply			

- 3. Define the relevant fields.
- 4. Click Apply. The Protocol group is modified, and the device is updated.

Defining VLAN Protocol Port

The Protocol Port Page adds interfaces to Protocol groups.

To define the protocol port:

1. Click Bridging > VLAN Management > Protocol Port. The Protocol Port Page opens:

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System Admin Statistics Bridging Address Tables Port Management VLAN Management VLAN Management VLAN Management Properties Membership Interface Setting CVRP Settings Protocol Group Protocol Port Spanning Tree Multicast Security Suite Cuality of Service	Protocol Port	Help Support Guide Logout

Protocol Port Page

2. Click the Add Button. The Add Protocol Port to VLAN Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



Add Protocol Port to VLAN Page



- 3. Define the relevant fields.
- 4. Click Apply. The protocol ports are mapped to VLANs, and the device is updated.

Configuring IP Information

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

- 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.

To enable a DNS client:

 Click System > System Management > Domain Name System > DNS Servers. The DNS Servers Page opens:

	DNS Servers Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System System Management System Information Reset Drain Name System Host Mapping SNMP Statistics Bridging Statistics Country Suite Country Suite Country Suite	DNS Servers	Help Support Guide Logout

2. Click the Add button. The Add DNS Server Page opens:

Add DNS Server Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add DNS Server	
DNS Server		
DNS Server Currently Acti	ve 10.4.5.110	
Set DNS Server Active		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The DNS server is added, and the device is updated.

Mapping DNS Hosts

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

 Click System > System Management > Domain Name System > Host Mapping. The Host Mapping Page opens:

. . .

	Host Mapping Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System System System Management System Information Reset Imme P Addressing NNS Servers NNMP Admin Statistics Bridging Security Suite Duality of Service	Host Mapping Host Names IP Address Delete Add	Help Support Guide Logout

2. Click the Add button. The Add DNS Host Page opens:

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

Add DNS Host Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add DNS Host	
Host Name		
IP Address		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The DNS Host settings are defined, and the device is updated.

Configuring Layer 2IP 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:

- Configuring IP Addressing
- Defining IP Routing

Configuring IP Addressing

The IP Addressing subsection contains the following pages:

- Defining IP Interfaces
- 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.

 Click System > System Management > IP Addressing > IP Interface. The IP Interface Page opens:

IP Interface Page		
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	IP Interface	Help
Svstem	Get Dynamic IP from DHCP Server	× Support
System Management 	C Static IP Address	Support
	Management VLAN 100 💌	Guide
	IP Address 10.6.25.67	
P Addressing	© Network mask 255.255.255.224	Logout
Printace Printace	C Prefix Length 727	
	User Defined Default Gateway	
	Active Default Gateway 10.6.25.65	
	Remove User Defined	
	Apply	

- 2. Define the relevant fields.
- 3. Click Apply. The IP Interface settings are modified, and the device is updated.



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.

To define ARP:

1. Click System > System Management > IP Addressing > ARP. The ARP Page opens:

	APD	
System System Management System Information System Information Freset Fride Domain Name System Statistics Bridging Security Suite Quality of Service	ARP Entry Age Out 00000 (Sec) Clear ARP Table Entries None Clear ARP Table Entries View Clear ARP Table Entries View Clear ARP Table Entries Clear AR	Support Guide Logout

2. Click on the Add ARP button. The Add ARP Page opens:

Add ARP Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add ARP	
Interface	VLAN 10 VLAN	
IP Address	0.0.0.0	
MAC Address		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The ARP Settings are defined, and the device is updated.
8

Modifying ARP Settings

- 1. Click System > System Management > IP Addressing > ARP. The ARP Page opens:
- 2. Click the Edit button. The Edit ARP Page opens:

	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 💌	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The ARP Settings are modified, and the device is updated.

Defining Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frames source address. Frames addressed to a destination MAC address that is not associated with any port, are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

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

- Defining Static Addresses
- Defining Dynamic Addresses

Defining Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and cannot be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

To define static addresses:

1. Click Bridging > Address Tables > Static. The Static Page opens:

A Division of Cisco Systems, Inc.	Static	
System Admin Statistics Admine Statistic Dynamic Oynamic Oynamic Oynamic Oynamic Oynamic Oynamic Multicast Security Suite Ouldity of Service	VLAN ID MAC Address Interface Status Delete Add	Support Guide Logout

2. Click the Add button. The Add Static MAC Address Page opens:

Static Page

SFE1000P Gigabit Ethernet Switch Administration Guide



Add Static MAC Address Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Add Static MAC Address	
Interface	• Port e1 - O LAG 1 -	
MAC Address		
💿 VLAN ID	10 💌	
C VLAN Name		
Status	Permanent	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The Static MAC Address is added, and the device is updated.

Defining Dynamic Addresses

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

The Dynamic Page contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.



1. Click Bridging > Address Tables > Dynamic. The Dynamic Page opens:

	Dynamic Page	
Linksys		
A Division of Cisco Systems, Inc.		
SFE 1000P	Dynamic	Help
😐 💼 System	Aning Interval 300 (See)	Support
in — Admin In — Statistics In — Bridging	Clear Table	Guide
Address Tables	Query by:	Logout
en Port Management en VLAN Management	Interface	
en Spanning Tree	MAC Address	
B ecurity Suite B envice	Address Table Sort Key	
	Query	
	VLAN ID MAC Interface	
	VLAN 100 00005e00011b e1	
	VLAN 100 000d562f43a0 e1	
	VLAN 100 0012223341aa e1	
	VLAN 100 00a1b00bdceb e1	-

- 2. Define the relevant fields.
- 3. Click **Query**. The Dynamic MAC Address Table is queried, and the results are displayed.
- 4. Click Apply. Dynamic addressing is defined, and the device is updated.

SFE1000P Gigabit Ethernet Switch Administration Guide



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.

To enable IGMP Snooping:

1. Click Bridging > Multicast > IGMP Snooping. The IGMP Snooping Page opens:

Nivision of Cisco Systems, Inc.	_						
SFE 1000P	IGMP \$	Snoopi	ng				Help
System Admin	Enable IG	MP Snoopir	ng Status				Support
Statistics Bridging Address Tables	VLAN ID	IGMP Snooping Status	Host Timeout	MRouter Timeout	Leave Timeout		Guide
VLAN Management	10	Disabled	260	300	10	Edit	Logout
Spanning Tree Multicast Multicast Multicast Group Forward Security Suite Quality of Service	100 Apply	Disabled	260	300	10	Edit	
adding of Deriver	,						

2. Define the relevant fields.

3. Click Apply. The IGMP Global Parameters are updated, and the device is updated.



Modifying IGMP Snooping

- 1. Click Bridging > Multicast > ICMP Snooping. The IGMP Snooping Page opens:
- 2. Click the Edit button. The Edit IGMP Snooping Page:

Edit IGMP Snooping Page

	SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
		Edit IGMP Snooping	
(
	VLAN ID	10 💌	
	IGMP Status Enable	Disable 💌	
	Auto-Learn	Enable 💌	
	Host Timeout	260	
	MRouter Timeout	300	
	Leave Timeout	₢ 10 ○ Immediate Leave	
		Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The IGMP Global Parameters are modified, and the device is updated.

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.

To define Multicast groups:

1. Click Bridging > Multicast> Multicast Groups. The Multicast Group Page opens:

LINKSYS [®] Division of Cisco Systems, Inc.		
SFE 1000P	Multicast Group	Help
System Admin Statistics Bridging Address Tables Port Management Spanning Tree Multicast Source Forward Forward Security Suite Quality of Service	Enable Bridge Multicast Filtering	Support Guide Logout

Multicast Group Page

2. Click the Add button. The Add Multicast Group Page opens:

Add Multicast Group Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add Multicast Group	
VLAN ID	100 💌	
Bridge IP Multicast		
Bridge Mac Multicast		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The Multicast Group settings are modified, and the device is updated.

Modifying a Multicast Group

- 1. Click Bridging > Bridge Multicast> Multicast Groups. The Multicast Group Page opens:
- 2. Click the Edit button. The Edit Multicast Group Page opens.

Edit Multicast Group Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Multicast Group	
	in the second	
VLAN ID	100	
Bridge IP Multicast	224-239.138 10.1.107	
Bridge Mac Multicast	01005e0a016b	
Interface	e2	
Interface Status	Excluded 💌	
	Apply	

- 3. Define the Multicast Group Port Settings.
- 4. Click Apply. The Multicast group parameters are saved, and the device is updated.

Defining Multicast Forwarding

The *Multicast Forward Page* contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

To define Multicast forward settings:

1. Click Bridging > Multicast > Forward. The Multicast Forward Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



Multicast Forward Page

LINKSYS [®] A Division of Cisco Systems, Inc.						
SFE 1000P	Forwar	'd 10 ▼		_		Help
🖨 🍓 Bridging Maddress Tables	Ports	C LAGs				Guide
Port Management OtLAN Management Spanning Tree	Interface e1	Interface Status Excluded	Edit			Logout
Multicast	e2	Excluded	Edit			
	e3	Excluded	Edit			
Forward	e4	Excluded	Edit			
Quality of Service	e5	Excluded	Edit		-]
	e6	Excluded	Edit			
	e7	Excluded	Edit			
	Ŷ				-	
						-dialia cisco

- 2. Define the relevant fields.
- 3. Click Apply. The multicast forward all settings are defined, and the device is updated.

Modifying Multicast Forwarding

- 1. Click Bridging > Multicast > Forward. The Multicast Forward Page opens:
- 2. Click the Edit button. The Edit Multicast Forward All Page opens:

Edit Multicast Forward All Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit Multicast Forward All	
VLAN ID	10	
Interface	e2	
Interface Status	Excluded •	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The multicast forward all settings are defined, and the device is updated.

Configuring Spanning Tree

The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following Spanning Tree versions:

- Classic STP Provides a single path between end stations, avoiding and eliminating loops.
- **Rapid STP** Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
- Multiple STP Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge.
- 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.

1. Click Bridging > Spanning Tree > Properties. The STP Properties Page opens:

STP Properties Page

Division of Cisco Systems, Inc.					
SFE 1000P	Properties				Help
System	Global Settings				Support
Statistics	Spanning Tree Stat	e Enab	le 💌		Outlete
Bridging Address Tables	STP Operation Mod	e Class	sic STP 💌		Guide
Port Management	BPDU Handling	Floor	ling 💌		Logout
Spanning Tree	Path Cost Default V	alues Long	V		
Interface Settings	Bridge Settings			-	
MSTP Multicast	Priority	32768			
Security Suite	Hello Time	2	(Sec)		
addinity of Dervice	C Max Age	20	(Sec)		
	C Forward Delay	15	(Sec)		
	Designated Root			-	
	Bridge ID	327	58-00:24:c6:26:49:00		
	Root Bridge IN	327	58-00:24:c6:26:49:00		•

- 2. Define the relevant fields.
- 3. Click Apply. STP is enabled, and the device is updated.



Defining Interface Settings

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

To assign STP settings to an interface:

1. Click Bridging > Spanning Tree > Interface Settings. The Interface Settings Page opens:

LINKSYS [®] livision of Cisco Systems, Inc.										
SFE 1000P	Inter	face	Settii	ngs						Help
System	⊙ Po	orts C	LAGs						<u>*</u>	Support
Admin Statistics Bridging	Port	STP	Port Fast	Root Guard	Port State	Port Role	Path Cost	Priority	Designated Bridge ID	Guide
Address Tables	e1	Enable	Disabled	Disable	Forwarding	Designated	200000	128	32768-00:24:cE	
- en Port Management	e2	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	Logout
Spanning Tree	e3	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
Interface Settings	e4	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
	e5	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
Multicast	eб	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
Security Suite Quality of Service	e7	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
	e8	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	
	•								▼ ▶	
									_	

- 2. Define the relevant fields.
- 3. Click Apply. STP is enabled on the interface, and the device is updated.

Modifying Interface Settings

- 1. Click Bridging > Spanning Tree > Interface Settings. The Interface Settings Page opens:
- 2. Click the Edit button. The Edit Interface Settings Page opens:

	zan monaco oonings rago	
SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Edit Interface	
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		
	Apply	

Edit Interface Settings Page

- 3. Define the relevant fields.
- 4. Click Apply. The interface settings are modified, and the device is updated.

Defining Rapid Spanning Tree

While the classic spanning tree prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops, and propagating status topology changes. Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

1. Click **Bridging > Spanning Tree > RSTP**. The *RSTP Page* opens:

sion of Cisco Systems, Inc.								
SFE 1000P	RSTP							Help
System Admin	Ports	ି LAGs					-	Support
Statistics Bridging	Interface	Role	Mode	Fast Link	Port Status	Point-to-Point Operational Status	Activate Protocol Migrat	Guide
Address Tables	e1	Designated	STP	Disable	Forwarding	Enable	Activate	
Port Management	e2	Disable	STP	Disable	Disabled	Enable	Activate	Logout
Spanning Tree	e3	Disable	STP	Disable	Disabled	Enable	Activate	
Interface Settings	e4	Disable	STP	Disable	Disabled	Enable	Activate	
	e5	Disable	STP	Disable	Disabled	Enable	Activate	
Multicast	e6	Disable	STP	Disable	Disabled	Enable	Activate	
Security Suite Quality of Service	e7	Disable	STP	Disable	Disabled	Enable	Activate	
	e8	Disable	STP	Disable	Disabled	Enable	Activate	
	4							

- 2. Define the relevant fields.
- 3. Click Apply. The Rapid Spanning Tree Settings are defined, and the device is updated.

Modifying RTSP

- 1. Click Bridging > Spanning Tree > RSTP. The RSTP Page opens:
- 2. Click the Edit button. The Edit Rapid Spanning Tree Page opens:

Edit Rapid Spanning Tree Page LINKSYS SFE 1000P Edit Rapid Spanning Tree Interface ● Port e1 ▼ O LAG 1 ▼ Designated Role STP Mode Disable **Fast Link Operational Status** Port State Forwarding Point to Point Admin Status Auto • Point to Point Operational Status Enable Activate Protocol Migration Test Г Apply

- 3. Define the relevant fields.
- 4. Click Apply. The Rapid Spanning Tree Settings are modified, and the device is updated.

Defining Multiple Spanning Tree

MSTP provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port is placed in the Forwarding State in another STP instance. The *MSTP Properties* page contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

The MSTP section contains the following 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.

To define MSTP:

1. Click Bridging > Spanning Tree > MSTP > Properties. The MSTP Properties Page opens:

	٨	ASTP Properties Page	
LINKSYS [®] A Division of Cisco Systems, Inc.			
SFE 1000P System Admin Statistics Bidging Address Tables VLAN Management VLAN Management VLAN Management Spanning Tree Properties Interface Settings SSTP MSTP MSTP Instance To VLAN Instance Settings Interface Settings Interface Settings Interface Settings Interface Settings Interface Settings	Properties Region Name Revision Max Hops IST Master Apply	00.24 cf3 25 43 00 0 20 32768-00.24 cf3 26 43 00	Help Support Guide Logout
			-deala- citata

- 2. Define the relevant fields.
- 3. Click Apply. The MSTP properties are defined, and the device is updated.

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.

The VLAN screen enables mapping VLANs to MSTP Instances.

1. Click Bridging > Spanning Tree > MSTP > Instance to VLAN. The Instance to VLAN Page opens:

nstanc	e To VL/	AN					ſ	Help
			120000000000000000000000000000000000000		120000000000000000000000000000000000000		<u> </u>	Support
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	Guide
VLAN 2	0	VLAN 18	0	VLAN 34	0	VLAN 50	0	
VLAN 3	0	VLAN 19	0	VLAN 35	0	VLAN 51	0	Logout
VLANA		VI AN 20		VLAN 36		VI AN 52		
VI AND		10-01-20		10.00.07		10.000.00		
VLAND		VLAN 21		VLAN 37		VLAN 55		
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		
	VLAN VLAN 1 VLAN 2 VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 8 VLAN 8	VLAN Instance ID (0.7) VLAN 1 0 VLAN 2 0 VLAN 3 0 VLAN 4 0 VLAN 5 0 VLAN 6 0 VLAN 8 0 VLAN 9 0	vLan Instance To VLAN VLAN 0.7) VLAN 1 0. VLAN 2 0. VLAN 3 0. VLAN 4 0. VLAN 5 0. VLAN 6 0. VLAN 8 0. VLAN 9 0.	vLan Instance ID (0.7) vLan Instance ID (0.7) VLAN 1 0 VLAN 17 0 VLAN 2 0 VLAN 18 0 VLAN 3 0 VLAN 19 0 VLAN 4 0 VLAN 20 0 VLAN 5 0 VLAN 21 0 VLAN 6 VLAN 23 0 0 VLAN 8 VLAN 24 0 0 VLAN 9 0 VLAN 25 0	vLan Instance ID (0.7) vLan Instance ID (0.7) vLan VLAN 1 0 vLAN 17 0 vLAN 33 VLAN 2 0 vLAN 18 0 vLAN 34 VLAN 3 0 vLAN 19 0 vLAN 36 VLAN 4 0 vLAN 20 0 vLAN 36 VLAN 5 0 vLAN 21 0 vLAN 37 VLAN 6 0 vLAN 22 0 vLAN 38 VLAN 7 0 vLAN 23 0 vLAN 38 VLAN 8 0 vLAN 24 0 vLAN 40 VLAN 9 0 vLAN 25 0 vLAN 40	VLAN Instance ID (J.7) VLAN Instance ID (J.7) VLAN Instance ID (J.7) VLAN 1 0 VLAN 17 0 VLAN 3 0 VLAN 2 0 VLAN 18 0 VLAN 4 0 VLAN 3 0 VLAN 19 0 VLAN 35 0 VLAN 4 0 VLAN 20 0 VLAN 36 0 VLAN 5 0 VLAN 21 0 VLAN 38 0 VLAN 6 0 VLAN 23 VLAN 38 0 VLAN 7 0 VLAN 24 VLAN 40 0 VLAN 8 0 VLAN 25 0 VLAN 41 0	vLan Instance ID (0.7) vLan 10 vLan 49 VLAN 1 0 vLAN 17 0 vLAN 33 0 vLAN 49 VLAN 2 0 vLAN 18 0 vLAN 35 0 vLAN 50 VLAN 3 0 vLAN 20 0 vLAN 36 0 vLAN 51 VLAN 4 0 vLAN 20 0 vLAN 36 0 vLAN 51 VLAN 5 0 vLAN 21 0 vLAN 37 0 vLAN 53 VLAN 6 0 vLAN 22 0 vLAN 38 0 vLAN 54 VLAN 7 0 vLAN 23 0 vLAN 40 vLAN 55 VLAN 8 0 vLAN 24 vLAN 40 0 vLAN 56 VLAN 9 0 vLAN 25 0 vLAN 41 0 vLAN 57	vlan Instance ID vlan 19 vlan 33 V vlan 40 Vlan 50 vlan 50 <th< td=""></th<>

Instance to VLAN Page

- 2. .Define the relevant fields.
- 3. Click Apply. The local user settings are modified, and the device is updated.

Defining MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

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

1. Click Bridging > Spanning Tree > MSTP > Instance Settings. The MSTP Instance Settings Page opens:

SFE 1000P	Instance Setting	s	Help
System	Instance ID	1 •	Support
Admin Statistics Bridging Address Tables Ort Management VLAN Management Spanning Tree	Included VLAN		Guide Logout
Properties Interface Settings	Bridge Priority	32768	
RSTP	Designated Root Bridge ID	32768-00:24:c6:26:49:00	
	Root Port	0	
	Root Path Cost	0	
Interface Settings	Bridge ID	32768-00:24:c6:26:49:00	
Len Multicast	Remaining Hops	20	
Quality of Service	Apply		

MSTP Instance Settings Page

- 2. Define the relevant fields.
- 3. Click Apply. The local user settings are modified, and the device is updated.

Defining MSTP Interface Settings

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

1. Click **Bridging > Spanning Tree > MSTP > Interface Settings**. The *MSTP Interface Settings Page* opens:

livision of Cisco Systems, Inc.			
SFE 1000P	Interface Sett	ngs	Help
System	Instance ID	1 💌	Support
Admin Statistics	Interface	• Port e1 • C LAG 1	
Bridging	Port State	N/A.	Guide
- Port Management	Туре	N/A.	Logout
-en VLAN Management	Role	N/A.	
	Mode	N/A.	
Interface Settings RSTP	Interface Priority	128	
MSTP	Path Cost	200000 🗌 Use Default	
Instance To VLAN	Designated Bridge ID	N/A.	
Interface Settings	Designated Port ID	N/A.	
Multicast	Designated Cost	N/A	
Quality of Service	Forward Transitions	N/A	
	Remain Hops	N/A.	
	Apply Inte	rface Table	

MSTP Interface Settings Page

2. Click the Interface Table button. The Interface Table Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



							v			
SFE	1000	•							LINKS	SYS [®] Systems, Inc.
					Interfac	е Та	able			
Instance	1	⊙ Po	rts O	LAGs						
Interface	Role	Mode	Туре	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
									Ap	olv

Interface Table Page

- 3. Define the relevant fields.
- 4. Click Apply. The Interface settings are modified, and the device is updated.

Configuring SNMP

The Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

SNMP v1 and v2

SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, User Security Model (USM) is defined for SNMPv3 and includes:

- Authentication Provides data integrity and data origin authentication.
- Privacy Protects against disclosure message content. Cipher 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

12

SFE1000P Gigabit Ethernet Switch Administration Guide

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.

1. Click System > SNMP > Security > Engine IP. The Engine ID Page opens:

Engine ID Page

A Division of Cisco Systems, Inc. SFE 1000P	Engine ID		Help
System Management System Management System Management Start Gerupy Gerupy Gerupy Gerups Geru	Local Engine ID (10-64 Hex Characters) Use Default Apply	EngineD not Configured	Support Guide Logout

- 2. Define the relevant fields.
- 3. Click Apply. The Engine ID settings are modified, and the device is updated.

12

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.

To define SNMP views:

Defining SNMP Views

1. Click System > SNMP > Security > Views. The SNMP Views Page opens:

SFE 1000P	View	s		Help
System	View N	lame Default 💌		Support
System Management				
ecurity		Object ID Subtree	View Type	Guide
Engine ID		1	Included	
Users		1.3.6.1.6.3.13	Excluded	Logout
Groups		1.3.6.1.6.3.16	Excluded	
Communities		1.3.6.1.6.3.18	Excluded	
Admin		1.3.6.1.6.3.12.1.2	Excluded	
Statistics		1.3.6.1.6.3.12.1.3	Excluded	
Bridging		1.3.6.1.6.3.15.1.2	Excluded	
Quality of Service		1.3.6.1.4.1.3955.89.2.7.2	Excluded	

2. Click the Add button. The Add SNMP View Page opens:

Add SNMP View Page

SFE 1000P				LINKSYS [®] A Division of Cisco Systems, Inc.
		Add SNN	IP View	
View Name				
Subtree ID Tree	☞ Select from List	system interfaces ip icmp tcp	Up Down	C Insert 1.3.6.1.2.1.1
View Type	Included 💌			Apply

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP views are defined, and the device is updated.

Defining SNMP Users

The SNMP Users Page provides information for creating SNMP 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.

1. Click System > SNMP > Security > Users. The SNMP Users Page opens:

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Users	Help
System Management System Management ShMP Engine ID Wews Groups Trap Management Management Statistics Bridging Security Suite Quality of Service	Luser Name Group Name Engine ID Authentication	Support Guide Logout

2. Click the Add button. The Add SNMP Group Membership Page opens:

Add SNMP Group Membership Page

SFE 1000P					LINKS A Division of Cisco Syst	YS [®] ems, Inc.
Add	SNMP	Group	Membe	rship		
User Name]		
Engine ID	@ Local	Remote				
Group Name	Y					
Authentication Method	None	~				
Password						
Authentication Key						
Privacy Key						
					Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Group Membership settings are modified, and the device is updated.



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.

- 1. Click System > SNMP > Security > Users to open the Edit SNMP User Page
- 2. Define the relevant fields.
- 3. Click Apply. The SNMP User is modified, and the device is updated.

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.

1. Click System > SNMP > Security > Groups. The SNMP Groups Profile Page opens:

SFE 1000P	Groups				Help
	🗖 Group Name	Security Model	Security Level	Operation	Support
SNMP			Re	ad Write Notify	Guide
Engine ID			Delete	Add	
Users					Logout
Communities					
Admin Statistics					
Bridging					

2. Click the Add button. The Add SNMP Group Profile Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



Add SNMP Group Profile Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Add SNMP Group Profile	
Group Name		
Security Model	SNMPv1 💌	
Security Level	No Authentication 💌	
Operation	🗆 Read Default 🔽 🗖 Write Default 🔽 🗖 Notify	Default
		Apply

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP settings are modified, and the device is updated.

Modifying SNMP Group Profile Settings

- 1. Click System > SNMP > Security > Groups. The SNMP Groups Profile Page opens:
- 2. Click the Edit Button. The Edit SNMP Group Profile Page opens:

Edit SNMP Group Profile Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	SNMP Group Profile Settings	
Group Name	snmp group 💌	
Security Model	SNMPv1 🔽	
Security Level	No Authentication	
Operation	Read Default Vrite Default Vrite Vrite	Default 💌
		Apply

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP settings are modified, and the device is updated.



Defining SNMP Communities

The Access rights are managed by defining communities in the SNMP Communities Page. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

To define SNMP Communities:

1. Click System > SNMP > Security > Communities. The SNMP Communities Page opens:

Division of Cisco Systems, Inc.		
SFE 1000P System System Management SumP Scurity Communities Communities Statistics Bridging Security Suite Quality of Service	Communities Basic Table Management Station Community String Access Mode View Name Advanced Table Management Station Community String Group Name Delete Add	Help Support Guide Logout

SNMP Communities Page

2. Click the **Add** button. The Add SNMP Community Page opens.

Add SNMP Community Page

SFE 1000P	
Add SNMP Commu	nity
SNMP Management Station C All (0.0.0.0) Community String	X)
ⓒ Basic Access Mode Read Only ▼ □ V ⓒ Advanced Group Name ▼	liew Name Default 💌

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP settings are modified, and the device is updated.

12

SFE1000P Gigabit Ethernet Switch Administration Guide

Modifying SNMP Community Settings

- 1. Click System > SNMP > Security > Communities. The SNMP Communities Page opens:
- 2. Click the Edit Button. The Edit SNMP Community Page:

Edit S	SNMP Commu	nity Page	
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
SNMP (Community	/ Settings	3
SNMP Management 124.0.0.0 Community String 12	•		
Basic Access Mode Advanced Group Name	Read Only 💌	🔽 View Name	Default
			Apply

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Community settings are defined, and the device is updated.

12

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.

 Click System > SNMP > Security > Trap Management > Trap Settings. The Trap Settings Page opens:

LINKSYS [®] A Division of Cisco Systems, Inc.	irap senings rage	
SFE 1000P	Enable SNMP Notifications Image: Comparison of the symplectic sy	Help Support Guide Logout

- 2. Define the relevant fields.
- 3. Click Apply. The trap settings are modified, and the device is updated.

Configuring Station Management

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

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

Chapter 12: Configuring SNMP Defining Trap Management



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.

1. Click System > SNMP > Security > Trap Management > Station Management. The Station Management Page opens:

Station	Management Pa	ge
---------	---------------	----

SFE 1000P	Sta	ation M	anagen	nent							Help
System	SN	MPv1,2 Noti	fication Rec	ipient							Support
 System Management SNMP Security 		Recipients IP	Notification Type	Commu String	nity Not Ver	ification sion	UDP Port	Filter Name	Timeout	Retries	Guide
Trap Management	SN	MPv3 Notifi	cation Recip	ient							Logout
Station Managemen 		Recipients IP	Notification Type	User Name	Security .evel	UDP Port	Filter Name	Timeou	t Retries		Logout
Admin Statistics								Delete		Add	
💼 Bridging											
Quality of Service											
<u> </u>											

2. Click the Add button. The Add SNMP Notification Recipient Page opens.

SFE1000P Gigabit Ethernet Switch Administration Guide



Add	SNMP	Notification	Recipient	Page
				<u> </u>

SFE 1000P	LINKSYS A Division of Cisco Systems, Inc.
	Add SNMP Notification Recipient
Recipient IP Notification Type	e Traps 💌
• SNMPv1,2 Community Strin Notification Vers	ng sion SNMPv1 •
C SNMPv3 User Name Security Level	NoAuthentication 💌
UDP Port Filter Name Timeout	162 15 (sec)
Retries	S Apply

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Recipient settings are defined, and the device is updated.

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.

- 1. Click System > SNMP > Security > Trap Management > Station Management.
- 2. Click the Edit button. The Edit SNMP Notification Page opens:

	Ean Statin Tash	icalion i ugo	
SFE 1000P			LINKSYS [®] A Division of Cisco Systems, Inc.
	SNMP Notificati	ion Reciever	
Recipient IP	210.0.0.0 💌		
Notification Type	Traps 💌		
• SNMPv1,2			
Community Stri	ng 1		
Notification Vers	sion SNMPv1 💌		
SNMPv3			
User Name			
Security Level	NoAuthentication 💌		
UDP Port	162		
🔲 Filter Name			
Timeout	15		
Retries	3		
	Apply		

Edit SNMP Notification Page

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Receivers are defined, and the device is configured.

Defining SNMP Filter Settings

The Filter Settings Page permits filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The Filter Settings Page also allows network managers to filter notifications.

 Click System > SNMP > Security > Trap Management > Filter Settings. The Filter Settings Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



Filter Settings Page

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System System Management Security Trap Management Trap Settings Station Management Station Management Statics Station Management Statics Control Statics Statics Control Statics Control Statics Security Suite Control Statics Control Statics Security Suite Control Statics Security Suite Security Suite Control Statics Security Suite Security Security	Filter Settings Filter Name Cobject ID Subtree Filter Type Coelete Add Apply	Heip Support Guide Logout

2. Click the Add button. The Add SNMP Notification Filter Page opens:

Add SNMP Notification Filter Page

SFE 1000P					A Division of Cisco System	15 ° ms, inc.
	Add	SNMP N	otification	Filter		
Filter Name						
New Object Identifier Tree	 Select from List 	system interfaces ip icmp tcp	▲ Up Down	C Object ID		
Filter Type	Included 💌					
					Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Filter is added to the list, and the device is updated.

Configuring Quality of Service

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
 - The ingress interface
 - Packet content
 - A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
 - The assignment of network traffic to a particular hardware queue
 - The assignment of internal resources
 - Traffic shaping

The terms Class of Service (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to trafficclasses, 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

13

SFE1000P Gigabit Ethernet Switch Administration Guide

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.

1. Click Quality of Service > General > CoS. The CoS Page opens:

CoS Page						
LINKSYS [®] A Division of Cisco Systems, Inc.						
	-					
SFE 1000P	CoS				Hel	p
💼 System	QoS M	ode Basic	•		Supp	ort
- Chatina - Chat						
Bidging C Ports C LAGs				Guid	le	
💼 Security Suite						
	Interfa	ce Default CoS		Restore Defaults	Logo	ut
- CoS	e1	0	Edit			
Queue	e2	0	Edit			
CoS to Queue	e3	0	Edit			
Bandwidth	e4	0	Edit			
- Advanced Mode	e5	0	Edit			
_	e6	0	Edit			
	e7	0	Edit			
	· .	~	e 1%	-	-	

- 2. Define the relevant fields.
- 3. Click Apply. The CoS settings are modified, and the device is updated.

Modifying Interface Priorities

- 1. Click Quality of Service > General > CoS. The CoS Page opens:
- 2. Click the Edit button. The Edit Interface Priority Page opens:

Edit Interface Priority Page

SFE 1000P	LINKSYS A Division of Cisco Systems, Inc.
Edit Interface Priority	
Interface 💿 Port et 💌 🔿 LAG 1 💌	
Set Default User Priority	
Apply	

- 3. Modify the Interface priority.
- 4. Click Apply. The Interface priority is set, and the device is updated.
Defining Queue

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

1. Click Quality of Service > General > Queues. The Queue Page opens:

LINKSYS® Division of Cisco Systems, Inc.				
SFE 1000P	Queur	e		Help
En System	C Stric	:t Priority	• WRR	Support
Statistics	-	61.1		Guide
-en Security Suite	Queue	Schedu	ng	
	Guouo	WRR	% of WRR Bandwidth	Logout
General	1	1	6.67	
	2	2	13.33	
CoS to Queue	3	4	26.67	
DSCP to Queue Bandwidth Advanced Mode Basic Mode	4	8	53.33	
	-			

- 2. Define the queues.
- 3. Click Apply. The queues are defined, and the device is updated.

Mapping CoS to Queue

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

1. Click Quality of Service > General > CoS to Queue. The Cos to Queue Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



Cos to Queue Page

LINKSYS [®] A Division of Cisco Systems, Inc.				
SFE 1000P C	oS to Que	ue		Help
 System Admin Statistics 	Restore Defaults			Support
Bridging	Class of Service	Queue		Guide
Curry Suite	0	1 •		Logout
General	1			
Queue	2			
CoS to Queue	4	3 -		
Bandwidth	5	3 •		
Basic Mode	6	4 💌		
	7	4 💌		
	Apply			

- 2. Define the relevant fields.
- 3. Click Apply. CoS to queues are mapped, and the device is updated.

Mapping DSCP to Queue

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

To map DCSP to Queues:

1. Click Quality of Service > General > DSCP to Queue. The DSCP to Queue Page opens:

SFE 1000P	DSCP 1	o Qu	eue				Help
System	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	Support
Admin Statistics	0	1 💌	25	2 💌	50	4 🔻	
Bridging	1	1 💌	26	2 💌	51	4	Guide
Security Suite	2	1 💌	27	2 🔻	52	4 💌	
equality of Service	3	1 💌	28	2 💌	53	4 💌	Logout
- CoS	4	1 💌	29	2 💌	54	4 💌	
	5	1 💌	30	2 -	55	4 -	
DSCP to Queue	6	1 💌	31	2 💌	56	4 💌	
Bandwidth	7	1 💌	32	2 -	57	4 💌	
Basic Mode	8	1 💌	33	3 💌	58	4 💌	
	9	1 💌	34	3 🕶	59	4	
	10	1 💌	35	3 🛩	60	4 -	
	11		20		C1		-

- 2. Define the relevant fields.
- 3. Click Apply. DSCP to queues are mapped, and the device is updated.

Configuring Bandwidth

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

Rate Limits and Shaping are defined per interface:

- Rate Limit sets the maximum bandwidth allowed on ingress interfaces.
- Shaping Rate sets the maximum bandwidth allowed on egress interfaces. On GE ports, traffic shape for burst traffic (CbS) can also be defined.
- 1. Click Quality of Service > General > Bandwidth. The Bandwidth Page opens:

SFE 1000P	Bandw	idth								Help
System	Ports	C LAGs							-	Suppo
Admin Statistics	Interface	Ingress	Rate Limit	Egress S	Shaping	Rates				
Bridging		Status	Rate Limit	Status	CIR	CBS				Guide
Security Suite Quality of Service	e1	Disable		Disable			Edit			
General	e2	Disable		Disable			Edit			Logou
CoS	e3	Disable		Disable			Edit			
CoS to Queue	e4	Disable		Disable		Ì	Edit			
Bandwidth	e5	Disable		Disable			Edit			
Advanced Mode	еб	Disable		Disable			Edit			
	e7	Disable		Disable			Edit			
								_		

Bandwidth Page

2. Click the Edit button. The Edit Bandwidth Page opens:

Edit Bandwidth Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
Edit	Bandwidth	
Interface : Port e1 🗾 C LAG		
Enable Egress Shaping Rate		
Committed Information Rate (CIR)	64	
Enable Ingress Rate Limit		
Ingress Rate Limit	62	
	Apply	

3. Modify the relevant fields.



4. Click Apply. The bandwidth settings are modified, and the device is updated.

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.

1. Click Quality of Service > Advanced Mode > DSCP Mapping. The DSCP Mapping Page opens:

LINKSYS®							
SFE 1000P	DSCP	Vappin	ıg			ſ	Help
💼 System	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	Support
Admin Statistics	0	0 💌	25	25 💌	50	50 💌	
Bridging	1	1 💌	26	26 💌	51	51	Guide
Security Suite	2	2 💌	27	27 💌	52	52 💌	-
- General	3	3 🔻	28	28 💌	53	53 💌	Logout
	4	4 💌	29	29 💌	54	54 💌	
Class Mapping	5	5 💌	30	30 💌	55	55 💌	
Policy Table	6	6 💌	31	31 💌	56	56 💌	
Policy Binding	7	7 💌	32	32 💌	57	57 💌	
	8	8 💌	33	33 💌	58	58 💌	
	9	9 🔻	34	34 💌	59	59 💌	
	10	10 -	25	25 -	en		

DSCP Mapping Page

- 2. Define the relevant fields.
- 3. Click Logout. The DSCP settings are modified, and the device is updated.

Defining Class Mapping

The *Class Mapping Page* contains parameters for defining class maps. One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned to packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

1. Click Quality of Service > Advanced Mode > Class Mapping. The Class Mapping Page opens:

	Class Mapping Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Class Mapping Class Map ACL 1 Match ACL 2 Delete Add	Help Support Guide Logout
		alut

2. Click the Add button. The Add QoS Class Map Page opens:

Add QoS Class Map Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add Qos Class Map	
Class Map Name		
Preferred ACL	IP Based ACL	
F IP ACL	V	
Match	And	
MAC ACL		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. QoS mapping is added, and the device is updated.

Defining Aggregate Policer

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

1. Click Quality of Service > Advanced Mode > Aggregate Policer. The Aggregate Policer Page opens:



- 2. Click the Add button. The Add QoS Aggregate Policer Page opens:

Aggregate Policer Page

SFE1000P Gigabit Ethernet Switch Administration Guide



Add QoS Aggregate Policer Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
Add QoS A	ggregate Poli	cer
Aggregate Policer Name		
Ingress Committed Information Rate (CIR)	3	(Kbits per Second)
Ingress Committed Burst Size (CBS)	3000	(Bytes per Second)
Exceed Action	None	
		Apply

- 3. Define the relevant fields.
- 4. Click Apply. The Aggregate policer is added, and the device is updated.

Modifying QoS Aggregate Policer

- 1. Click Quality of Service > Advanced > Aggregate Policer. The Aggregate Policer Page opens:
- 2. Click the Edit Button. The Edit QoS Aggregate Policer Page opens:

Edit QoS Aggregate Policer Page

SFE 1000P		LINKSYS A Division of Clisco Systems, Inc.
Edit QoS A	ggregate Poli	cer
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	
		Apply

- 3. Modify the relevant fields.
- 4. Click Apply. QoS aggregate policer settings are modified, and the device is updated.

13

Configuring Policy Table

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

1. Click **Quality of Service > Advanced > Policy Table**. The *Policy Table Page* opens:

	Policy Table Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Policy Table	Help
Gradinin Statistics Grading Statistics Grading Gradin	Delete Add	Support Guide Logout
		abab

2. Click the Add button. The Add QoS Policy Profile Page opens:

Add QoS Policy Profile Page

SFE 1000P			
	Add QoS I	Policy Profile	
New Policy Name			
🗖 Class Map	Y		
	Trust CoS-DSCP		
C Action	C Set DSCP New Y	(0 - 63)	
Police			
Туре	Single		
Aggregate Policer	agPol1 🔽		
Ingress Committed Information Rate (CIR)	3	(Kbits per Second)	
Ingress Committed Burst Size (CBS)	3000	(Bytes)	
Exceed Action	None		
		Ap	pply

- 3. Add a QoS policy profile.
- 4. Click Apply. The QoS policy profile is added, and the device is updated.

Modifying the QoS Policy Profile

 Click Quality of Service > Advanced > QoS Policy Profile. The Edit QoS Aggregate Policer Page opens:

Edit QoS Policy Profile Page

SFE 1000P		A Division of Cisco Systems, Inc.
Edit	Qos Policy Profile	
Policy Name	Qos Policy 💌	
🗌 Class Map	Y	
_	Trust CoS-DSCP	
Action	Set DSCP New Value	(0 - 63)
Police		
Туре	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 Typ	e Aggregate CIR CBS Exceed Action Policer Name Delete	
		Apply

- 2. Define the relevant fields.
- 3. Click Apply. The QoS policy profile is defined, and the device is updated.

13

Defining Policy Binding

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

1. Click Quality of Service > Advanced > Policy Binding. The Policy Binding Page opens:

	Policy Binding Page	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Policy Binding Interface Policy Name Delete Add	Help Support Guide Logout
		diala

2. Click the Add button. The Add QoS Policy Binding Page opens:

Add QoS Policy Binding Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add Qos Policy Binding	
Interface	● Port e1 ▼ OLAG 1 ▼	
Policy Name	Qos Policy 💌	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The QoS Policy Binding is defined, and the device is updated.

13

Modifying QoS Policy Binding Settings

- 1. Click Quality of Service > Advanced > Policy Binding. The Policy Binding Page opens:
- 2. Click the Edit button. The Edit QoS Policy Binding Page opens:

Edit QoS Policy Binding Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Qos Policy Binding Settings	
Interface	e1	
Policy Name	Qos Policy	
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The QoS policy binding is defined, and the device is updated.

Defining QoS Basic Mode

The *Basic Mode Page* contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

1. Click Quality of Service > Basic Mode. The Basic Mode Page opens:

	Basic Mode Page	
System Admin Statistics Division of Claco Systems, Inc. System Admin Statistics Dirdiging Security Suite Guality of Service General Gos Queue Cos to Queue Cos to Queue	Basic Mode Page Basic Mode Trust Mode Cos Always Rewrite DSCP CSCP Rewrite Apply	Help Support Guide Logout
Bardwidth Bardwidth dvanced Mode DSCP Mapping Class Mapping Agregate Policer Policy Table Policy Binding Basic Mode		
		ahaha cisco

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

2. Click the **DSCP Rewrite** button. The DSCP Mapping Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



DSCP Mapping Page

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

- 3. Define the DSCP mappings.
- 4. Click Apply. The DSCP mappings are defined, and the device is updated.

4

SFE1000P Gigabit Ethernet Switch Administration Guide

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.

SFE1000P Gigabit Ethernet Switch Administration Guide



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.

1. Click Admin > File Management > Firmware Upgrade. The Firmware Upgrade Page opens:

SFE 1000P	Firmware Upgrade	Help
System	© UPGRADE ○ BACKUP	Support
Admin 	File Type Software Image	
Firmware Upgrade Save Configuration	TFTP Server	Guide
Copy Files	Source File	Logout
Active Image	Destination File None Active Image	
Diagnostics		
Bridging	Apply	
Security Suite Quality of Service		
_		

- 2. Define the relevant fields.
- 3. Click Apply. Firmware upgrade is defined, and the device is updated.

Save Configuration

The configuration files control the operation of the switch, and contain the functional settings at the device and the port level. Configuration files are one of the following types:

- **Factory Default** Contains preset default parameter definitions which are downloaded with a new or upgraded version.
- **Running Configuration** Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device was started or rebooted. When the device shuts down or reboots the next time, this configuration becomes the Starting Configuration.
- **Starting configuration** Contains the parameter definitions which were valid in the Running Configuration when the system last rebooted or shut down.
- **Backup configuration** Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_"). In the *Save Configuration Page*, define the parameters of the system configuration files.

1. Click Admin > File Management > Save Configuration. The Save Configuration Page opens:

SFE 1000P	Save Configuration	Help Support Guide Logout
-----------	--------------------	------------------------------------

Save Configuration Page

- 2. Define the relevant files.
- 3. Click Apply. The save configuration is defined, and the device is updated.

Copy Files

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

1. Click Admin > File Management > Copy Files. The Copy Files Page opens:



LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System Admin File Management File Management Save Configuration Copy Files Logs Diagnostics Statistics Bridging Security Suite Coulty of Service	Copy Files Restore Configuration Factory Defaults Copy Configuration Source File Name Destination File Name Running Configuration Apply	Help Support Guide Logout
		abab

- 2. Define the relevant fields.
- 3. Click Apply. Copy Files is configured, and the device is updated.

Active Image

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

1. Click Admin > File Management > Active Image. The Active Image Page opens:

	Active Image Page	
LINKSYS® A Division of Cisco Systems, Inc.		
SFE 1000P Admin File Management See Configuration Copy Files Logs Diagnostics Statistics Statistics Statistics Court Files Court Files C	Active Image After Reset Image 1 Image	Help Support Guide Logout
		alialia

- 2. Define the relevant fields.
- 3. Click Apply. Active image is define, and the device is updated.

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.

To define Log Global Parameters:

1. Click Admin > Logs > Logs Settings. The Log Settings Page opens.

		Lo	g Settin	gs Page		
LINKSYS [®] A Division of Cisco Systems, Inc.						
SFE 1000P	Log Sett	ings			ſ	Help
ia-∎ System ia-⊕Admin ia- File Management	Enable Loggi	ng 🔽			-	Support
Logs	Severity	Console	Memory Logs	Log Flash		Guide
Log Settings	Emergency	2	v	V		
Flash	Alert	~	V	V		Logout
Remote Log Servers	Critical	V	V	V		
Diagnostics	Error	V	V	7		
i - m Bridging	Warning	•	2			
🗄 🂼 Security Suite	Notice	2	V			
	Informational	V	~			
	Debug					
	Apply				-	
						alialie

- 2. Define the relevant fields.
- 3. Click Apply. The global log parameters are set, and the device is updated.

15

Viewing the Device Memory Logs

The *Memory Page* contains all system log entries in chronological order that are saved in RAM (Cache). After restart, these log entries are deleted.

To open the Memory Page:

1. Click Admin > Logs > Memory. The Memory Page opens.

Memory Page

SFE 1000P	Memory				Help
- en System	Log Index	Log Time	Severity	Description	Support
Admin	2147483546	01-Dec-2006 21:16:50	Informational	%AAA-I-CONNECT: New http connection for	
File Management	2147483547	01-Dec-2006 20:55:19	Informational	%AAA-I-DISCONNECT: User CLI session for	Guide
Log Settings	2147483548	01-Dec-2006 20:51:43	Informational	%AAA-I-DISCONNECT: http connection for u	
- Memory	2147483549	01-Dec-2006 20:51:18	Informational	%AAA-I-CONNECT: New http connection for	Logout
- 🕒 Flash	2147483550	01-Dec-2006 20:50:39	Informational	%AAA-I-CONNECT: New http connection for	
Remote Log Servers Disgnaction	2147483551	01-Dec-2006 20:45:17	Informational	%AAA-I-CONNECT: User CLI session for us	
Statistics	2147483552	01-Dec-2006 20:42:52	Informational	%AAA-I-DISCONNECT: User CLI session for	
💼 Bridging	2147483553	01-Dec-2006 20:40:16	Informational	%AAA-I-DISCONNECT: http connection for u	
e in Security Suite	2147483554	01-Dec-2006 20:39:17	Informational	%AAA-I-CONNECT: New http connection for	
- Cuality of Service	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 connection	
	2147483557	01-Dec-2006 20:32:43	Warning	%AAA-W-REJECT: New console connection	
	2147483558	01-Dec-2006 20:28:25	Informational	%AAA-I-DISCONNECT: User CLI session for	

2. Observe the log files and look for any pertinent information.

Clearing Message Logs

Message Logs can be cleared from the Memory Page. To clear the Memory Page:

- 1. Click Admin > Logs > Memory. The Memory Page opens.
- 2. Click the Clear Logs button. The message logs are cleared.



Viewing the Flash Logs

The *Flash Page* contains information about log entries saved to the Log File in FLASH, including the time the log was generated, the event severity, and a description of the log message. The Message Log is available after reboot.

To view the Flash Logs:

1. Click Admin > Logs > Flash. The Flash Page opens:

Flash Page

	Floop			1	
SFE 1000P	Flash				Help
- Contraction - System	Log Index	Log Time	Severity	Description	Support
	2147477238	01-Dec-2006 01:42:24	Emergency	%SOCK-F-TCP: SOCKP_socket: TCP error -	
File Management	2147478315	01-Dec-2006 01:02:28	Emergency	%SOCK-F-MEM: SOCKP_tcp_open_call: Col	Guide
Log Settings	2147479317	01-Dec-2006 01:56:13	Emergency	%SOCK-F-TCP: SOCKP_socket: TCP error -	
- Memory	2147479454	01-Dec-2006 01:34:06	Alert	%TFTP-A-TftpRxERROR: An error message v	Logout
- 🗋 Flash	2147479591	01-Dec-2006 01:31:40	Alert	%TFTP-A-TftpRxERROR: An error message v	
Remote Log Servers	2147479728	01-Dec-2006 01:31:08	Alert	%TFTP-A-TftpRxERROR: An error message v	
Statistics	2147479865	01-Dec-2006 01:30:49	Alert	%TFTP-A-TftpRxERROR: An error message v	
- 💼 Bridging	2147479986	01-Dec-2006 01:03:36	Error	%INIT-E-ApplErr: Errors occurred during initial	
💼 Security Suite	2147480179	01-Dec-2006 01:01:26	Error	%MNG_DIAG-E-DIAGATINIT: Init: SNMPCen(
Quality of Service	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	

2. Observe the log files and look for any pertinent information.

Clearing Message Logs

Message Logs can be cleared from the FLASH Log Page. To clear the Flash Page:

- 1. Click Admin > Logs > FLASH. The Flash Page opens.
- 2. Click Clear Logs. The message logs are cleared.

Viewing Remote Logs

The *Remote Log Servers Page* contains information for viewing and configuring the Remote Log Servers. New log servers and the minimum severity level of events sent to them may be added.

1. Click Admin > Logs > Remote Log Servers. The Remote Log Servers Page opens:

Remote Log Servers Page

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Remote Log Servers	Help Support Guide Logout

2. Click the Add button. The Add Syslog Server Page opens:

Add Syslog Server Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Add Syslog Server	
Log Server IP Address		
UDP Port	514	
Facility	Local 7 💌	
	<u> </u>	
Description		
	Y	
Minimum Severity	Informational 💌	
	Apply	

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

- 3. Define the relevant fields.
- 4. Click **Apply.** The Add Syslog Server Page closes, the syslog server is added, and the device is updated.

15

Modify Syslog Server Settings

1. Click Admin > Logs > Remote Log Servers. The Remote Log Servers Page opens:

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

	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	4	
Severity To Include	Informational 💌	
	Apply	

_

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

- 3. Define the relevant fields.
- 4. Click Apply. The Syslog Server settings are modified, and the device is updated.

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. To define system time:

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

	`	
SFE 1000P	System Time	He
System System Management	Clock Source	© Use Local Settings C Use SNTP Server
	Local Settings	Gu
	Date	01/Dec/06 (DDMMM/YY)
System Time	Local Time	21:31:29 (HHMM:SS)
SNTP Authenticatio	n Time Zone Offset	GMT 💌
Domain Name System	Daylight Saving	C USA C European C Other
Admin	Time Set Offset	60 (Min)
Statistics Bridging	From	(DDAMMMYY) (HH:MM)
Security Suite	То	(DDAMM/YY) (HH:MM)
Quality of Service	Recurring	
	From	Day Sun 💌 Week First 💌 Month Jan 💌 Time 00:00 (HH:MM)
	_	

System Time Page

- 2. Define the relevant fields.
- 3. Click Apply. The Time Settings are defined, and the device is updated.

Defining SNTP Settings

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

To define SNTP global settings:

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

	SNTP Settings Page	
A Division of Claco Systems, Inc.	SNTP Settings	Help Support Guide
System Information Reset System Time SNTP Settings SNTP Authentica PAddressing SNMP Addressing SNMP Statistics Bridging Security Suite	Unicast SNTP Servers SNTP Server Poll Interval Encryption Key ID Preference Status Last Response Delete (Guide
		aha

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

Add SNTP Server Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add SNTP Server	
SNTP Server		
🗖 Enable Poll Interval		
Encryption Key ID		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The SNTP Server is added, and the device is updated.

Defining SNTP Authentication

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

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

	er till / tellitellitealleri i age	
LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P System System Management Zoom System Information Reset Time SNTP Settings SNTP Authentics SNTP Admin Statistics Bridging Security Suite	SNTP Authentication C Enable SNTP Authentication C Encryption Key ID Authentication Key Trusted Key Delete Add Apply	Help Support Guide Logout
		altah

SNTP Authentication Page

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

Add SNTP Authentication Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Add SNTP Authentication	
Encryption Key ID		
Authentication Key		
Trusted Key		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The SNTP Authentication is defined, and the device is updated.



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.

1. Click Statistics > Ethernet > Interface. The Interface Page opens:

LINKSYS [®] Division of Cisco Systems, Inc.		
SFE 1000P	Interface	Help
System Admin Statistics Ethernet	Interface © Port of v C Lac I v Refresh Rate	Support Guide
Interface Etherlike GVRP EAP	Receive Statistics Total Bytes (Octets) 18537219	Logout
Endging	Unicast Packets 66651	
Security Suite Output Output <	Multicast Packets 92751	
	Broadcast Packets 16559	
	Packets with Errors 0	
	Transmit Statistics	

2. Click the appropriate radio buttons and pulldowns to select an interface.

17

SFE1000P Gigabit Ethernet Switch Administration Guide

Resetting Interface Statistics Counters

- 1. Click **Statistics > Ethernet > Interface**. The *Interface Page* opens:
- 2. Click the Clear Counters button. The interface statistics counters are cleared.

Viewing Etherlike Statistics

The Etherlike Page contains interface statistics.

To view Etherlike Statistics:

1. Click **Statistics > Ethernet >Etherlike**. The *Etherlike Page* opens:

herlike erface 은 Port et 및 C Lac	1 9	Help
herlike erface @ Poxt @T 및 C LAG	1 9	Help
efresh Rate No Refresh 💌		Guide
rame Check Sequence (FCS) Errors	0	Logout
ate Collisions	0	
xcessive Collisions	0	
versize Packets	0	
ternal MAC Receive Errors	0	
eceived Pause Frames	0	
ransmitted Pause Frames	0	-
	rame Check Sequence (FCS) Errors ingle Collision Frames ate Collisions xccessive Collisions versize Packets atternal MAC Receive Errors eceived Pause Frames ransmitted Pause Frames	rame Check Sequence (FCS) Errors ingle Collision Frames ate Collisions ate Collisions cocesive Collisions versize Packets teternal MAC Receive Errors ecceived Pause Frames 8

Etherlike Page

2. Click the appropriate radio buttons and pulldowns to select an interface.

Resetting Etherlike Statistics Counters

- 1. Click Statistics > Ethernet > Etherlike. The Etherlike Page opens:
- 2. Click the Clear Counters button. The interface statistics counters are cleared.

17

Viewing GVRP Statistics

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

To view GVRP statistics:

1. Click Statistics > GVRP Statistics. The GVRP Page opens.

GVRP Page				
LINKSYS [®] A Division of Cisco Systems, Inc.				
SEE 1000P	GVRP	Hein		
SFE 1000P	Interface C Port of C LAG 1 V Refresh Rate No Refresh V	Support Guide		
interface Etherlike	Attribute (Counter) Received Transmitted	Logout		
RMON	Join Empty 0 0 Empty 0 0			
Becurity Suite	Leave Empty 0 0			
	Join In 0 0			
	Leave In 0 0			
	Leave All 0 0	-		

2. Click the appropriate radio buttons and pulldowns to select an interface.

Resetting GVRP Statistics Counters

- 1. Click Statistics > GVRP Statistics. The GVRP Page opens.
- 2. Click Clear Counters. The GVRP statistics counters are cleared.



Viewing EAP Statistics

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

To view the EAP Statistics:

1. Click Statistics > Ethernet > EAP Statistics. The EAP Page opens.

LINKSYS® A Division of Cisco Systems, Inc.			
SFE 1000P	EAP Port et v Refresh Rate No Retresh v		Help Support Guide
Chremit Interface Cherike CVRP EAP RMON	Frames Receive Frames Transmit Start Frames Receive	0 4 0	Logout
⊕ en Bridging ⊕ en Security Suite ⊕ en Quality of Service	Log off Frames Receive Respond ID Frames Receive Respond Frames Receive	0 0	
	Request ID Frames Transmit Request Frames Transmit Invalid Frames Receive	0 0	<u> </u>
			alada cisco

2. Click the appropriate pulldowns to select an interface.

SFE1000P Gigabit Ethernet Switch Administration Guide



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.

PMON Statistics Page

To view the RMON statistics:

1. Click Statistics > RMON > Statistics. The RMON Statistics Page opens:

LINKSYS [®] A Division of Cisco Systems, Inc.			
SFE 1000P	Statistics		Help
- En System - En Admin - Statistics	Interface Refresh Rate	Port et C LAG 1	Support
RMON	Received Bytes (Octets) Received Packets	19218777 181978	Logout
Alarms	Broadcast Packets Received	16846	
- Security Suite Call Quality of Service	Multicast Packets Received CRC & Align Errors	94414	
	Undersize Packets	0	
	Oversize Packets Fragments	0	
	Jabbers	0	_

2. Select an interface in the Interface field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

- 1. Click Statistics > RMON > Statistics. The RMON Statistics Page opens:
- 2. Click the Reset Counters button. The RMON statistics counters are cleared.

SFE1000P Gigabit Ethernet Switch Administration Guide

Configuring RMON History

This section contains the following topics:

- Defining RMON History Control
- Viewing the RMON History Table

Defining RMON History Control

The RMON History Control Page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods. To view RMON history information:

1. Click Statistics > RMON > History. The RMON History Control Page opens.

LINKSYS® A Division of Cisco Systems, Inc.		
SFE 1000P	History History Source Sampling Sampling Current Number Owner Entry No. Interface Interval Requested of Samples Delete Add	Heip Support Guide Logout

RMON History Control Page

2. Click the Add button. The Add RMON History Page opens:

Add RMON History Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add RMON History	
New History Entry	1	
Source Interface	Port e1 C LAG 1	
Owner		
Max No. of Samples to Keep	50	
Sampling Interval	1800	
	Apply	

3. Define the relevant fields.



4. Click Apply. The entry is added to the RMON History Control Page, and the device is updated.

Modify History Control Settings

- 1. Click Statistics > RMON > History. The RMON History Control Page opens.
- 2. Click the Edit button. The Edit RMON History Page opens:

	Ean Millort Thislory Tage	
SFE 1000P		LINKSYS A Division of Cisco Systems, In
	History Control Settings	
History Entry No.	1 -	
Source Interface	• Port e1 🗨 C LAG 1	
Owner		
Max No. of Samples to Keep	50	
Sampling Interval	1800	
	Apply	

Edit RMON History Page

- 3. Define the relevant fields.
- 4. Click Apply. The history control settings are defined, and the device is updated.

Viewing the RMON History Table

The RMON History Table Page contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

- 1. Click Statistics > RMON > History. The RMON History Control Page opens:
- 2. Click the History Table button. The RMON History Table Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



RMON History Table Page

LINKSYS [®] A Division of Cisco Systems, Inc.										
SFE 1000P	Hist	ory						ſ	Help	
ie — Eystem ie — — Admin		History Entry No.	Source Interface	Sampling Interval	Sampling Requested	Current Number of Samples	Owner		Support	
Statistics Statistics MON Statistics Statistics	His	1 tory Table	e1	1800	50	50	elete	Edit Add	Guide Logout	
Events Alarms Bridging Security Suite Society of Sprice										
B Gdairy of Centre										
	· •)
									.1	1

3. To return to the RMON History Control Page, click the Interface Table button.

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.

To view RMON events:

1. Click Statistics > RMON > Events. The RMON Events Page opens:

SFE1000P Gigabit Ethernet Switch Administration Guide



RMON Events Page

LINKSYS [®] A Division of Cisco Systems, Inc.		
SFE 1000P	Events Event Entry Community Description Type Time Owner Delete Add Events Log	Help Support Guide Logout

2. Click the **Add** button. The Add RMON Events Page opens:

Add RMON Events Page

SFE 1000	P	LINKSYS [®] A Division of Cisco Systems, Inc.
	Add RMON Events	
Event Entry	1	
Community	Default Community	
Description	Default Description	
Туре	None	
Owner		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The RMON event is added, and the device is updated.

Modify Event Control Settings

- 1. Click Statistics > RMON > Events. The RMON Events Page opens:
- 2. Click Edit. The Edit RMON Events Page opens:
Chapter

SFE1000P Gigabit Ethernet Switch Administration Guide



Edit RMON Events Page

SFE 1000P		LINKSYS A Division of Cisco Systems, Inc.
	Edit RMON Events	
Event Entry No.	1	
Community	Default Community	
Description	Default Description	
Туре	None	
Owner		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The event control settings are modified. and the device is updated.

Viewing the RMON Events Logs

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

- 1. Click Statistics > RMON > Events. The Events Log Page opens:
- 2. Click the Events Log button. The Events Log Page opens :

Events Log Page

SFE 1000P	Events	Help
■ System ■ Admin	Event Log No. Log Time Description	Support
	Rmon Events Control	Guide
Bridging Security Suite Quality of Service		

3. To return to the RMON Events Page, click the RMON Events Control button.

Defining RMON Alarms

The *RMON Alarms Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To set RMON alarms:

Chapter 17: Viewing Statistics Managing RMON Statistics

17

1. Click Statistics > RMON > Alarms. The RMON Alarms Page opens:

	RMOI	N Alarms Page	
Home - Microsoft Internet Explorer		_	
File Edit View Favorites Tools Help			🥂 🕺
Ġ Back 🝷 🕥 🖌 💌 💋 🐔 🔎 S	Search 🤺 Favorites 🚱 🔗 🕇	😓 🖻 - 📙 🗱 🦓 👘 👘	
Address 🕘 http://10.6.25.67/home.htm			💌 🄁 Go 🛛 Links » 📆 🗸
LINKSYS [®] A Division of Cisco Systems, Inc.			
SFE 1000P	Alarms		Help
System Admin Statistics Heneret RNON Statistics History Statistic Admin Statistics Ströging Sidging Source Quality of Service	Counter Name	a Interface Counter Value Sample Type	Rising Threshold Rising Event Support Guide Logout
Done	•		

2. Click the Add button. The Add RMON Alarm Page opens:

Add RMON Alarm Page

SFE 1000P		LINKSYS® A Division of Cisco Systems, Inc.
	Add RMON Alarm	
Alarm Entry	1	
Interface	Port e1 C 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		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The RMON alarm is added, and the device is updated.

Chapter

17

Modify RMON Alarm Settings

- 1. Click Statistics > RMON > Alarms. The RMON Alarms Page opens:
- 2. Click the Edit Button. The Edit RMON Alarms Page opens:

Edit RMON Alarms Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Edit RMON Alarm	
Alarm Entry	1 -	
Interface	Port e1 C LAG 1	
Counter Name	Total Bytes (Octets)- Receive 💌	
Counter Value	0	
Sample Type	Absolute 💌	
Rising Threshold	100	
Rising Event	1 - Default Description 💌	
Falling Threshold	20	
Falling Event	1 - Default Description 💌	
Startup Alarm	Rising and Falling 💌	
Interval (Sec)	100	
Owner		
	Apply	

- 3. Define the relevant fields.
- 4. Click Apply. The RMON alarms are modified, and the device is updated.

8

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 ٠
- 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.

To test cables:

1. Click Admin > Diagnostics > Copper Ports. The Copper Ports Page opens:

	Copper Ports Page	
Division of Cisco Systems, Inc.		
SEE 1000P	Copper Ports	Help
System	Port Test Result Cable Fault Distance Last lindate Cable Length	
Admin	e1 Test	Support
- en File Management - en Logs	e2 Test	Guide
Diagnostics	e3 Test	
Optical Test	e4 Test	Logout
Port Mirroring	e5 Test	
Statistics	e6 Test	
Security Suite	e7 Test	
Cuality of Service	e8 Test	
	g1 Test	
	g2 Test	C,

Connor Ports Page

2. Click the **Test** button to run the cable test. The results of the test appear.

18

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.

1. Click Admin > Diagnostics > Optical Test. The Optical Tests Page opens:

Optical Test Page

LINKSYS [®] A Division of Cisco Systems, Inc.							
SFE 1000P	Optical Test					ſ	Help
	Port Temperature	Voltage Current	Output Power	Input Power	Transmitter Fault	Lo	Support Guide Logout
						D	

2. Observe the output for any discrepancies.

Chapter

18

Configuring Port Mirroring

Port Mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as diagnostic tool and/or a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators configure port mirroring by selecting a specific port to copy all packets, and different ports from which the packets are copied.

To enable port mirroring:

1. Click Admin > Diagnostics > Port Mirroring. The Port Mirroring Page opens:

	YS [°] Iems, Inc.	LINKSYS [®] A Division of Cisco Systems, Inc.
Help Support Guide Logout	IOP Port Mirroring Imment Imment Ports Source Port Type Status Test Delete itization Add	SFE 1000P

Port Mirrorina Paae

2. Click the Add button. The Add Port Mirroring Page opens:

Add Port Mirroring Page

SFE 1000P		LINKSYS [®] A Division of Cisco Systems, Inc.
	Add Port Mirroring	
Source Port	e1 💌	
Туре	Tx Only	
Apply		

- 3. Define the relevant fields.
- 4. Click Apply. Port mirroring is added, and the device is updated.

Chapter

8

Modifying Port Mirroring

- 1. Click Admin > Diagnostics > Port Mirroring. The Port Mirroring Page opens:
- 2. Click the Edit Button. The Edit Port Mirroring Page opens:

SFE 1000P Edit Port Mirroring Page Edit Port Mirroring Source Port 1/e1 Type Tx Only • Apply

- 3. Define the relevant fields.
- 4. Click Apply. The Port mirroring is modified, and the device is updated.

Defining CPU Utilization

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

1. Click Admin > Diagnostics > CPU Utilization. The CPU Utilization Page opens

CPU Util	lization	Page
----------	----------	------

Support
Guide
Clck to activate and use this control

2. Click the appropriate pulldowns and observe the output.



Console Interface Configuration

Overview

The SFE1000P features a menu-driven console interface for basic configuration of the Switch and management of your network. The Switch can be configured using CLI through the console interface or through a telnet connection. This chapter describes console interface configuration. Configuration can also be performed through the web utility.

Configuring the HyperTerminal Application

Before you use the console interface, you will need to configure the HyperTerminal application on your PC.

1. Click the **Start** button. Select **Programs** and choose **Accessories**. Select **Communications**. Select **HyperTerminal** from the options listed in this menu.



Finding HyperTerminal

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



2. On the *Connection Description* screen, enter a name for this connection. In the example, the name of connection is SFE1000P. Select an icon for the application. Then, click the **OK** button.

Connection Description ? 🔀
New Connection
Enter a name and choose an icon for the connection:
Name:
SFE1000P
Icon:
冬 🗟 🗞 🗠 🖉
OK Cancel

Connection Description

3. On the *Connect To* screen, select a port to communicate with the Switch: **COM1**, **COM3**, or **TCP/IP**.

Connect To				
SFE1000P				
Enter details for the phone number that you want to dial:				
Country/region:	United States (1)			
Area code:	303			
Phone number:				
Connect using:	СОМЗ			
	OK Cancel			

Connect To Screen

A

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

4. Set the serial port settings as follows:

Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

COM3 Properties			? 🗙
Port Settings			
Bits per second:	38400	*	
Data bits:	8	~	
Parity:	None	*	
Stop bits:	1	*	
Flow control:	None	*	
	l	Restore Defa	ults
		ancel	Apply

Serial Port Settings

Then, click the **OK** button.



Connecting to the SFE1000P through a Telnet Session

- Open a command line editor and enter telnet <ip address of the device>. Then, press the Enter key.
- 2. The Login screen will now appear. The first time you open the command line interface, select **Edit** and hit Enter. Enter **admin** in the User Name field. Leave the Password field blank.

		Login Scre	en		
		User Name:			
		Password:			
ction->	Edit	Execute			
TAB/	BACK-Move	SPACE=Toggle	ENTER=Select	ESC=Back	

3. Press the **Esc** button and you will return to the login screen. Use the right arrow button to navigate to **Execute** and press the **Enter** button to enter the CLI interface.

B

Contacts

For additional information or troubleshooting help, refer to the User Guide on the CD-ROM. Additional support is also available by phone or online.

US/Canada Contacts

- 24-Hour Technical Support: 800-326-7114
- RMA (Return Merchandise Authorization): http://www.linksys.com/warranty
- Website: http://www.linksys.com
- FTP Site: ftp://ftp.linksys.com
- Support: http://www.linksys.com/support
- Sales Information: 800-546-5797 (800-LINKSYS)

EU Contacts

- Website: http://www.linksys.com/international
- Product Registration: http://www.linksys.com/registration

Warranty Information

LIMITED WARRANTY

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified for this product at www.linksys.com/warranty. The internet URL address and the web pages referred to herein may be updated by Linksys from time to time; the version in effect at the date of purchase shall apply.

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non.Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE

Appendix C: LIMITED WARRANTY SFE1000P 8-port 10/100 Ethernet Switch with PoE Administration Guide



LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact the Value Added Reseller (VAR) from whom you purchased the product or Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

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



Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at: www.linksys.com/support. This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623

Regulatory Information

This appendix includes the following regulatory statements:

- "Federal Communications Commission Interference Statement," on page 152
- "Industry Canada Statement," on page 152
- "Règlement d'Industry Canada," on page 153
- "EC Declaration of Conformity (Europe)," on page 153
- "User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)," on page 153

Federal Communications Commission Interference Statement

This product has been tested and complies with the specifications for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

Industry Canada Statement

This device complies with Industry Canada ICES-003 rule.

Operation is subject to the following two conditions:

This device may not cause interference and

This device must accept any interference, including interference that may cause undesired operation of the device.

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

Règlement d'Industry Canada

Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

Le fonctionnement est soumis aux conditions suivantes :

- Ce périphérique ne doit pas causer d'interférences;
- Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable..

EC Declaration of Conformity (Europe)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, and Amendment Directive 93/68/EEC, this product meets the requirements of the following standards:

- EN55022 Emission
- EN55024 Immunity

The following acknowledgements pertain to this software license.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



English - Environmental Information for Customers in the European Union



European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ върху изделието и/или опаковката му, да не се изхвърля т с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

Ceština (Czech) - Informace o ochranì _ivotního prostøedí pro zákazníky v zemích Evropské unie

Evropská smirnice 2002/96/ES zakazuje, aby zaøízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netøídiným komunálním odpadem. Tento symbol udává, _e daný produkt musí být likvidován oddileni od bì_ného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zaøízení prostøednictvím určených sbirných míst stanovených vládou nebo místními úøady. Správná likvidace a recyklace pomáhá pøedcházet potenciálním negativním dopadům na _ivotní prostøedí a lidské zdraví. Podrobnijší informace o likvidaci starého vybavení si laskavi vy_ádejte od místních úøadù, podniku zabývajícího se likvidací komunálních odpadù nebo obchodu, kde jste produkt zakoupili.

Dansk (Danish) - Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr. SFE1000P 8-port 10/100 Ethernet Switch with PoE Administration Guide



Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist , nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español (Spanish) - Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.



ξλληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français (French) - Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano (Italian) - Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

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



Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti (Maltese) - Informazzjoni Ambjentali ghal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-taghmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipali li ma giex isseparat. Is-simbolu jindika li dan il-prodott ghandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tieghek li tarmi dan it-taghmir u kull taghmir iehor ta' l-elettriku u elettroniku permezz ta' facilitajiet ta' gbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklagg jghin jipprevjeni konsegwenzi negattivi potenzjali ghall-ambjent u ghas-sahha tal-bniedem. Ghal aktar informazzjoni dettaljata dwar ir-rimi tat-taghmir antik tieghek, jekk joghgbok ikkuntattja lill-awtoritajiet lokali tieghek, is-servizzi ghar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

Magyar (Hungarian) - Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyûjtőredszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta. SFE1000P 8-port 10/100 Ethernet Switch with PoE Administration Guide



Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met nietgescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk (Norwegian) - Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/ eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte



as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol pe produs şi/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obișnuit. Este responsabilitatea dvs. să casați acest produs și alte echipamente electrice și electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea și reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului și a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubrizare sau magazinul de la care ați achiziționat produsul.

Slovenčina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenèina (Slovene) - Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embala_i – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo dr_avne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če _elite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/ tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen. SFE1000P 8-port 10/100 Ethernet Switch with PoE Administration Guide



Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.



Environmental Specifications

Dimensions	12.01"x1.73"x6.69" (305 mm x 44 mm x 170 mm)
Unit Weight	3.02 lbs. or 48.33 oz (1.37 kg)
Power	48 VDC, 100-240V 3.5A
Certification	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47), Class A EN60950 (2001)
Security	ACL, 802.1x
Operating Temp	0°C to 40°C (32°F to 104°F)
Storage Temp	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 90% relative humidity, Non-Condensing
Storage Humidity	10% to 95% relative humidity, Non-Condensing

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

Safety Information

The following statements are warnings or safety guidelines. A warning means danger. You are in a situation that could cause bodily injury. Before working on equipment, be aware of the hazards involved with electrical circuitry and standard safety practices to prevent accidents.

Meaning of the Warning Symbol



IMPORTANT SAFETY INSTRUCTIONS

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

General Safety Information



WARNING: Work During Lightning Activity

Do not work on the system or connect or disconnect cables during periods of lightning



WARNING: Installation Instructions

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



WARNING: SELV Circuit

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.



WARNING: Equipment Installation

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

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



WARNING: Local National Electrical Codes

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



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

Power Safety Information



WARNING: TN Power The device is designed to work with TN power systems.



WARNING: Warning Ground Conductor Warning Never defeat the ground conductor or operate the equipment in

the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.



WARNING: Power Supply Installation Warning

The power supply must be placed indoors.



WARNING: Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240 VAC, 10A international)



WARNING: Warning Main Disconnecting Device

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.



Software License Agreement

Software in Linksys Products:

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pt. Ltd. or Cisco-Linksys K.K. ("Linksys") contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at www.linksys.com/gpl or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from www.linksys.com/gpl. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: www.linksys.com/gpl/ or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Software Licenses:

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: www.linksys.com and www.linksys.com/gpl/ respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

Schedule 1 Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("LINKSYS") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL



PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

"Software" includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/ or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

Software Upgrades etc. If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

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



Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at http://www.linksys.com/gpl. If You would like a copy of the GPL or other open source code in this Software on a CD, Linksys will mail to You a CD with such code for \$9.99 plus the cost of shipping, upon request.

Term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

Disclaimer of Liabilities. IN NO EVENT WILL LINKSYS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

END OF SCHEDULE 1

Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at http://www.gnu.org/copyleft/gpl.html

GNU GENERAL PUBLIC LICENSE

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



Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the

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



Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

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



3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order,

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



agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND



PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at http://www.openssl.org/source/license.html

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"



4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
Appendix

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



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

END OF SCHEDULE 3



©2008 Cisco Systems, Inc. All rights reserved. Linksys is a registered trademark and the Linksys One logo is a trademark of Cisco Systems, Inc. March2008Rev1.0-CH

ıılıılı cısco.