

December 2007

CISCO SYSTEMS

© 2006-2007 Copyright 2006-2007 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	December 2007	Added switch stacking information.

# Contents

Chapter 1: Getting Started	1
Starting the Application	1
Understanding the Interface	4
Device Representation	5
Using the Linksys Management Buttons	6
Using Screen and Table Options	7
Adding Device Information	7
Modifying Device Information	7
Deleting Device Information	8
Resetting the Device	9
Logging Off The Device	9
Chapter 2: Managing Device Information	11
Understanding the Device Zoom View	11
Defining General System Information	12
SFE 2000P System Information	12
Managing Stacks	13
Building Automatically-Configured Stacks	14
Building a New Stack	14
Adding Units to a Running Stack	14
Building Manually-Configured Stacks	14
Building a New Stack	14
Adding Units to a Running Stack	14
Understanding Stack Resiliency	15
Understanding Advanced Stacking	15
Unit IDs	15
Stack Master	15
Stack Backup Master	15
Stack Members	16
Master-Enabled Units	16
Unit ID Allocation	16
Stack Unit Startup Process	17
Master Discovery Process	17
Master Election Process	17
Unit ID Allocation and Duplicate Unit ID Conflict Resolution	18
Configuring Units and Ports	19
Setting the Unit's Operational Mode	19
Configuring the Stack Master and Unit ID	19
Resetting the Unit to Factory Default Mode	21
Understanding LED Indicators	21
Stack Troubleshooting and Maintenance	21
Replacing a Failed Member Stack Unit in an Operational Stack	21
Replacing a Failed Stack Master Unit in an Operational Stack	23

Splitting a Stack	24
The Stack Master and Backup Master Units Remain in a Group	24
The Stack Master or the Backup Master Unit Remains in a Group	24
Neither the Stack Master Unit or the Backup Master Unit Remains in the Group	25
Merging Two Stacks	26
Understanding Stacking Cable Failure	27
Inserting Too Many Units into a Stack	27
Inserting a Standalone Unit into a Running Stack	28
Viewing Device Health	28
Chapter 3: Managing Power-over-Ethernet Devices	. 31
Defining PoE System Information	31
Chapter 4: Configuring Device Security	. 37
Passwords Management	38
Defining User Authentication	38
Defining Authentication	40
Defining Profiles	40
Mapping Profiles	42
Defining TACACS+	43
Defining RADIUS	47
Defining Access Method	51
Defining Access Profiles	51
Defining Profile Rules	54
Defining Traffic Control	60
Defining Storm Control	60
Defining Port Security	62
Defining 802.1x	66
Defining 802.1X Properties	67
Defining Port Authentication	68
Defining Multiple Hosts	71
Defining Authenticated Host	74
Defining Access Control	75
Defining MAC Based ACL	75
Defining IP Based ACL	77
Defining ACL Binding	84
Defining DOS Prevention	85
Global Settings	85
Defining Martian Addresses	87
Chapter 5: Configuring Device Interfaces	. 89
Defining Port Settings	89
Defining LAG Management	94
Defining LAG Settings	96
Configuring LACP	99

Chapter 6: Configuring VLANs	•	•		103
Defining VLAN Properties				104
Defining VLAN Membership				106
Defining Interface Settings				108
Configuring GVRP Settings				111
Protocol Group				114
Protocol Port				116
Chapter 7: Configuring IP Information	•	•		119
Domain Name System				120
Defining DNS Server				120
Host Mapping				122
Configuring Layer 2				124
Configuring IP Addressing:				124
IP Interface				124
ARP				125
Configuring Layer 3				129
Configuring IP Addressing				129
IP Interface				129
ARP Proxy				132
UDP Relay				133
DHCP Relay				136
ARP Defining IB Pouting				137 140
Defining IP Routing				140
Chapter 8: Defining Address Tables	•	•		143
Defining Static Addresses				144
Defining Dynamic Addresses				146
Chapter 9: Configuring Multicast Forwarding	•	•		149
IGMP Snooping				149
Defining Multicast Bridging Groups				152
Defining Multicast Forwarding				155
Chapter 10: Configuring Spanning Tree				157
Defining STP on Interfaces	•	•		158
Defining Interface Settings				160
Defining Rapid Spanning Tree				164
Defining Multiple Spanning Tree				168
Defining MSTP Properties				169
Instance to VLAN				170
Instance Settings				170
Interface Settings				171
Chapter 11: Configuring SNMP				177
SNMP v1 and v2	•	•	••	177
				1//
Contents				3

4

	SNMP v3	177
	Configuring SNMP Security	178
	Defining Engine ID	178
	Defining SNMP Views	179
	Defining SNMP Users	181
	Define SNMP Groups	183
	Defining SNMP Communities	185
	Defining Trap Management	189
	Defining Trap Settings	189
	Configuring Station Management	190
	Defining SNMP Filter Settings	196
Ch	apter 12: Configuring Quality of Service	199
	Defining General Settings	200
	Defining CoS	200
	Defining Queue	202
	Mapping CoS to Queue	202
	Mapping DSCP to Queue	201
	Configuring Bandwidth	205
	Defining Advanced Mode	203
	Configuring DSCP Mapping	208
	Defining Class Mapping	200
	Defining Aggregate Policer	211
	Configuring Policy Table	211
	Defining Policy Binding	217
	Defining QoS Basic Mode	219
Ch	apter 13: Managing System Files	221
	File Management Overview	221
	Firmware Upgrade	221
	Save Configuration	222
	Copy Files	223
	Active Image	224
Ch	apter 14: Managing System Logs	227
CII	Enabling System Logs	227
	Viewing the Device Memory Logs	229
	Clearing Message Logs	229
	Viewing the Flash Logs	22)
	Clearing Message Logs	230 230
	Viewing Remote Logs	230
Ch	apter 15: Configuring System Time	235
~ 11	Defining System Time	236
	Defining System Time Defining SNTP Settings	230
	Defining SNTP Authentication	238 240
		240

Chapter 16: Viewing Statistics	243
Viewing Ethernet Statistics	243
Defining Ethernet Interface	243
Resetting Interface Statistics Counters	245
Viewing Etherlike Statistics	245
Resetting Etherlike Statistics Counters	247
Viewing GVRP Statistics	247
Resetting GVRP Statistics Counters	249
Viewing EAP Statistics	249
Managing RMON Statistics	252
Viewing RMON Statistics	253
Resetting RMON Statistics Counters	254
Configuring RMON History	255
Defining RMON History Control	255
Viewing the RMON History Table	258
Configuring RMON Events	259
Defining RMON Events Control	259
Viewing the RMON Events Logs	262
Defining RMON Alarms	263
Chapter 17: Managing Device Diagnostics	269
Viewing Integrated Cable Tests	269
Performing Optical Tests	271
Configuring Port Mirroring	272
Defining CPU Utilization	275
Appendix A: Linksys One Contact Information	277

# Contents

1

# **Getting Started**

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

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

# **Starting the Application**

This section contains information for starting the Linksys User Interface.

**Note** By default, the IP address of the device is assigned dynamically. The IP address can be changed. It is recommended to configure the IP address statically, if the system is in stack mode, in order to prevent the user from disconnecting from the network in the event of master switchover.

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 Appendix 1, "Enter Network Password Page" opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

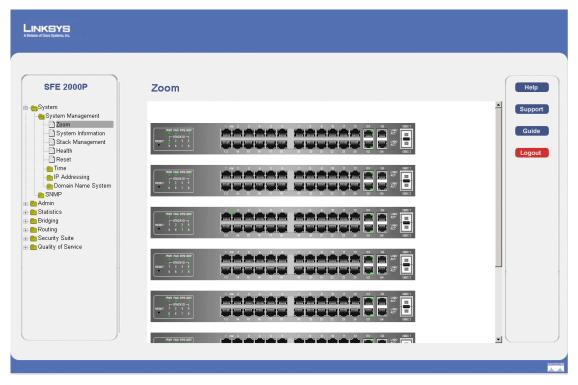
	Linei Periori Passion Page	
LINKSYS A Disease of Data Systems, bit.		
	User Name Password	
	Login Clear	

#### Enter Network Password Page

- 3. 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.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Embedded Web System Home Page



1

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

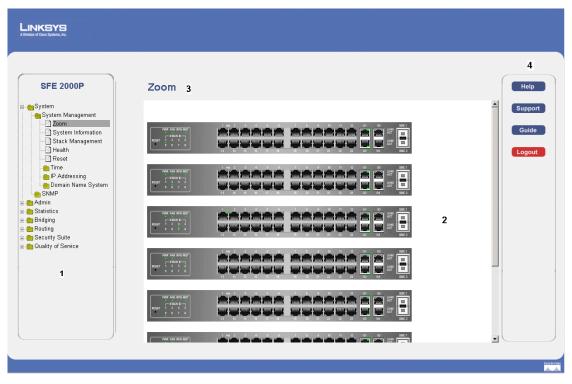
# **Understanding the Interface**

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.

#### Linksys User Interface Components



1

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:

PVR FAN RPS NST 	
PAR FAN RPS NST 	
PARE FAIL RPS MET 	
PARE FAN RPS MOT 	
PAR FAN RPS NOT 	
PVR FAN APS NST 	

**Device Representation** 

The Linksys home page contains a graphical SFE2000 and SFE2000P front panel illustration.

1

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# Using the Linksys Management Buttons

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

#### **Device Management Buttons**

Button Name	Button	Description
Apply	Apply	Applies changes to the device.
Clear All 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 the settings of Selected Port to Default	Reset	Resets the settlings of a selected port to the default settings
Test Now	Test	Performs cable tests.

1

# **Using Screen and Table Options**

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

- Appendix 1, "Adding Device Information"
- Appendix 1, "Modifying Device Information"
- Appendix 1, "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

SGE 2000		LINKSYS A Diseber of Disco Systems, Inc.
	Add SNTP Server	
SNTP Server		
🔲 Enable Poll Interval		
Encryption Key ID	V	
	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:

#### Edit Interface Priority



- 4. 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:

Reset Page

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

SGE 2000	Reset Reset the device by selecting Reset'. Reset Unit No.	Help Support
System Information     Stack Management     Health     Reset     Dradoressing     Domain Name System     SNMP     SNMP     Statistics     Bridging     Routing     Scurity Suite	Reset	Guide
Quality of Service		

- 2. Click the **Reset** button. Each unit can be reset individually. Resetting the stack master results in resetting the entire stack. If the master unit is reset, 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 stack is not part of a full Linksys One system. If the stack is part of a Linksys One system, login is automatically done from the Service Router.

# **Logging Off The Device**

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

1

# **Managing Device Information**

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

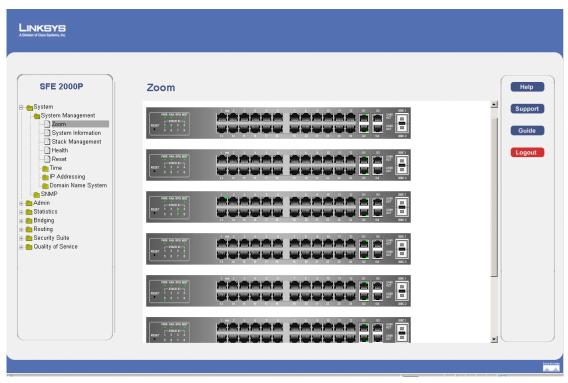
- Understanding the Device Zoom View
- Defining General System Information
- Managing Stacks

# **Understanding the Device Zoom View**

The *Zoom Page* is the main window used for viewing the devices either in stand-alone mode or operating in a stack. To open the Zoom Page:

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

Zoom Page



The Zoom Page contains the following port indicators:

- Green Indicates the port is currently operating.
- Red indicates the port is not currently operating.

Chapter 2:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Defining General System Information**

### **SFE 2000P System Information**

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

SFE 2000P	System Informatio	n	Help
SFE 2000P	Model Name System Name System Location System Contact System Object ID System Up Time Base MAC Address Hardware Version Software Version Boot Version Switch Operation Mode After Res	24-port 10/100 Ethernet Switch with PoE	Support Guide Logout
	Арріу		-

#### SFE 2000P System Information Page

The System Information page contains the following fields:

- Model Name Displays the user defined user name.
- System Name Displays the user configured name of the system. Configured in the Network page.
- System Location Defines the location where the system is currently running. The field range is up-to 0-160 Characters.
- System Contact Defines the name of the contact person. The field range is up to 0-160 Characters.
- System Object ID— Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- System Up Time Displays the amount of time that has elapsed since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example: 41 days, 2 hours, 22 minutes and 15 seconds.



- **Base MAC Address** Displays the device MAC address. If the system is in stack mode, the Base MAC Address of the master unit is displayed.
- **Hardware Version** Displays the hardware version number. If the system is in stack mode, the hardware version of the master unit is displayed.
- Software Version Displays the software version number. If the system is in stack mode, the version of the master unit is displayed.
- **Boot Version** Indicates the system boot version currently running on the device. If the system is in stack mode, the version of the master unit is displayed.
- Switch Operation Mode After Reset Indicates the mode the device operates in after the system is reset. A switch may operate in one of two modes: stack or standalone. Either mode is selected by the user during software boot or in the web interface's System Information page. The new mode takes effect after the unit is reset. The factory default is stack mode. The possible field values are:
  - Standalone Indicates the device operates as a Standalone device after the system is reset.
     A switch operating in standalone mode runs as an independent, single unit. All ports of a standalone switch operate as normal Ethernet links. A standalone switch does not participate in a stack even if physically connected to a stack.
  - Stack Indicates the device operates as a Stacked unit after the system is reset. A switch operating in stack mode is not an independent unit, but a member of an organized group of switches known as a stack. A stack consists of one Stack Master control switch, one Master Backup switch and up to six Stack Member switches. In some cases, a unit in stack mode that is not connected to any other units may operate as a "stack–of-one."
- 2. Define the relevant fields.
- 3. Click Apply. The system information is defined, and the device is updated.

# **Managing Stacks**

Stacking allows you to build a switch with many more ports than would be available in a single unit. The stack is managed by one of the units (called the Stack Master) and all of the other units serve as ports only.

You can build stacks by building a new stack from a group of switches, or adding new units to an existing stack. Stacks can be automatically or manually configured.



**NOTE:** Two ports of each unit in a stack mode (ports 12 and 24 on GE units, and ports G1 and G2 on FE units) are reserved for stacking links, and cannot be used for regular network connections.



# **Building Automatically-Configured Stacks**

### **Building a New Stack**

The easiest way to build a stack is to use a group of switches, each of which is in factory default mode:



**NOTE:** If the units to be used in building the new stack have been used previously, we recommend that you reset them to the factory default by holding the reset button for at least 10 seconds before using them.

- 1. Connect the units physically through the stacking ports, using standard Ethernet cables.
- Power the units on. After a short interval the stack becomes operational, with one of the units selected as the Stack Master. The unit selected as Stack Master is indicated by a lit green "MST" LED on its front panel. If a serial console connection is desired, the serial cable should be connected to the console port of the unit serving as the Stack Master.

# Adding Units to a Running Stack

- 1. Reset the units that will be added by restoring them to the factory default mode. Connect the units physically to the stack.
- 2. Power the units on. After a short interval, they will become members of the stack.

# **Building Manually-Configured Stacks**

You can manually configure stacks, including choosing a specific unit as the Stack Master. You must assign a unique Unit ID (from 1 to 8) to each stack member.

# **Building a New Stack**

- 1. Reset all relevant units to by restoring them to the factory default mode.
- 2. Connect the units physically through the stacking ports, using standard Ethernet cables.
- 3. Assign each unit its desired number, making sure no duplicates exist, and reset the stack.

# Adding Units to a Running Stack

- 1. Reset the units to be added by restoring them to the factory default mode.
- 2. Connect the units physically to the stack.



- 3. Power the units on. After a short interval, they will become stack members, but will have automatically-assigned Unit IDs. Assign each such unit its desired Unit ID (using the Stack Management Interface through the console port, by Telnet, or by using the graphical user interface (GUI).
- 4. Reset the units to make this assignment permanent.



**NOTE:** We recommended that if you manually assign a Unit ID to one unit, you manually assign Unit IDs to all units. Using a mix of both system-assigned and manuallyassigned IDs in your network can impact system performance.

The unit that is assigned the Unit ID 1 is the Stack Master, and its front panel "MST" LED lights green. The unit assigned the Unit ID 2 is the Backup Master.

# **Understanding Stack Resiliency**

Stacks can be configured in ring or chain topologies. We recommend configuring the stack in ring topology, due to the high resiliency in case of unit failure or stacking links failure.

Additionally, if a redundant power supply is present, we recommend connecting the Stack Master and Backup Master units to the redundant power supply.

# **Understanding Advanced Stacking**

To understand advanced stacking, you must understand Unit IDs and how they are allocated, and the stack unit startup process.

### Unit IDs

Each unit in a stack has an assigned unique Unit ID number. The following sections describe the Unit IDs and their characteristics.

#### **Stack Master**

The unit assigned the Unit ID number 1 serves as the Stack Master. All other units are stack members. The Stack Master provides a single point of control, configuration and management for the entire stack, and stores the configuration for all stack members. (Members do not store any configuration information.)

#### **Stack Backup Master**

The unit assigned the Unit ID number 2 is a special stack member that serves as the stack Backup Master. A stack Backup Master assumes the role of Stack Master for the remaining stack members if the stack Master fails or is disconnected.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

The Stack Master stores a copy of the active configuration on the Backup Master. This copy is used only if the Backup Master assumes the role of Stack Master.



**NOTE:** Only the configuration file is copied. Any dynamically-filled tables (for example, learned addresses) are not copied from the Stack Master to the Backup Master. If the Backup Master assumes the role of Stack Master, it builds its own dynamic tables.

#### **Stack Members**

The units assigned the Unit IDs 3 through 8 are called stack members. A stack member operates only as a member of the stack under the direction of an operational Stack Master (or a Backup Master that has assumed the Stack Master role). Stack members are not directly manageable and configurable, and must be managed through the Stack Master. They do not contain any meaningful configuration information, including their own configuration. If an operational Stack Master is not present and reachable, these units are not functional.

#### **Master-Enabled Units**

Units that are assigned a Unit ID number of 1 or 2 are called master-enabled units. Only master-enabled units participate in the Master Election process (see below) when they are initialized, are inserted into a new stack, or lose connectivity with the existing Stack Master. Only master-enabled units participate in the Master Election process and can become the Stack Master or Backup Master. (Units that are assigned a Unit ID of 3 through 8 can only become a Stack Master or a Backup Master if they are manually configured by the system administrator or if they are reset to the factory default mode.)

#### **Unit ID Allocation**

Units are shipped from the factory without an assigned Unit ID, and must be assigned a unique Unit ID before they can operate as part of a stack. Unit ID numbers are assigned to units in one of two ways:

- Unit ID numbers are assigned by the system administrator, and can be changed only manually by the system administrator.
- Unit ID numbers are allocated to a stack member unit by the Stack Master during system initialization.

A unit that was assigned a Unit ID will usually keep this number even after it is rebooted. The Stack Master may reallocate Unit IDs during system initialization to resolve duplicate Unit ID conflicts (see below). Manually assigned Unit IDs cannot be changed by the Stack Master, even if there is a conflict.

Unit ID assignment or change takes effect only during system initialization and does not take place during system runtime. Units of a stack do not have to be numbered in sequence, and can be interconnected as long as each unit has a unique ID and at least one unit of the stack serves as Stack Master.

### **Stack Unit Startup Process**

When a unit in stack mode is initialized (powered up or rebooted), it goes through the following steps:

- 1. The Master Discovery and Master Election processes.
- 2. Unit ID allocation by the Stack Master (including duplicate Unit ID conflict resolution).
- 3. Unit and port configuration by the Stack Master.

#### **Master Discovery Process**

When a unit in stack mode initializes, its behavior depends on its Unit ID (if one is configured):

- If the unit does not have a current Unit ID (that is, the unit is in factory default mode) and if there is a Stack Master, the unit is allocated a Unit ID number from the Stack Master. If there is no Stack Master, then the unit participates in the Master Election process, and may be chosen as the new Stack Master or Backup Master.
- If the unit's current Unit ID is 1 or 2 (that was previously allocated, even if used in a different stack), then the unit participates in the Master Election process.
- If the unit has a current Unit ID (that was previously allocated, even if used in a different stack), the unit tries to act according to its Unit ID number in the new stack. For example, if the unit's current Unit ID is 3 through 8, it will try to connect to the running Stack Master, and will not proceed to the next stage until contact with the Stack Master is made. These units will not participate in the Master Election process, and if no Stack Master is present, the units are effectively shut down.

The Stack Master and all other stack units carry out a continuous process of Master Discovery by frequently exchanging stack control messages. This allows units to know if another unit fails or becomes unreachable.

#### **Master Election Process**

When units in stacking mode initialize, one of the units is elected as the Stack Master. If a unit in the stack was set to "Force Master" by the system administrator, that unit is elected as the Stack Master. Only master-enabled stack units (for example, those with the Unit ID of 1 or 2) can be configured as "Force Master."

If the stack contains units whose unique Unit ID is 1 or 2, then one of these two units will be the Stack Master. It does not matter if the Unit ID was originally assigned automatically or manually. These units are called master-enabled units. If there is only one master-enabled unit, it will be elected as the Stack Master (even if its Unit ID is 2).

If there are two master-enabled units, the two units decide which of them is the Master by checking which one has been running for a longer time (in intervals of 10 minutes). The unit that has been running for the longer time will be the Stack Master. If they have been running for the same amount of time, the unit with the Unit ID of 1 will be the Stack Master. If both units have been running for the same amount of time and both units have the same Unit ID, the unit with a lower MAC (hardware) address will be selected as the Stack Master.

Chapter 2:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

If the stack contains one or more units without a current Unit ID (the units are in factory default mode), then one of these units will be the Stack Master. The unit selected to be the Stack Master is the one running for the longest time (in intervals of 10 minutes), or, if all units are running for the same amount of time, the one with the lowest MAC (hardware) address.

The Master Election process ensures that the stack has a Stack Master. The Stack Master has the Unit ID of 1 and the Backup Master, if it exists, has the Unit ID of 2. Alternatively, the Stack Master has the Unit ID of 2 and the Backup Master, if it exists, has the unit ID of 1.

If a master-enabled unit is added to a stack and powered on, when it comes up it invokes the Master Election process, even though the rest of the stack already has an elected master. Because the unit is new, it loses the election and joins as a stack member or Backup Master.

#### Unit ID Allocation and Duplicate Unit ID Conflict Resolution

After a Stack Master is elected, it allocates Unit IDs to units that do not have a currently assigned Unit ID (units that are in factory default mode). The Stack Master also attempts to resolve all cases of units with duplicate Unit IDs. The Stack Master changes the Unit IDs of units that have a duplicate current Unit ID, provided that there are available, unused Unit IDs. In a merged stack, if the Stack Master unit remains as the Stack Master, units that were in its group will keep their unit IDs. Members of other groups are renumbered.

If the conflict occurs after the units reboot, the conflict is resolved as follows:

- If both duplicate units are in auto (self ordering) mode, then the unit ID with the lower MAC (hardware) address will keep its unit ID. The other unit is assigned a new unit ID.
- If one of the duplicates is in auto (self ordering) mode, and the other unit is in manual mode, then the manual mode unit will keep its ID and the other is assigned a new unit ID.
- If both duplicate units are in manual mode, then both of them are shut down.

If the Stack Master is able to allocate a unique Unit ID to each unit, then all units can operate as a stack. If the Stack Master is unable to allocate a Unit ID to a unit, that unit is effectively shut down and will not participate in the stack. For example, units with a conflicting manually-set Unit ID number are shut down because the Stack Master cannot override the system administrator's assignment and resolve the conflict.

If there are more units than the maximum number allowed in a stack, and the incoming units are already in factory default mode (they do not have unit ID assigned), then a Stack Master is elected following the Master Discovery and Master Election processes. All other units remain shut down.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



Occasionally, due to a race condition during the boot process, some of the units might be connected and join the stack. If the incoming units already have a unit ID, then none of them will join the stack and all are left in shutdown mode because there is no way for the Stack Master to determine their Unit ID preference.



**NOTE:** If a unit is shut down, its stacking links are inactive. If the stacking units are connected in a chain topology, the shutdown of one unit breaks the chain and can cause other units to be shut down if they have no active link to the Stack Master unit.

# **Configuring Units and Ports**

After the Master Discovery and Master Election processes, each unit in the stack has a unique Unit ID, one of the units is the Stack Master, and one of the units may serve as the Backup Master. The Stack Master then configures each of the member units and its ports according to the configuration file present on the Stack Master. If the stack has a Backup Master, the configuration file is copied to the Backup Master.

After all the units and ports are configured, the stack enters normal operational mode. If a change is made to the system configuration, the change is stored by the Stack Master and is copied to the Backup Master if one exists.

You can use the command-line interface (CLI) or GUI to configure the stack units.

# Setting the Unit's Operational Mode

Use the GUI to set the unit's operational mode to standalone or stack. This configuration takes effect after the next reboot.

# Configuring the Stack Master and Unit ID

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

To open the Stack Management Page:

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

2

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Stack Management Page

LINKSYS A Divisor of Occo Systems, Inc.		
SGE 2000 System System Management System Information System Information Stack Management Health Reset Time Domain Name System SNMP Statistics Berdinin Statistics Berdinin Statistics Berdinin SumP	Stack Management Master Election Stacking Ports After Reser Unit No. Unit No. After Reset Apply	Help Support Guide Logout
		Class System

The Stack Management Page contains the following fields:

- Master Election Indicates the method of electing the Stack Master device. The possible values are:
  - Automatically The master is selected automatically by software.
  - *Force Master* The unit is forced to be master of the stack. Note that only units with the Unit ID of 1 or 2 can be the stack master.
- Stacking Ports After Reset Allows the user to decide what cable type is in use. The possible values are:
  - Combo Ports -- Indicates that the combo port is used as the stacking port.
  - Copper Ports Indicates that the copper port is used as the stacking port.
- Unit No.— Displays the current Stacking Master.
- Unit No. After Reset Indicates the stacking member elected Stacking Master after the device is reset.
- 2. Define the relevant fields.
- 3. Click Apply. Stack management is defined, and the device is updated.

2

# **Resetting the Unit to Factory Default Mode**

To reset the unit to the factory default settings, press the front panel RESET button (see Figure 3.) The unit is set to Stack mode with a Unit ID of 0.

				GBIC 1
FWR FAN RPS MST		State state state state state		LINK/
-STACK D		Allering Restory Restory Restory Restory	Rent Rent	
	Sound Sound Sound Sound Sound Sound	From a former and a source and a source		ACT
				GRIC 2

### **Understanding LED Indicators**

Each unit contains a Master LED indicator and eight unit LEDs. The LED status definitions are shown in the table below.

LED	Mode	Color	Description
Master	Solid	Green	The switch is the Stack Master.
	Off	N/A	The switch is not the Stack Master or the switch is not stacked.
ID n	Solid	Green	The switch is Unit ID <i>n</i> .
	Off	N/A	The switch is not Unit ID $n$ or the switch is not stacked.
All ports	Solid	Red	The switch is powered on, but not operational.

# **Stack Troubleshooting and Maintenance**

### **Replacing a Failed Member Stack Unit in an Operational Stack**

If a unit that is not the Stack Master fails in an operational stack, the Stack Master discovers that the unit is no longer responding during the Master Discovery process. The Stack Master directs all other stack members to route unit-to-unit traffic around the failed unit using the ring topology of the stacking connections. Concurrently, the Stack Master notifies the system administrator of the failure by sending SYSLOG messages and SNMP traps.

Because all traffic has been routed around the failed unit, when it is disconnected from the stack, the stack continues to run as long as all other stacking connections are left intact.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

When a new unit is inserted in the stack and powered on, the following occurs:

- 1. The incoming unit, which is in stack mode, performs the Master Discovery process, and may participate in the Master Election process.
  - If the incoming unit has a Unit ID of 1 or 2 (it is a master-enabled unit) it initiates the Master Election process. However, because the running Stack Master has a longer runtime, the current Stack Master retains its position and the incoming unit does not become the new Stack Master.
  - If the incoming unit has a Unit ID of 3 through 8, it attempts to become a member unit of the stack, subject to control by the already running Stack Master, and the Master Election process does not occur.
- 2. The Stack Master performs Unit ID allocation and the conflict resolution process.
  - If the incoming unit did not have an assigned Unit ID (that is, it is in factory default mode), it is assigned the lowest available Unit ID by the Stack Master. We recommend that you use the automatically-assigned unit ID mode because it provides better resiliency to the stack.
  - If the incoming unit already has an assigned Unit ID, and that Unit ID is unused in the current stack, the incoming unit keeps its assigned Unit ID and the Stack Master applies any configuration relevant to that Unit ID to the incoming unit.
  - If the incoming unit already has an assigned Unit ID, and that Unit ID conflicts with a unit ID in the current stack, the Stack Master allocates a new Unit ID to the incoming unit, giving it the lowest available Unit ID. However, if the incoming unit has a manually assigned Unit ID, the Stack Master cannot change it. If the incoming unit cannot be assigned an available Unit ID, then it is shut down and is not joined to the stack.
- 3. The Stack Master performs unit and port configuration for the incoming unit.
  - Any configuration information that is relevant to the number assigned to the incoming unit is applied by the Stack Master. For example, if the incoming unit is assigned the same Unit ID of the unit it replaced, then when possible, it receives the same configuration as the failed unit.
  - If the incoming unit is identical to the replaced unit, the entire configuration of the replaced unit is applied to the incoming unit and the stack returns to the state it was in before unit failure.

If the incoming unit is not identical to the unit that failed, the Stack Master applies the configuration in the following manner:

• If a 24-port unit replaces a failed 48-port unit, the ports of the incoming unit are configured according to the configuration of the first 24 ports of the failed unit.



**NOTE:** The configuration of all 48 ports of the failed unit is kept in memory, even though the first 24 are currently applied. If, in the future, a 48 port unit is inserted and assigned the same Unit ID, it is configured the same as the original failed 48-port unit.



- If a 48-port unit replaces a 24-port unit, then the first 24 ports of the incoming unit are configured according to configuration of the ports of the failed unit. The remaining ports of the incoming are configured according to the default settings.
- If the units have uplink ports, then the first uplink port of the incoming unit is configured according to the configuration of the first uplink port of the failed unit.

### **Replacing a Failed Stack Master Unit in an Operational Stack**

When the Stack Master unit fails, the stack Backup Master, using the Master Discovery process, discovers that the Stack Master unit no longer responds. The Backup Master takes over as the Stack Master. The Backup Master (now the Stack Master) directs all other stack members to route unit-to-unit traffic around the failed unit using the ring topology of the stacking connections. Concurrently, the Backup Master notifies the system administrator of the failure by sending SYSLOG messages and SNMP traps.

Because all traffic has been routed around the failed unit, when it is disconnected from the stack, the stack continues to run as long as all other stacking connections are left intact.

When a new unit is inserted in the stack and powered on, the following occurs:

- 1. The incoming unit, which is in stack mode, performs the Master Discovery process, and may participate in the Master Election process.
  - If the incoming unit has a Unit ID of 1 or 2 (it is a master-enabled unit) it initiates the Master Election process. However, because the running stack Backup Master has a longer runtime (if it has been running for more than 10 minutes) it remains the Stack Master and the incoming unit does not become the new Stack Master. This can cause an incoming unit with a Unit ID of 1 to serve as the stack Backup Master, while the current unit with the Unit ID of 2 remains the active Stack Master.
- 2. The Stack Master performs Unit ID allocation and the conflict resolution process.
  - If the incoming unit did not have an assigned Unit ID (that is, it is in factory default mode), it is assigned the lowest available Unit ID by the Stack Master. We recommend that you use the automatically-assigned unit ID mode because it provides better resiliency to the stack.
  - If the incoming unit already has an assigned Unit ID, and that Unit ID is unused in the current stack, the incoming unit keeps its assigned Unit ID and the Stack Master applies any configuration relevant to that Unit ID to the incoming unit.
  - If the incoming unit already has an assigned Unit ID, and that Unit ID conflicts with a unit ID in the current stack, the Stack Master allocates a new Unit ID to the incoming unit, giving it the lowest available Unit ID. However, if the incoming unit has a manually assigned Unit ID, the Stack Master cannot change it. If the incoming unit cannot be assigned an available Unit ID, then it is shut down and is not joined to the stack.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- 3. The Stack Master performs unit and port configuration for the incoming unit.
  - Any configuration information that is relevant to the number assigned to the incoming unit is applied by the Stack Master. For example, if the incoming unit is assigned the same Unit ID of the unit it replaced, then when possible, it receives the same configuration as the failed unit.
  - If the incoming unit is identical to the replaced unit, the entire configuration of the replaced unit is applied to the incoming unit and the stack returns to the state it was in before unit failure.

### **Splitting a Stack**

A working stack can be split into two groups, either by failure of a stacking link connecting two units in the stack, or by a failed unit in a chain topology that causes disconnection between two units in the stack. In this case, each group is considered as an independent running stack configuration. For each group, there are three scenarios.

#### The Stack Master and Backup Master Units Remain in a Group

In this scenario, the Stack Master routes around the missing units. The Master Discovery, Master Election and Unit ID Allocation & Duplicate Unit ID Conflict Resolution processes occur with the following results:

- Any configuration information contained in the Stack Master that is relevant to the units which remained in the split group remains unchanged.
- Topology information (the information for each unit on how to send traffic to any other unit in the stack) managed by the Stack Master includes only units that are reachable (connected) following the split.
- The split stack continues to work as it previously did, but with fewer units.
  - No unit ID changes are performed in each of the split stacks.
  - The Stack Master notifies the system administrator of the removed units and ports that belong to the unreachable units by sending SYSLOG messages and SNMP traps. They are reported as "not present."

#### The Stack Master or the Backup Master Unit Remains in a Group

If the Stack Master unit remains in the group, the scenario described in "Replacing a Failed Member Stack Unit in an Operational Stack" applies. If the Backup Master unit remains in the group, the scenario described in "Replacing a Failed Stack Master Unit in an Operational Stack" applies.



**NOTE:** If the stack is split in two groups, one with the Stack Master and one with the Backup Master, both groups will function.



The Master Discovery, Master Election and Unit ID Allocation & Duplicate Unit ID Conflict Resolution processes occur with the following results:

- If the Stack Master unit remains in the split stack, the Stack Master discovers (using the Master Discovery process) that the Master Backup unit no longer responds. The Stack Master notifies the system administrator (using SYSLOG messages and SNMP traps) of the removed units and ports that belong to the unreachable units and they are reported as "not present."
- If the Backup Master unit remains in the split stack, the Backup Master determines this as a case of Stack Master failure and takes over and manages the remaining units as a stack while keeping its previous Unit ID number. Because the Backup Master was not acting as a master prior to the split, it initiates a topology database and ports learning process. Traffic might be halted for a short period of time until synchronization (unit and port configuration) is completed. New units discovered by the Backup Master notify the system administrator (using SYSLOG messages and SNMP traps).
- The partial stacks both continue to work as they did previously, but with fewer units.
- No unit ID changes are performed in each of the partial stacks.
- If each part of the stack has a Stack Master (for example, one contains the original Stack Master, and one contains the Backup Master), and are operating as two separate stacks, both Stack Masters contain the same configuration and use the same IP address.



**CAUTION:** If both Stack Masters use the same IP Address, problems can occur on the network, because users cannot connect to one of the stacks through its IP address.

#### Neither the Stack Master Unit or the Backup Master Unit Remains in the Group

This scenario is the same as that of a failed Stack Master where no Backup Master is available. The following concepts apply:

- Units whose ID numbers are 3 through 8 in this part of the original stack will not renumber themselves, and will remain shut down until a master-enabled unit is connected and begins to operate as the Stack Master. The Master Discovery process discovers that the Stack Master has failed.
- In this group, the units lose connection with the Stack Master. Since they began as a running stack and none of them are in factory default mode, renumbering does not occur, and even a reset of the units will not affect unit ID assignment, because units can be renumbered only by a Stack Master.
- No unit ID changes are performed in each one of the two groups.



**NOTE:** None of the units in either group will renumber themselves.

Chapter 2:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Merging Two Stacks**

To merge two working stacks and create one stack, first decide if you will merge the stacks while the incoming units are powered off during insertion, or if both stacks will be running when merged.

If the incoming units are powered off, follow the procedures described in "Building a New Stack" in the "Building Automatically-Configured Stacks" or "Building Manually-Configured Stacks" sections. Repeat the process for each unit inserted into the stack.

If both stacks to be merged are running (for example, you are connecting the stacking cables of two stacks), the following occurs:

- If each of the joined stacks has a Stack Master unit, both Stack Master units perform the Master Discovery process and participate in the Master Election process. One of the Stack Master units is selected as the Stack Master unit for the merged stack. The criteria for choosing the Stack Master are as follows:
  - Force Master: If Force Master is enabled, the unit that is configured as the forced unit is selected as the Stack Master.
  - System Up Time: Up time is measured by quantities of 10-minute intervals. If the number of 10 minute intervals is higher for one of the units, this unit is selected as the Stack Master.
  - Lowest Unit ID: If both units have the same up time (measured in intervals of 10 minutes), the unit with the lowest unit ID is selected as the Stack Master.
  - Lowest MAC: If both Master unit ID numbers are equal, the unit with the Lower MAC address is chosen as the Stack Master.

The Stack Master unit that loses its "mastership" in the Master Election process is renumbered if the unit ID was dynamically allocated. The new Stack Master allocates it a new number and configures it as a stack member or a Backup Master. It will be shut down if the unit ID was manually allocated. We recommend that the administrator configure the unit to receive an auto-assigned Unit ID before reconnecting it to the stack.



**NOTE:** There will never be two units with the same Unit ID at the end of the merge.

When two stacks are combined, all of the configuration information for one of the stacks is lost. Only the surviving Stack Master (after the discovery and election processes are complete) maintains its configuration information.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



We recommend that when combining two stacks, you reset the switches in one stack to factory default mode and then add the switches as described in "Adding Units to a Running Stack" in the "Building Automatically-Configured Stacks" section.

• If one of the merged stacks had neither a Stack Master unit nor a Backup Master unit, then units belonging to this group are inserted into the stack as described in "Replacing a Failed Member Stack Unit in an Operational Stack." The Master either connects the running units to the stack using the current Unit ID numbers or renumbers them.



**NOTE:** Any time two stacks are combined into one stack, there is no way to maintain the configuration for both sets of switches. All dynamic information of the units that belong to the portion of the stack that was not re-elected to be the Stack Master is relearned.

### **Understanding Stacking Cable Failure**

If the stacking connection cables fail and cause a stack split, the scenario described in "Merging Two Stacks" applies. This occurs only if the stack uses a chain topology. Single stacking cable failure will not cause a stack split if a ring topology is used.

### **Inserting Too Many Units into a Stack**

If you try to insert too many units into a stack, when all units (existing and newly inserted) are powered on at the same time, the following occurs:

- 1. A Stack Master is elected following the Master Discovery and Master Election processes.
- 2. All other units are shut down.



**NOTE:** Occasionally, due to a race condition during the boot process, some of the units might be connected and join the stack.

When a running group of units is added to an existing stack and each one of the stack groups has an elected Stack Master, and the total of existing units and inserted units exceeds the maximum allowed number of units (8) in a stack:

- The Master Detection and Master Election processes determine the Stack Master out of one of the two combined stacking groups.
- When switches are added to a running stack, the Unit ID Allocation and Duplicate ID conflict resolution processes detect an error if too many switches are present in the stack, and no changes are made to units that originally belonged to the group managed by the newly-elected Stack Master. The original switches retain their ID assignments and configurations. The units that originally belonged to the group managed by the Stack Master that lost its "mastership" are shut down.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

### Inserting a Standalone Unit into a Running Stack

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

If a unit is in standalone mode, it will not participate in the Master Discovery process (it will not look for a Stack Master and will not respond to master queries). As a result, it will not join the stack but will continue to run as a standalone unit. The ports that are connected to the other units' stacking links will not pass any traffic, and the Stack Master will consider them as failed stacking links and route all traffic around them.

# **Viewing Device Health**

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

SFE 2000P	Health	1							ſ	Help
System	Unit No.	Powe	r Supply Status	Fan S	tatus				4	Suppor
- en System Management 	Unit HU.		RPS			Fan3	Fan4	Fan5		
	1		Not Present	ОK		ОК	OK	OK		Guide
		PS	RPS	Fan1	Fan2	Fan3	Fan4	Fan5		Logout
- Time	2	OK	Not Present	ОK	OK	ОK	ОK	OK		
Domain Name System	3	PS	RPS	Fan1	Fan2	Fan3	Fan4	Fan5		
Admin     Admin     Statistics     Bridging     Routing     Security Suite     Quality of Service	3	OK	Not Present	ОK	ΟK	Not Present	Not Present	Not Present		
	4	PS	RPS	Fan1	Fan2	Fan3	Fan4	Fan5		
	4	OK	Not Present	ΟK	OK	ОК	OK	OK		
	5	PS	RPS	Fan1	Fan2	Fan3	Fan4	Fan5		
		OK	Not Present	ОK	OK	ОК	OK	OK		
	6	PS	RPS	Fan1	Fan2	Fan3	Fan4	Fan5		
		OK	Not Present	OK	OK	OK	OK	OK		
	7		RPS	Fan1	Fan2	Fan3	Fan4	Fan5		
	'	OK	Not Present	ОK	ΟK	Not Present	Not Present	Not Present		

#### Health Page

The *Health Page* contains the following fields:

- Unit No. Indicates the unit number for which the device information is displayed.
- **Power Supply Status** The power supply status. Power supply 1 is displayed as PS1 in the interface, while the redundant power supply is displayed as RPS.



- **Fan Status** The fan status. The device has five fans. Each fan is denoted as fan plus the fan number in the interface. The possible field values are:
  - OK The fan is operating normally.

•

- Fail — The fan is not operating normally.

2

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

3

## **Managing Power-over-Ethernet Devices**

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources.

Power-over-Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- PDAs
- Audio and video remote monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports. Guard Band protects the device from exceeding the maximum power level. For example, if 400W is maximum power level, and the Guard Band is 20W, if the total system power consumption exceeds 380W no additional PoE components can be added. The accumulated PoE components power consumption is rounded down for display purposes, therefore remove value after decimal point.



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

## **Defining PoE System Information**

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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### PoE Settings Page

#### LINKSYS A Division of Cisco Systems, Inc.

SFE 2000P	PoE	Settings	3					Help
System Admin Statistics				U	nit No. 1	×		Support Guide
Bridging Address Tables Port Management	Port	Admin Status	Priority	Power Alloction (3000-15400miliwatts)	Mode	Power Consumption (miliwatts)		.ogout
Port Settings 	1/e1	Enable	Low	0	Searching	0	Edit	
LAG Settings	1/e2	Enable	Low	0	Searching	0	Edit	
PoE Settings	1/e3	Enable	Low	0	Searching	0	Edit	
VLAN Management Spanning Tree	1/e4	Enable	Low	0	Searching	0	Edit	
Multicast Routing	1/e5	Enable	Low	0	Searching	0	Edit	
Security Suite	1/e6	Enable	Low	0	Searching	0	Edit	
Quality of Service	1/e7	Enable	Low	0	Searching	0	Edit	
	1/e8	Enable	Low	0	Searching	0	Edit	
	1/e9	Enable	Low	0	Searching	0	Edit	
	1/e10	Enable	Low	0		0	Edit	
)'	1/e11	Enable	Low	0	Searching	0	Edit	

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

- **Port** Displays the selected port's number.
- Admin Status Indicates whether PoE is enabled or disabled on the port. The possible values are:
  - Enable Enables PoE on the port. This is the default setting.
  - Disable Disables PoE on the port.
- **Priority** Indicates the PoE ports' priority. The possible values are: *Critical*, *High* and *Low*. The default is *Low*.
- **Power Allocation (3000-15400 milliwatts)** Indicates the power allocated to the port. The range is 3000-15400 milliwatts.
- Mode Indicates if the port is enabled to work on PoE. The possible field values are:
  - On Indicates the device is delivering power to the interface.
  - Off Indicates the device is not delivering power to the interface.
  - *Test Fail* Indicates the powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
  - *Testing* Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.



- Searching Indicates that the device is currently searching for a powered device.
   Searching is the default PoE operational status.
- *Fault* Indicates that the device has detected a fault on the powered device. For example, the powered device memory could not be read.
- **Power Consumption (milliwatts)** Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used. The field values are represented in Watts. The possible field values are:
  - 0.44 12.95 Indicates that the port is assigned a power consumption level of .44 to 12.95 Watts.
  - 0.44 3.8 Indicates that the port is assigned a power consumption level of .44 to 3.8 Watts.
  - 3.84 6.49 Indicates that the port is assigned a power consumption level of 3.84 to 6.49 Watts.
  - 6.49 12.95 Indicates that the port is assigned a power consumption level of 6.49 to 12.95 Watts.
- 2. Click the Edit button. The Edit PoE Settings Page opens:

Edit DoE Sol	tingo	A control of Calus Spilleria, Inc.
Edit PoE Set	unys	
Port	1/e1 💌	
Enable PoE	V	
Power Priority Level	Low 💌	
Power Consumption	0	
Overload Counter	0	
Short Counter	0	
Denied Counter	0	
Absent Counter	0	
Invalid Signature Counter	0	
Power Allocation(3000-15400)	0	
Mode	off	

#### Edit PoE Settings Page

The Edit PoE Settings Page contains the following fields:

- **Port** Indicates the specific interface for which PoE parameters are defined, and assigned to the powered interface connected to the selected port.
- **Enable PoE** Enables or disables PoE on the port. The possible values are:
  - Enable Enables PoE on the port. This is the default setting.
  - Disable Disables PoE on the port.
- **Power Priority Level** Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply

Chapter 3:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power. The possible field values are:

- Low Defines the PoE priority level as low. This is the default level.
- *High* Defines the PoE priority level as high.
- *Critical* Defines the PoE priority level as Critical. This is the highest PoE priority level.
- **Power Consumption** Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used. The field values are represented in Watts. The possible field values are:
  - 0.44 12.95 Indicates that the port is assigned a power consumption level of 0.44 to 12.95 Watts.
  - 0.44 3.8 Indicates that the port is assigned a power consumption level of 0.44 to 3.8 Watts.
  - 3.84 6.49 Indicates that the port is assigned a power consumption level of 3.84 to 6.49 Watts.
  - 6.49 12.95 Indicates that the port is assigned a power consumption level of 6.49 to 12.95 Watts.
- **Overload Counter** Indicates the total power overload occurrences.
- Short Counter Indicates the total power shortage occurrences.
- Denied Counter Indicates times the powered device was denied power.
- Absent Counter Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.
- **Invalid Signature Counter** Indicate the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signature are generated during powered device detection, classification, or maintenance.
- **Power Allocation (milliwatts)** Indicates the power allocated to the port. The range is 3000-15400 milliwatts.
- Mode Indicates if the port is enabled to work on PoE. The possible field values are:
  - On Indicates the device is delivering power to the interface.
  - Off Indicates the device is not delivering power to the interface.
  - *Test Fail* Indicates the powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
  - *Testing* Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.



- Searching Indicates that the device is currently searching for a powered device.
   Searching is the default PoE operational status.
- *Fault* Indicates that the device has detected a fault on the powered device. For example, the powered device memory could not be read.
- 3. Define the relevant fields.
- 4. Click **Apply**. The PoE Settings are defined, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

4

# **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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Passwords Management**

The Passwords Management section contains the following screens:

- Defining User Authentication
- **Note** By default, a single user name is defined, "admin," with no password. An additional user name/ password is configured for use in the Linksys One system.

## **Defining User Authentication**

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

LINKSYS A Division of Claus Systems, Inc.		
SCE 2000 System Satisfics Statisfics Security Suite Security Suite Security Suite Adhemication Access Method Trafic Control Cost Prevention Cost Pre	User Authentication	Help Support Guide Logout
		Cost of the A

#### User Authentication Page

The User Authentication Page contains the following fields:

- User Name Displays the user name.
- 2. Click the Add button. The Add Local User Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Add Local User Page

SGE 2000		LINKSYS A Diele of Data Typical, In
	Add Local User	
User Name		
Password		
Confirm Password		
	Apply	
	Chbil	

The Add Local User Page contains the following fields:

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

#### Modifying the Local User Settings

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

Local User Settings Page

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

# SCE 2000 LINKSYS Local User Settings

The Local User Settings Page contains the following fields:

- User Name Displays the user name.
- **Password** Specifies the new password. The password is not displayed. As it entered an "\*" corresponding to each character is displayed in the field. (Range: 1-159 characters)
- **Confirm Password** Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.
- 3. Define the relevant fields.
- 4. Click Apply. The local user settings are modified, and the device is updated.

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Defining Authentication**

The Authentication section contains the following pages:

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

### **Defining Profiles**

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

SFE 200P   System   System </th <th></th>	

The Profiles Page contains the following fields:

- Profile Name Displays the Profile name defined for the Login Table.
- **Methods** Specifies the authentication method used for port authentication. The possible field values are:
  - *Local* Authenticates the user at the device level. The device checks the user name and password for authentication.
  - RADIUS Authenticates the user at the RADIUS server.
  - TACACS+ Authenticates the user at the TACACS+ server.

**Profiles** Page



- None Indicates that no authentication method is used to authenticate the port.
- 2. Click the Add button. The Add Authentication Profile Page opens:

Add Authentication Profile Page

SGE 2000		LINKSYS a Dinder at Data Typitana, Ira
Ad	d Authenticatio	n Profile
Profile Name		
Authentication Method		
Optional Methods	Selected Methods	
TACACS+	>>	
	Apply	

The Add Authentication Profile Page contains the following fields:

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

Modify the Authentication Profile

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

#### Edit Authentication Profile Page

Authentication Profile	
Selected Methods	
Local	

The Edit Authentication Profile Page contains the following fields:

Chapter 4:

Δ

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Profile Name** Displays the Authentication profile name.
- Authentication Methods Defines the user authentication methods. The possible field values are:
  - *Local* Authenticates the user at the device level. The device checks the user name and password for authentication.
  - RADIUS Authenticates the user at the RADIUS server.
  - TACACS+ Authenticates the user at the TACACS+ server.
- 3. Define the relevant fields.
- 4. Click Apply. The authentication profile is defined, and the device is updated.

## **Mapping Profiles**

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

#### Mapping Profiles Page

LINKSYS A Danier of Chur Systems, Inc.			
SGE 2000 System System Management System Management Marking Source Statistics Bridging Socurity Suite Paswords Management Socurity Suite Profiles Mapping Profiles TACACS+ Mapping Profiles TACACS+ Access Method Traffic Control BO2 1X Access Control DoS Prevention Dos Prevention	RADIUS TACACS+ None HTTP Optional Methods Set	- -	Help Support Guide Logout
	Арріу		

The Mapping Profiles Page contains the following fields:

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

42

4

Optional Methods — Lists available authentication methods.

- *RADIUS* Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks.
- *TACACS*+ Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.
- None Indicates that no authentication method is used to authenticate the port.

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

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

Optional Methods — Lists available authentication methods.

- *RADIUS* Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks.
- TACACS+ Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.
- None -- Indicates that no authentication method is used to authenticate the port.

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

- None Indicates that the authentication method is localized.
- 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 user-defined passwords.
- Authorization Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

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

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

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### TACACS+ Page

SGE 2000	TAC	ACS+								Help
System Admin Statistics Bridging Routing Security Suite		Parameters IP Address ing	0.0.0.0							Suppor
Passwords Management     Authentication     Profiles     Mapping Profiles		it for Reply Host	5	Source	(Sec) Authentication	Timeout	Single			Logout
Mapping Promes     TACACS+     RADIUS     Access Method     Traffic Control     802.1X		IP Address	Priority 20	IP Address Default	Port 49	for Reply Default	Connection false	Status Not Connected Delete	Edit Add	
Quality of Service		pply								

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

- Source IP Address Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- **Timeout for Reply** Displays the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- Host IP Address Displays the TACACS+ Server IP address.
- Priority Displays the order in which the TACACS+ servers are used. The default is 0.
- Authentication Port Displays the port number through which the TACACS+ session occurs. The default is port 49.
- Single Connection Maintains a single open connection between the device and the TACACS+ server when selected
- Status Displays the connection status between the device and the TACACS+ server. The possible field values are:
  - Connected There is currently a connection between the device and the TACACS+ server.
  - Not Connected There is not currently a connection between the device and the TACACS+ server.
- 2. Click The Add button. The Add TACACS+ Server Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

4

#### Add TACACS+ Server Page

SGE 2000	
5GE 2000	A Uniter of Dara Sectors, IG
	Add TACACS+ Server
Host IP Address	
Priority	
Source IP Address	Use Default
Key String	Use Default
Authentication Port	49
Timeout for Reply	(sec) 🗖 Use Default
Single Connection	
	Apply

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

- Host IP Address Displays the TACACS+ Server IP address.
- **Priority** Displays the order in which the TACACS+ servers are used. The default is 0.
- Source IP Address Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- Authentication Port Displays the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** Displays the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- Single Connection Maintains a single open connection between the device and the TACACS+ server when selected
- Use Default Uses the device default configuration.
- 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+ Settings Page opens:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### TACACS+ Settings Page

TACACS+       Host IP Address     192.16.1.1 ▼       Priority     20       Source IP Address     Default       Key String     Default       Authentication Port     49       Timeout for Reply     Default       (sec)     F Use Default	INKSYS
Priority     20       Source IP Address     Default       Key String     Default       Authentication Port     49	
Priority     20       Source IP Address     Default     (X.X.X.)     IF     Use Defa       Key String     Default     IF     Use Defa       Authentication Port     49     IF     IF	
Source IP Address Default (X.X.X.)  Use Defa Key String Default Use Defa Authentication Port 49	
Key String Default IV Use Defa Authentication Port 49	
Authentication Port 49	ult
	ult
Timeout for Reply Default (sec) 🔽 Use Defa	
	ult
Status Not Connected	
Single Connection	

The *TACACS*+ *Settings Page* contains the following fields:

- Host IP Address Displays the TACACS+ Server IP address.
- **Priority** Displays the order in which the TACACS+ servers are used. The default is 0.
- Source IP Address Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- Authentication Port Displays the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** Displays the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- Status Displays the connection status between the device and the TACACS+ server. The possible field values are:
  - Connected There is currently a connection between the device and the TACACS+ server.
  - Not Connected There is not currently a connection between the device and the TACACS+ server.
- Single Connection Maintains a single open connection between the device and the TACACS+ server when selected
  - Use Default Uses the device default configuration.
- 3. Define the relevant fields.
- 4. Click Apply. The TACACS+ settings are modified, and the device is updated.

4

## **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 Management > Security Suite > Authentication. The *RADIUS Page* opens:

SGE 2000	DAI	olus										ſ	_
SGE 2000	KAI	5103											Help
💼 System 💼 Admin	Defau	lt Parameter	5										Support
En Statistics	Defau	It Retries		3									Guide
Bridging Routing	Defau	lt Timeout fo	r Reply	3	(Sec)								
Security Suite	Defau	lt Dead Time		0	(Min)								Logout
Authentication	Defau	lt Key String											
Mapping Profiles	Sourc	e IP Address		0.0.0									
Access Method		IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply		Key String	Source IP Address	Usage Type			
-en 802.1X -en Access Control		192.1.1.120	0	1812	Default	Default	Default	Default	Default	All	Edit		
DoS Prevention Quality of Service									De	lete	Add		
		Apply											

#### **RADIUS Page**

The RADIUS Page contains the following fields:

- Default Retries Provides the default retries.
- Default Timeout for Reply Provides the device default Timeout for Reply.
- **Default Dead Time** Provides the device default Dead Time.
- Default Key String Provides the device default Default Key String.
- Source IP Address Provides the device default Timeout for Reply.
- IP Address The Authentication Server IP addresses.
- **Priority** The server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- Authentication Port Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.

Chapter 4:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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

SGE 2000			LINKSYS
362 2000	Add RADI	US Server	A Divider of Dear Systems, No.
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)	<b>I</b> ♥Use Default
Key String		(Alpha Numeric)	⊏Use Default
Source IP Address	Default		<b>I</b> ♥Use Default
Usage Type	All		
			Apply

Add Radius Server Page

The Add Radius Server Page contains the following fields:

- Host IP Address Displays the *RADIUS* Server IP address.
- **Priority** The server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- Authentication Port Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.



- Number of Retries Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 10. Three is the default value.
- **Timeout for Reply** Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 30. Three is the default value.
- **Dead Time** Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- Key String Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- Source IP Address Defines the source IP address that is used for communication with RADIUS servers.
- Usage Type Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:

Login — Indicates that the RADIUS server is used for authenticating user name and passwords.

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

*All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.

- Use Default Uses the system default settings.
- 3. Define the relevant fields.
- 4. Click Apply. The Radius Server is added, and the device is updated.

#### Modifying RADIUS Server Settings

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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SGE 2000			
	RADIUS Se	erver Setting	IS
IP Address	192.1.1.120 💌		
Priority	0		
Authentication Port	1812		
Number of Retries	Default		<b>I</b> ♥Use Default
Timeout for Reply	Default	(Sec)	<b>⊽</b> Use Default
Dead Time	Default	(Min)	<b>I</b> ♥Use Default
Key String		(Alpha Numeric)	⊏Use Default
Source IP Address	Default	(X.X.X.X)	<b>I</b> ♥Use Default
Usage Type	All		
			Apply

#### Edit RADIUS Settings Page

The Edit RADIUS Settings Page contains the following fields:

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

4

## **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

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:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **Access Profiles Page**

LINKSYS A Desister of Check Systems, Inc.		
SFE 2000P Admin System Satistics Bridging Routing Security Suite Paswords Management Access Mathod Profile Rules Trific Control DoS Prevention Quality of Service	Access Profile Name Current Active Access Profile Name Access Profile None & Console Only C Profi C Delete Add	Help Support Guide Logout

The Access Profiles Page contains the following fields:

- Access Profile Name Defines the access profile name. The access profile name can contain up to 32 characters.
- Current Active Access Profile Defines the access profile currently active.
- **Remove** Removes the selected access profile. The possible field values are:
  - Checked Removes the selected access profile.
  - Unchecked Maintains the access profiles.
- 2. Click the Add button. The Add Access Profile Page opens:

# 4

#### Add Access Profile Page

S	FE 2000P	LINKSYS A Dataer from fam. to	
		Add Access Profile	
Acce	ess Profile Name		
Rule	e Priority		
Man	agement Method	All	
n 🗆	nterface	CPort 🔽 CLAG 🔽 CVLAN 1	
<b>⊡</b> \$¢	ource IP Address	Network Mask     Prefix Length	
Acti	on	Permit 💌	
		Apply	

The Add Access Profile Page contains the following fields:

- Access Profile Name Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- Management Method Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - All Assigns all management methods to the rule.
  - *Telnet* Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - Secure Telnet (SSH) Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - HTTP Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - Secure HTTP (HTTPS) Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - SNMP Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- Interface Defines the interface on which the access profile is defined. The possible field values are:

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Port Specifies the port on which the access profile is defined.
- LAG Specifies the LAG on which the access profile is defined.
- VLAN Specifies the VLAN on which the access profile is defined.
- Source IP Address Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- Network Mask Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- Action Defines the action attached to the rule. The possible field values are:
  - Permit Permits access to the device.
  - Deny Denies access to the device. This is the default.
- 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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

4

#### Profile Rules Page

LINKSYS Advader of Datas Systems, Tec		
SFE 2000P	Access Profile Name     # Priority Interface   Management   PAddress   Interface   Method   PAddress   Length   Action   Interface   Method   PAddress   Length   Action   Interface   Management   Surce   Prefix   Length   Action   Interface   Method   PAddress   Length   Action   Interface   Method   PAddress   Length   Action   Interface   Method   PAddress   Length   Action	Help Support Guide Logout
		Cost Strategy

The Profile Rules Page contains the following fields:

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

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Secure Telnet (SSH) Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- *HTTP* Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
- Secure HTTP (HTTPS) Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
- *SNMP* Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- Source IP Address Defines the interface source IP address to which the rule applies.
- **Prefix Length** Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- Action Defines the action attached to the rule. The possible field values are:
  - Permit Permits access to the device.
  - Deny Denies access to the device. This is the default.
- **Remove** Removes rules from the selected access profiles. The possible field values are:
  - Checked Removes the selected rule from the access profile.
  - Unchecked Maintains the rules attached to the access profile.
- 2. Click the Add button. The Add Profile Rule Page opens:

#### Add Profile Rule Page

SFE 2000P		Unities of Dace Systems, Inc.
	Add Profile Rule	
Access Profile Name		
Priority		
Management Method	All	
<b>∏Interface</b>	CPort 🔽 CLAG 🔽 CVLAN 1	
Source IP Address	CNetwork Mask	
Action	Permit 💌	
		Apply

The Add Profile Rule Page contains the following fields:

• Access Profile Name — Defines the access profile name. The access profile name can contain up to 32 characters.

56

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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### 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 2000P	LINKSYS A Davier of Court Jones, Inc.	
	Edit Profile Rule	
Access Profile Name	AP1	
Priority		_
Management Method	All	
<b>∏Interface</b>	CPort 🔽 CLAG 🔽 CVLAN 1 🗹	
Source IP Address	CNetwork Mask	
Action	Permit 💌	
	Apply	

The Edit Profile Rule Page contains the following fields:

- Access Profile Name Defines the access profile name. The access profile name can contain up to 32 characters.
- **Priority** Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- Management Method Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - All Assigns all management methods to the rule.
  - *Telnet* Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - Secure Telnet (SSH) Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - HTTP Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - Secure HTTP (HTTPS) Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.



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



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Defining Traffic Control**

The Traffic Control section contains the following pages:

- Defining Storm Control
- Defining Port Security

## **Defining Storm Control**

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

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

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

*The Storm Control Page* provides fields for configuring Broadcast Storm Control. To define storm control:

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

).							
SGE 2000	St	orm	Control				Help
💼 System 💼 Admin 💼 Statistics	Co	py from	Entry Number	To Entry Number(s)	(Exam	ple: 1,3,5-10)	Suppo
Bridging Bridging	Uni	it Numb	er 1 💌				Guide
egSecurity Suite	#	Port	Enable Broadcast Control	Broadcast Rate Threshold	Broadcast Mode		Logou
Authentication	1	1/g1	Disabled	3500	Broadcast Only	Edit	
en Access Method	2	1/g2	Disabled	3500	Broadcast Only	Edit	
	3	1/g3	Disabled	3500	Broadcast Only	Edit	
- en 802.1X	4	1/g4	Disabled	3500	Broadcast Only	Edit	
Access Control	5	1/g5	Disabled	3500	Broadcast Only	Edit	
Quality of Service	6	1/g6	Disabled	3500	Broadcast Only	Edit	
	7	1/g7	Disabled	3500	Broadcast Only	Edit	
A 4	8	1/g8	Disabled	3500	Broadcast Only	Edit	
	9	1/g9	Disabled	3500	Broadcast Only	Edit	
	10	1/q10	Disabled	3500	Broadcast Only	Edit	
)'		-	N 11 1	2500		r-lta	-

Storm Control Page

The Storm Control Page contains the following fields:



- Copy From Entry Number Indicates the row number from which storm control parameters are copied.
- To Entry Number(s) Indicates the row number to which storm control parameters are copied.
- Unit Number Displays the stacking member for which the storm control parameters are displayed.
- **Port** Indicates the port from which storm control is enabled.
- Enable Broadcast Control Indicates if Broadcast packet types are forwarded on the specific interface. The possible field values are:
  - Enable Enables Broadcast packet types to be forwarded.
  - Disable Disables Broadcast packet types to be forwarded.
- **Broadcast Rate Threshold** The maximum rate (packets per second) at which unknown packets are forwarded. The rate is 3,500 1,000,000 kb/sec.
- **Broadcast Mode** Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  - Multicast & Broadcast -- Counts Broadcast and Multicast traffic together.
  - Broadcast Only Counts only Broadcast traffic.
- 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

Edit Storm Control	
1/g1	
Broadcast Only	
3500	
Apply	
	1/g1 Broadcast Only 3500

The Edit Storm Control Page contains the following fields:

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

Chapter 4:

Δ

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Broadcast Mode** Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  - Multicast & Broadcast Counts Broadcast and Multicast traffic together.
  - Broadcast Only Counts only Broadcast traffic.
- **Broadcast Rate Threshold** The maximum rate (packets per second) at which unknown packets are forwarded. The rate is 3,500 1,000,000 kb/sec.
- 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 Security Page.

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

4

To define port security:

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

Port	Security	Page
------	----------	------

SGE 2000	Port S	ecurity							Help
System		Df Unit 👤 ் L	AGs						Suppo
Statistics Bridging Routing	Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency (Sec)		Guid
Security Suite	1/g1	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	Logo
Authentication	1/g2	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
en Access Method	1/g3	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
	1/g4	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
e 802.1X	1/g5	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
- en Access Control - en DoS Prevention	1/g6	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
Quality of Service	1/g7	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
	1/g8	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
-	1/g9	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
	1/g10	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	
	1/g11	Unlocked	Classic Lock	1	Discard	Disable	10	Edit	

The Port Security Page contains the following fields:

- **Ports** Indicates the port number on which port security is configured.
- LAGs Indicates the LAG number on which port security is configured.
- Of Unit Displays the stacking member for which the port security parameters are displayed.
- Interface Displays the port or LAG name.
- Interface Status Indicates the port security status. The possible field values are:
  - Unlocked Indicates the port is currently unlocked. This is the default value.
  - Locked Indicates the port is currently locked.
- Learning Mode Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. The possible field values are:
  - Classic Lock Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
  - Limited Dynamic Lock Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated.

- Max Entries Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- Action Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
  - Forward -- Forwards packets from an unknown source without learning the MAC address.
  - Discard Discards packets from any unlearned source. This is the default value.
  - *Shutdown* Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- Trap Enables traps when a packet is received on a locked port. The possible field values are:
  - Enable Enables traps.
  - *Disable* Disables traps.
- **Trap Frequency (Sec)** The amount of time (in seconds) between traps. The default value is 10 seconds.
- 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

SGE 2000		
	Edit Port Security	
Interface	● Port 1/g1 💌 C LAG 1 💌	
Lock Interface		
Learning Mode	Classic Lock	
Max Entries	1	
Action on Violation	Discard 💌	
Enable Trap		
Trap Frequency	10	
	Apply	

The Edit Port Security Page contains the following fields:

- Interface Displays the port or LAG name.
- Lock Interface Indicates the port security status. The possible field values are:

- Unchecked Indicates the port is currently unlocked. This is the default value.
- Checked Indicates the port is currently locked.
- **Learning Mode** Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. The possible field values are:
  - *Classic Lock* Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
  - Limited Dynamic Lock Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.

In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated.

- **Max Entries** Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- Action on Violation Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
  - Forward -- Forwards packets from an unknown source without learning the MAC address.
  - Discard Discards packets from any unlearned source. This is the default value.
  - Shutdown Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- Enable Trap Enables traps when a packet is received on a locked port. The possible field values are:
  - *Enable* Enables traps.
  - Disable Disables traps.
- **Trap Frequency** The amount of time (in seconds) between traps. The default value is 10 seconds.
- 3. Modify the relevant fields.
- 4. Click Apply. Port security is modified, and the device is updated.

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **Defining 802.1x**

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

- Authenticators Specifies the port, which is authenticated before permitting system access.
- Supplicants Specifies host connected to the authenticated port requesting to access the system services.
- Authentication Server Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port based authentication creates two access states:

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

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

The 802.1x section contains the following pages:

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

### **Defining 802.1X Properties**

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

802.1X	Properties	s Page
--------	------------	--------

Properties	Help
Port Based Authentication State Authentication Method None C Guest VLAN C Apply	Support Guide Logout
	Authentication Method None  Guest VLAN Guest VLAN ID 10

The 802.1X Properties Page contains the following fields:

- **Port Based Authentication State** Indicates if Port Authentication is enabled on the device. The possible field values are:
  - Enable Enables port-based authentication on the device.
  - Disable Disables port-based authentication on the device.
- Authentication Method Defines the user authentication methods. The possible field values are:
  - *RADIUS* Authenticates the user at the RADIUS server.
  - *RADIUS, none* Authenticates the user at the RADIUS server if one is available, otherwise it assigns no authentication method.
  - None Assigns no authentication method to the authentication profile.
- Guest VLAN Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - Enable Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field.

Chapter 4:

Δ

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Disable Disables port-based authentication on the device. This is the default.
- Guest VLAN ID Displays the Guest VLAN ID.
- 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:

SGE 2000	Po	ort A	uthe	nticatio	n						He
System Admin Statistics	Co	py from	Entry N	umber		To Entry Number	(s)	(Example: 1,3,5-10)			Supp
Bridging Routing	Uni	it Numb	er 1	·							Gui
Security Suite	#	Port	User Name	Current Port Control	Guest VLAN	Periodic Reauthentication	Reauthentication Period	Authenticator State	Quiet Period	Resending EAP	Max Logo Req
-en Authentication -en Access Method	1	1/g1		Authorized	Disable	Disable	3600	Force Authorized	60	30	2
Traffic Control	2	1/g2		•	Disable	Disable	3600	Initialize	60	30	2
	3	1/g3		*	Disable	Disable	3600	Initialize	60	30	2
Port Authentication Multiple Host	4	1/g4		•	Disable	Disable	3600	Initialize	60	30	2
Authenticated Host	5	1/g5		•	Disable	Disable	3600	Initialize	60	30	2
DoS Prevention	6	1/g6		*	Disable	Disable	3600	Initialize	60	30	2
Quality of Service	7	1/g7		÷	Disable	Disable	3600	Initialize	60	30	2
	8	1/g8			Disable	Disable	3600	Initialize	60	30	2
	9	1/g9		*	Disable	Disable	3600	Initialize	60	30	2
					e 11	N 11	~~~ ,	a second	~~		- <u>-</u>

The 802.1X Port Authentication Page contains the following fields:

- Copy From Entry Number Indicates the row number from which port authentication parameters are copied.
- To Entry Number(s) Indicates the row number to which port authentication parameters are copied.
- Unit Number Displays the stacking member for which the port authentication parameters are displayed.
- **Port** Indicates the port name.
- User Name Displays the user name.
- Current Port Control Displays the admin port authorization state.
- **Guest VLAN** Displays the Guest VLAN.

68

4

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

Modifying 8021X Security

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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SGE 2000	
Port Aut	hentication Settings
Port	1/g1 💌
User Name	
Current Port Control	Authorized
Admin Port Control	forceAuthorized 💌
Enable Guest VLAN	
Enable Periodic Reauthentication	
Reauthentication Period	3600
Reauthenticate Now	
Authenticator State	Force Authorized
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
Termination Cause	Undefined
	Apply

#### Port Authentication Settings Page

The Port Authentication Settings Page contains the following fields:

- **Port** Indicates the port name.
- User Name Displays the user name.
- Current Port Control Displays the current port authorization state.
- Admin Port Control Displays the admin port authorization state.
- Enable Guest VLAN Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - Enable Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field.
  - Disable Disables port-based authentication on the device. This is the default.
- Enable Periodic Reauthentication Permits immediate port reauthentication.
- **Reauthentication Period** Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Reauthenticate Now** Specifies that authentication is applied on the device when the **Apply** button is pressed.
- Authenticator State Specifies the port authorization state. The possible field values are as follows:
  - Force-Authorized The controlled port state is set to Force-Authorized (forward traffic).
  - Force-Unauthorized The controlled port state is set to Force-Unauthorized (discard traffic).

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

#### 802.1X Multiple Host Page

									-	
SGE 2000	Mul	tiple Hos	t						f f	Help
System	Unit	1 💌							-	Support
e 💼 Statistics e 🍋 Bridging	Port	Multiple Hosts	Action on Violation	Traps	Trap Frequency	Status	Number of Violations			Guide
e 💼 Routing Beessecurity Suite	1/g1	Single	Discard	Disable	10	Not in auto mode	0	Edit		Logout
Passwords Management	1/g2	Single	Discard	Disable	10	Not in auto mode*	0	Edit		Logour
Access Method	1/g3	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
- maffic Control - maffic Control	1/g4	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
Properties 	1/g5	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
Multiple Host	1/g6	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
-en Access Control	1/g7	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
DoS Prevention	1/g8	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
	1/g9	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
	1/g10	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
	1/g11	Single	Discard	Disable	10	Not in auto mode*	0	Edit		
	1/g13	Single	Discard	Disable	10	Not in auto mode*	0	Edit	J	

The 802.1X Multiple Host Page contains the following fields:

Chapter 4:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Unit Number Displays the stacking member for which the Multiple Hosts parameters are displayed.
- **Port** Displays the port number for which advanced port-based authentication is enabled.
- **Multiple Hosts** Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
- Action on Violation Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - Forward Forwards the packet.
  - Discard Discards the packets. This is the default value.
  - *DiscardDisable* Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- Traps Indicates if traps are enabled for Multiple Hosts. The possible field values are:
- **Trap Frequency** Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- Status Indicates the host status. If there is an asterisk (\*), the port is either not linked or is down. The possible field values are:
  - Unauthorized Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
  - Not in Auto Mode Indicates that the port control is Forced Authorized, and clients have full port access.
  - *Single-host Lock* Indicates that the port control is Auto and a single client has been authenticated via the port.
  - No Single Host Indicates that Multiple Host is enabled.
- **Number of Violations** Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

#### Modifying Multiple Host Settings

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



Multiple Host Settings Page

SGE 2000		LINKSYS A Distance of Class Typetienes, Inc.	•
M	ultiple Hosts Settings		
Port	1/g1 •		
Enable Multiple Hosts			
Action on Violation	Discard 💌		
Enable Traps			
Trap Frequency	10		
	Apply		

The Multiple Host Settings Page contains the following fields:

- Port Displays the port number for which advanced port-based authentication is enabled.
- Enable Multiple Hosts Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
  - Checked Multiple host mode is enabled.
  - Unchecked Single host mode is enabled. This is the default value.
- Action on Violation Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - Forward Forwards the packet.
  - Discard Discards the packets. This is the default value.
  - *DiscardDisable* Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- Enable Traps Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - Checked Indicates that traps are enabled for Multiple hosts.
  - Unchecked Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- 3. Modify the relevant fields.
- 4. Click Apply. The multiple host settings are defined, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

### **Defining Authenticated Host**

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

802.1X Authenticated Host Page

SGE 2000	Authen	ticat	ted Host			Help
- Curtur						<b>_</b>
🗄 💼 System 🗄 💼 Admin	Unit 1 💌					Suppor
🗄 💼 Statistics	User Name	Port	Session Time	Authentication Method	MAC Address	
🗄 💼 Bridging	ouer nume	1/g1	66981	Remote	00000000000	Guide
n Routing		1/g2	0	Remote	00000000000	
⊟ — en Security Suite — en Passwords Management		1/g3	0	Remote	000000000000	Logout
- Authentication		1/g4	0	Remote	00000000000	
Access Method		1/g5	0	Remote	000000000000	
- 💼 Traffic Control		-			00000000000	
-ea802.1X		1/g6	0	Remote Remote	000000000000	
Port Authentication		1/g7	0	Remote	000000000000	
Multiple Host		1/g8	0			
Authenticated Host		1/g9	0	Remote	00000000000	
Access Control		1/g10		Remote	00000000000	
DoS Prevention		1/g11		Remote	00000000000	
		1/g13		Remote	0000000000	
		1/g14		Remote	00000000000	-
		1/g15		Remote	00000000000	
		1/g16		Remote	00000000000	
J		1/g17		Remote	00000000000	_
		1/a18	n	Remote	000000000	<b>_</b>

The 802.1X Authenticated Host Page contains the following fields:

- Unit Number Displays the stacking member for which the Authenticated Hosts parameters are displayed.
- User Name Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** Displays the port number.
- Session time Displays the amount of time (in seconds) the supplicant was logged on the port.
- Authentication Method Displays the method by which the last session was authenticated. The possible field values are:
  - Remote 802.1x authentication is not used on this port (port is forced-authorized).
  - None The supplicant was not authenticated.
  - RADIUS The supplicant was authenticated by a RADIUS server.
- MAC Address Displays the supplicant MAC address.
- 2. Define the relevant fields.
- 3. Click Apply. The authenticated host settings are defined, and the device is updated.

## **Defining Access Control**

The Access Control section contains the following pages:

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

### **Defining MAC Based ACL**

The *MAC Based ACL Page* page allows a MAC- based ACL to be defined. ACEs 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:

LINKSYS A Division of Cloce Systems, Inc.											
SGE 2000		C Bas Name ma	ed ACL ₫ I								Help Support
ia ● Bridging ia ● Routing ia ● Security Suite		Priority	Source MAC Address	Mask	Destination MAC Address	Mask	VLAN ID	CoS	Cos Mask	Ether Typ	Guide Logout
Passwords Management     Authentication     Access Method     Traffic Control     B02.1X     Access Control     MAC Based ACL     D Passed ACL     Access Control     AccL Binding     DoS Prevention     Guality of Service		20			MAC A007655		100				
	4									F	

MAC Based ACL Page

The MAC Based ACL Page contains the following fields:

- ACL Name Displays the user-defined MAC based ACLs.
- **Remove ACL** Deletes the selected ACL.
- Deny Following Destination MAC Addresses Matches the destination MAC address and denies packet access.
- 2. Click the Add ACL button. The Add MAC Based ACL Page opens:

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SGE 2000	Add I	MAC Based /	LINKSYS ACL
ACL Name			
New Rule Priority			
Source MAC Address	0	Wild Card Mask	CAny
Dest. MAC Address	0	Wild Card Mask	CAny
VLAN ID			
CoS			
CoS Mask			
Ether Type			
Action	Permit		
			Apply

#### Add MAC Based ACL Page

The Add MAC Based ACL Page contains the following fields:

- ACL Name Displays the user-defined MAC based ACLs.
- New Rule Priority Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- Source Address
  - MAC Address Matches the source MAC address to which packets are addressed to the ACE.
  - Mask Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source IP Address. Wild card masks specify which bits are used and which bits are ignored. A wild card mask of ff: ff:ff:ff:ff:ff indicates that no bit is important. A wildcard of 00.00.00.00.00 indicates that all the bits are important. For example, if the source IP address 14.36.18.19.1.1 and the wildcard mask is 255.36.184.00.00.00, the middle two bits of the IP address are used, while the last three bits are ignored.
- Destination Address
  - MAC Address Matches the destination MAC address to which packets are addressed to the ACE.
  - Mask Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination IP Address. Wild card masks specify which bits are used and which bits are ignored. A wild card mask of ff: ff:ff:ff:ff:ff:ff indicates that no bit is important. A wildcard of 00.00.00.00.00 indicates that all the bits are important. For example, if the source IP address 14.36.18.19.1.1 and the wildcard mask is 255.36.184.00.00.00, the middle two bits of the IP address are used, while the last three bits are ignored.
- VLAN ID Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **CoS** Class of Service of the packet.
- CoS Mask Wildcard bits to be applied to the CoS.
- **Ether Type** The Ethernet type of the packet.
- Action Indicates the ACL forwarding action. The possible field values are:

- Permit Forwards packets which meet the ACL criteria.
- Deny Drops packets which meet the ACL criteria.
- *Shutdown* Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.
- 3. Define the relevant fields.
- 4. Click Apply. The MAC Based ACL is defined, and the device is updated.

Adding Rule to MAC Based ACL

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

SFE 2000				Ļ	_INKSYS
		A	Add Rule		
CL Name					
lew Rule Priority					
iource MAC Address	·		Wild Card Mask		CAny
est. MAC Address	œ		Wild Card Mask		CAny
'LAN ID					
coS					
CoS Mask					
ther Type					
ction		Permit 💌			

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

#### **Defining IP Based ACL**

The Defining IP Based ACL page contains information for defining IP Based ACLs, including defining the ACEs defined for IP Based ACLs.

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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### IP Based ACL Page

#### 

SFE 2000P	IP B	ased	ACL											
rstem			_											s
System Management	ALL N	ame ip1												
SNMP dmin														
atistics	* Flag S	Set prese	nt the flag	types in	the follo	owing o	rder: Ur	g, Ack, Psh,	Rst, Syn	, Fin. Set is r	epresen	ted as 1,	unset as	D and don
idging outing		Rule		Flag	ICMP	ICMP	IGMP							
ecurity Suite		Priority	Protocol	Set	Туре	Code	Туре	Source		Destination		DSCP	IP-Prec.	Action
Passwords Management Authentication								IP Address	Mask	IP Address	Mask			
Access Method		60	TCP	111111				50.1.1.50	0.0.0.0	50.1.1.100	0.0.0.0	50		Permit
Traffic Control		80	TCP	111111				50.1.1.50	0000	50.1.1.100	0000	30		Permit
802.1X Access Control								00.1.1.00	0.0.0.0	00.111100	0.0.0.0			1 on the
- MAC Based ACL													Dele	te Rule
DoS Prevention													De	ete ACL
uality of Service														
														1

The IP Based ACL Page contains the following fields:

- ACL Name Displays the user-defined IP based ACLs.
- **Remove ACL** Deletes the selected ACL.
- **Rule Priority** Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** Creates an ACE based on a specific protocol.
  - Any Matches the protocol to any protocol.
  - *IDRP* Matches the packet to the Inter-Domain Routing Protocol (IDRP).
  - IDPR Matches the packet to the Inter-Domain Policy Routing Protocol (IDPR).
  - *RVSP* Matches the packet to the ReSerVation Protocol (RSVP).
  - *AH* Indicates that the Authentication Header (AH) protocol is used to classify network flows.
  - *EIGRP* Indicates that the Enhanced Interior Gateway Routing Protocol (EIGRP) is used to classify network flows.
  - OSPF Matches the packet to the Open Shortest Path First (OSPF) protocol.
  - *IPIP* Matches the packet to the IP Protocol
  - PIM Matches the packet to Protocol Independent Multicast (PIM).

- *L2IP* Matches the packet to Layer 2 Internet Protocol (L2IP).
- ISIS Indicates that the Intermediate System to Intermediate System (ISIS) protocol is used to classify network flows.
- Flag Set Sets the indicated TCP flag that can be triggered.
- ICMP Type Filters packets by ICMP message type. The field values is 0-255.
- ICMP Code Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP Type** Filters packets by IGMP message or message types.
- Source

IP Address — Matches the source port IP address to which packets are addressed to the ACE.

**Mask** — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.

• Destination

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

Mask — Defines the destination IP address wildcard mask. Select either Match DSCP or Match IP

- **DCSP** Matches the packets DSCP value.
- **IP Prec** Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- Action Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - Permit Forwards packets which meet the ACL criteria.
  - Deny Drops packets which meet the ACL criteria.
  - *Shutdown* Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.
  - Match IP Precedence Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- 2. Click the Add Button. The Add IP Based ACL Page opens:

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SFE 2000P	LINKSYS Albert Ora Vana Ka
	Add IP Based ACL
ACL Name	
New Rule Priority 🗖	
Protocol	Select from List ICMP Protocol ID
Source Port	@ @Any
Destination Port	@ @Any
TCP Flags	🔲 Urg Set 🔽 Ack Set 💌 Psh Set 💌 Rst Set 💌 Syn Set 💌
ІСМР 🥅	CICMP Type
ICMP Code 🥅	
IGMP	Celect from List DVMRP CIGMP Type 19 CAny
Source IP Address	C CAny Wild Card Mask C CAny
Dest. IP Address	C CAny Wild Card Mask C CAny
Match DSCP	e
Match IP Precedence	
Action	Permit V

#### Add IP Based ACL Page

The Add IP Based ACL Page contains the following fields:

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



- Match IP Precedence Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- Action Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - Permit Forwards packets which meet the ACL criteria.
  - Deny Drops packets which meet the ACL criteria.
  - Shutdown Drops packet that meets the ACL criteria, and disables the port to which the
    packet was addressed. Ports are reactivated from the Port Management page.
- 3. Define the relevant fields,
- 4. Click Apply. The IP Based ACL is defined, and the device is updated.

Defining Rules Associated with IP-ACL

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

SFE 2000P	LINKSYS Hand Gardana ka
	Rules Associated with IP-ACL
ACL Name	ip1
New Rule Priority	60
Protocol	CSelect from List TCP Protocol ID 6
Source Port	C ©Any
Destination Port	C GAny
TCP Flags	r Urg Set ▼ Ack Set ▼ Psh Set ▼ Rst Set ▼ Syn Set ▼ I
	CICMP Type CAny
ICMP Code	
	Select from List DVMRP GIGMP Type 19 CAny
Source IP Address	© 50.1.1.50 CAny Wild Card Mask © 0.0.0. CAny
Dest. IP Address	© 50.1.1.100 CAny Wild Card Mask © 0.0.0.0 CAny
Match DSCP	c 50
Match IP Precedence	c
Action	Permit
Apply	

#### Rules Associated with IP-ACL Page

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

- ACL Name Displays the user-defined IP based ACLs.
- New Rule Priority Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** Creates an ACE based on a specific protocol.
- **TCP Flags** Filters packets by TCP flag. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. The possible field values are:

Chapter 4:

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **ICMP** Indicates if ICMP packets are permitted on the network. The possible field values are as follows:.
- ICMP Code Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- IGMP Filters packets by IGMP message or message types.
- Source IP Address Matches the source port IP address to which packets are addressed to the ACE.
- **Dest. IP Address** Matches the destination port IP address to which packets are addressed to the ACE.
- Match DSCP Matches the packet to the DSCP tag value.
- Match IP Precedence Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- Source Port Defines the TCP/UDP source port to which the ACE is matched. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 65535.
- Destination Port Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 65535.
- Action Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - Permit Forwards packets which meet the ACL criteria.
  - Deny Drops packets which meet the ACL criteria.
  - *Shutdown* Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

#### Adding an IP Based Rule

- 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:



#### Add IP Based Rule Page

SFE 2000P		LINKSYS
	Add IP Based Rule	
ACL Name	ip1	
New Rule Priority		
Protocol	©Select from List ICMP CProtocol ID	
Source Port	C GAny	
Destination Port	C @Any	
TCP Flags	TUrg Set Ack Set Psh Set Ret Set Set Set Set Set Set Set Set Set S	yn Set 💌
	CSelect from List Echo-Reply	
ICMP Code 🕅		
IGMP	CSelect from List DVMRP CIGMP Type 19 CAny	
Source IP Address	C CAny Wild Card Mask C CAny	
Dest. IP Address	C CAny Wild Card Mask C CAny	
Match BSCP	c	
Match IP Precedence	c	
Action	Permit	

The Add IP Based Rule Page contains the following fields:

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

Chapter 4:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- 4
- Match IP Precedence Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- Action Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - Permit Forwards packets which meet the ACL criteria.
  - Deny Drops packets which meet the ACL criteria.
  - *Shutdown* Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

#### **Defining ACL Binding**

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

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

LINKSYS A Division of Cisco Systems, Inc.		
SFE 2000P	ACL Binding	Help
⊟- <mark>en</mark> System I en System Management	Copy from Entry Number To Entry Number(s) (Example: 1,3,5.10)	Support
Admin	C Ports Of Unit I ▼ C LAGs	Guide
e 💼 Bridging Routing	# Interface ACL Name	Logout
egecurity Suite	□ 1 1/e1 Edit	
Passwords Management Called Authentication	□ 2 1/e2 Edit	
-en Access Method	🗆 3 1/e3 Edit	
	🗆 4 1/e4 Edit	
	□ 5 1/e5 Edit	
IP Based ACL	□ 6 1/e6 Edit	
DoS Prevention	🗆 7 1/e7 Edit	
adanty of Dervice	□ 8 1/e8 Edit	
	□ 9 1/e9 Edit	
	🗆 10 1/e10 Edit	
		2

ACL Binding Page

The ACL Binding Page contains the following fields:

- Copy From Entry Number Indicates the ports/LAGs from which the ACL are copied.
- To Entry Number(s) Indicates the ports/LAGs to which the ACL are copied.
- **Ports** Displays the ports bound by the ACL.

- LAGs Displays the LAGs bound by the ACL.
- Of Unit Displays the stacking member for which the ACL binding parameters are displayed.
- Interface Indicates the interface to which the ACL is bound.
- ACL Name Indicates the ACL which is bound the interface.

#### Modifying ACL Binding

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

#### **Bind** ACL Page

The Bind ACL Page contains the following fields:

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

4

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **Global Settings Page**

SFE 2000P	Global Settings		Help
a⊷ <mark>en</mark> System - <mark>- en</mark> System Management	Copy from Entry Number	To Entry Number(s) (Example: 1,3,5-10)	Suppo
Admin Statistics	⑦ Ports Of Unit I ▼ ○ LAGs		Guide
e 💼 Bridging e 💼 Routing	F # Interface ACL Name		Logou
e Security Suite	🗆 1 1/e1	Edit	
Passwords Management	🗆 2 1/e2	Edit	
Access Method	□ 3 1/e3	Edit	
- 💼 802.1X	□ 4 1/e4	Edit	
-en Access Control -en DoS Prevention	□ 5 1/e5	Edit	
Global Settings	□ 6 1/e6	Edit	
Martian Addresses		Edit	
	□ 7 1/e7		
	□ 8 1/e8	Edit	
	□ 9 1/e9	Edit	
J	🗖 10 1/e10	Edit	-

The Global Settings Page contains the following fields:

- Security Suite Status Indicates if DOS security is enabled on the device. The possible field values are:
  - Enable Enables DOS security.
  - *Disable* Disables DOS security on the device. This is the default value.
- **Denial of Service Protection** Indicates if service is enabled. If the service protection is disabled, the *Stacheldraht Distribution*, *Invasor Trojan*, and *Back Office Trojan* fields are disabled.
- Stacheldraht Distribution Discard TCP packets with source TCP port equal to 16660
- Invasor Trojan Discard TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- **Back Office Trojan** Discard UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.
- 2. Define the relevant fields.
- 3. Click Apply. The Dos prevention global settings are defined, and the device is updated.

### **Defining Martian Addresses**

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

LINKSYS A Division of Carlo Systems, No.		
SFE 2000P  System System Management Shifting Routing Routing Scurty Suite Routing Securty Suite Cocess Method Trific Control B02.1% Access Control D0S Prevention Cold Settings Martian Addresses Could Service	Martian Addresses	Help Support Guide Logout
		Case Structure

The Martian Addresses Page contains the following fields:

- IP Address Displays the IP addresses for which DOS attack is enabled.
- Mask Displays the Mask for which DOS attack is enabled.
- 2. Click the Add button. The Add Martian Addresses Page opens:

#### Add Martian Addresses Page

SFE 2000P				LINKSYS + Dieler of Dara Fattern, In
	Add	Martian Ad	dresses	
Include Reserved Martian Addresses				
IP Address	CSelect from Known Martian Addresses	10.0.0/8	New IP Address	
Mask				
O Prefix Length				
				Apply

The Add Martian Addresses Page contains the following fields:

- Include Reserved Martian Addresses Indicates that packets arriving from Martian addresses are dropped. When enabled, the following IP addresses are included:
  - 0.0.0.0/8 (except 0.0.0.0/32), 127.0.0.0/8

Chapter 4:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- 192.0.2.0/24, 224.0.0.0/4
- 240.0.0/4 (except 255.255.255.255/32)
- IP Address Enter the IP addresses for which DOS attack is enabled.
- Mask Enter the Mask for which DOS attack is enabled.
- **Prefix Length** Defines the IP route prefix for the destination IP.
- 3. Define the relevant fields.
- 4. Click Apply. The martian addresses are added, and the device is updated.

# **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 **SFE 2000P Port Settings** ia — System ia — Madmin Copy From Entry Number To Entry Number(s) (Example: 1,3,5-10) 🗄 💼 Statistics Bridging Guide Unit Number 1 🔻 Address Tables en Port Management Port Duplex LAG Logout Port Status Port Settings # Interface Port Type Edit 1 1/e1 100M-copper Down 2 1/e2 100M-copper Edit Down IN Management 3 1/e3 100M-copper Down 💼 Spanning Tree 4 1/e4 100M-copper Multicast Down Routing 5 1/e5 100M-copper Up 100M Full 1 Edit 💼 💼 Security Suite 100M-copper a Cuality of Service 6 1/e6 Down 7 1/e7 100M-copper Down 8 1/e8 100M-copper Down 9 1/e9 100M-copper Edit Down Edit 10 1/e10 100M-copper Up 100M Eull

**Port Settings Page** 

The Port Settings Page contains the following fields:

- Copy from Entry Number Copies port information from the selected port.
- to Entry Number(s) Copies port information to the selected port.
- Unit Number Indicates the stacking member for which the ports are defined.
- Interface Displays the port number.

Chapter 5:

5

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Port Type** Displays the port type. The possible field values are:
  - *Copper/ComboF/ComboC* Indicates the port has a copper port connection.
  - Fiber Indicates the port has a fiber optic port connection.
- **Port Status** Displays the port connection status.
- **Port Speed** Displays the current port speed.
- **Duplex Mode** Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
  - *Full* Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
  - Half Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **PVE** Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it.
- LAG Defines if the port is part of a Link Aggregation (LAG).
- 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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



SFE 2000P	LINKSYS I State of Sec. In
	Edit Port
Port	1/e1 •
Description	
Port Type	100M-copper
Admin Status	Up 💌
Current Port Status	Down
Reactivate Suspended Port	п
Operational Status	Active
Admin Speed	100M 🔽
Current Port Speed	
Admin Duplex	Full 🔽
Current Duplex Mode	
Auto Negotiation	Enable 💌
Current Auto Negotiation	
Admin Advertisement	Max Capability 10 Half 10 Full 100 Half 100 Full 1000 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Back Pressure	Disable 💌
Current Back Pressure	
Flow Control	Disable
Current Flow Control	
MDI/MDIX	AUTO -
Current MDI/MDIX	
LAG	
	Apply

#### Edit Port Settings Page

The Edit Port Settings Page contains the following fields:

- **Port** Displays the port number.
- **Description** Displays the device port ID.
- **Port Type** Displays the port type. The possible field values are:
  - *Copper/ComboF/ComboC* Indicates the port has a copper port connection.
  - Fiber Indicates the port has a fiber optic port connection.
- Admin Status Enables or disables traffic forwarding through the port.
- Current Port Status Displays the port connection status.
- **Reactivate Suspended Port** Reactivates a port if the port has been disabled through the locked port security option.
- **Operational Status** Defines whether the port is currently operational or non-operational.
- Admin Speed The configured rate for the port. The port type determines what speed setting options are available. You can designate admin speed only when the port auto-negotiation is disabled.
- Current Port Speed Displays the current port speed.
- Admin Duplex Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:

5

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- *Full* Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
- *Half* Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- Current Duplex Mode Displays the port current duplex mode.
- Auto Negotiation Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- Current Auto Negotiation Displays the Auto Negotiation status on the port.
- Admin Advertisement Specifies the capabilities to be advertised by the Port. The possible field values are:
  - Max Capability Indicates that all port speeds and Duplex mode settings can be accepted.
  - *10 Half* Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.
  - *10 Full* Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
  - *100 Half* Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.
  - *100 Full* Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.
  - *1000* Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- Neighbor Advertisement The neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- **Back Pressure** Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. The Back Pressure mode is configured for ports currently in the Half Duplex mode or on LAGs.
- Current Back Pressure Displays the Back Pressure mode on the port.
- Flow Control Enables or disables flow control or enables the auto negotiation of flow control on the port.
- Current Flow Control Displays the current Flow Control setting.



- **MDI/MDIX** Displays the Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX) status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
  - MDIX Use for hubs and switches.
  - Auto Use to automatically detect the cable type.
  - *MDI* Use for end stations.
- Current MDI/MDIX Displays the current MDI/MDIX setting.
- LAG Defines if the port is part of a Link Aggregation (LAG).
- **PVE** Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it.
- 3. Define the relevant fields.

٠

4. Click Apply. The Port Settings are modified, and the device is updated.

5

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

### **Defining LAG Management**

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

The device supports both static LAGs and *Link Aggregation Control Protocol* (LACP) LAGs. LACP LAGs negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them. Ensure the following:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to 64 LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports. To define Lag management:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

5

#### Lag Management Page

Help Support Guide Logout	r Edit	Management	LAG M	SFE 2000P
Guide		Name Link State		
	Edit		LAG Nam	System
		Link Not Present	LAG 1	En Statistics
Logout	Edit	Link Not Present	LAG 2	Bridging Address Tables
	Edit	Link Not Present	LAG 3	
	Edit	Link Not Present	LAG 4	
	Edit	Link Not Present	LAG 5	LAG Settings
	Edit	Link Not Present	LAG 5	PoE Settings
	Edit	Link Not Present	LAG 7	
	Edit	Link Not Present	LAG 8	່ 💼 Multicast b Routing ມີ
		tino	Bold - Active	Security Suite
			Grayed - Pas	
				).

The Lag Management Page contains the following fields.

- LAG Displays the LAG number.
- **Name** Displays the LAG name.
- Link State Displays the link operational status.
- Member Displays the ports configured to the LAG.
- 2. Define the relevant fields.
- 3. Click Apply. Lag Management is defined, and the device is updated.

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:

5

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SFE 2000P		LINKSYS A Unidate of Class Systems, Inc.
	Edit LAG Membershi	р
LAG 1 -		
LAG Name		
LACP		
Unit 1 💌		
Port List	Lag Members	
1/e1 1/e2 1/e3 1/e4 1/e5	>> <<	
	Apply	

#### Edit LAG Membership Page

The Edit LAG Membership Page contains the following fields.

- LAG Displays the LAG number.
- LAG Name Displays the LAG name.
- LACP Indicates that LACP is enable on the LAG.
- Unit Number Displays the stacking member for which LAG information is defined.
- 3. Define the relevant fields.
- 4. Click Apply. The Lag membership is defined, and the device is updated.

### **Defining LAG Settings**

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

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

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

5

#### Lag Settings Page

#### LINKSYS

System Admin Statistics	Copy Fre	m Entry Nun	nber	To E	ntry Numb	er(s)	(Exam	ple: 1,3,5-8)	Support
Bridging Address Tables Port Management D'Port Settings	LAG	Description	Туре	Status	Speed	Auto Negotiation	Flow Control		Guide
	LAG 1		Unknown	Unknown	Unknown	Unknown	Unknown 🌘	Edit	Logout
LAG Management 	LAG 2		Unknown	Unknown	Unknown	Unknown	Unknown 🌘	Edit	
LACP PoE Settings	LAG 3		Unknown	Unknown	Unknown	Unknown	Unknown 🌘	Edit	
Number of VLAN Management	LAG 4		Unknown	Unknown	Unknown	Unknown	Unknown 🌘	Edit	
💼 Spanning Tree 💼 Multicast	LAG 5		Unknown	Unknown	Unknown	Unknown	Unknown 🌘	Edit	
Routing 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	
	Ар	bly							

The Lag Settings Page contains the following fields:

- Copy from Entry Number Copies the LAG information from the selected port.
- To Entry Number(s) Indicates the ports to which the port QoS information is copied.
- LAG Displays the LAG Id number.
- **Description** Displays the user-defined port name.
- **Type** The port types that comprise the LAG.
- Status Indicates if the LAG is currently operating.
- **Speed** The configured speed at which the LAG is operating.
- Auto Negotiation The current Auto Negotiation setting.
- Flow Control The user-designated Flow Control setting.
- 2. Click the Edit button. The Lag Configuration Settings opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

LAG       I         Description       I         LAG Type       I         Admin Status       Up         Current LAG Status       I         Reactivate Suspended LAG       I         Operational Status       Active         Admin Auto Negotiation       Enable         Current Auto Negotiation       Inable         Admin Advertisement       Unknown         Neighbor Advertisement       Unknown         Neighbor Advertisement       Unknown         Admin Speed       IOM         Current LAG Speed       IOM         Admin Flow Control       Disable	SFE 2000P		
LAG       1         Description       Image: Component of the second of the secon		LAG Configuration Settings	
Description       Image: Comparison of the second of the sec			
LAG Type         Admin Status       Up •         Current LAG Status         Reactivate Suspended LAG       •         Operational Status       Active         Admin Auto Negotiation       •         Current Auto Negotiation       •         Admin Advertisement       •         Admin Advertisement       •         Vinknown       •         Heighbor Advertisement       •         Unknown       •         Admin Speed       •         IOM •       •         Current LAG Speed       •         Admin Flow Control       Disable •	LAG		
Admin Status     Up I       Admin Status     Up I       Current LAG Status     Image: Control Status       Reactivate Suspended LAG     Image: Control Status       Operational Status     Active       Admin Auto Negotiation     Image: Control Status       Current Auto Negotiation     Image: Control Status       Admin Advertisement     Image: Control Status       Very Advertisement     Unknown       Neighbor Advertisement     Unknown       Admin Speed     Image: Control Status       Admin Flow Control     Disable	Description		
Current LAG Status         Reactivate Suspended LAG         Operational Status         Admin Auto Negotiation         Current Auto Negotiation         Admin Advertisement         VMax Capability 10 Full 1000 Full         Current Advertisement         Unknown         Neighbor Advertisement         Unknown         Admin Speed         IOM *         Current LAG Speed         Admin Flow Control	LAG Type		
Reactivate Suspended LAG     Image: Constant of the subsectivate Suspended LAG       Operational Status     Active       Admin Auto Negotiation     Image: Constant of the subsectivate Subsec	Admin Status	Up 💌	
Operational Status     Active       Admin Auto Negotiation     Enable       Current Auto Negotiation     FMax Capability 10 Full 100 Full 1000 Full       Admin Advertisement     FMax Capability 10 Full 100 Full 1000 Full       Current Advertisement     Unknown       Neighbor Advertisement     Unknown       Admin Speed     IOM       Current LAG Speed     Eisable	Current LAG Status		
Admin Auto Negotiation     Enable       Admin Auto Negotiation     Enable       Admin Advertisement     Max Capability 10 Full 100 Full 1000 Full       Current Advertisement     Unknown       Neighbor Advertisement     Unknown       Admin Speed     10M       Current LAG Speed     Disable	Reactivate Suspended LAG		
Current Auto Negotiation       Admin Advertisement       Virknown       Neighbor Advertisement       Unknown       Admin Speed       Current LAG Speed       Admin Flow Control	Operational Status	Active	
Admin Advertisement     Max Capability 10 Full 100 Full 1000 Full       Current Advertisement     Unknown       Neighbor Advertisement     Unknown       Admin Speed     10M        Current LAG Speed     Disable	Admin Auto Negotiation	Enable 💌	
Current Advertisement     Unknown       Neighbor Advertisement     Unknown       Admin Speed     10M       Current LAG Speed     Disable	Current Auto Negotiation		
Neighbor Advertisement     Unknown       Admin Speed     IOM       Current LAG Speed     Disable	Admin Advertisement	🔽 Max Capability 📁 10 Full 📁 100 Full 📁 1000 Full	
Admin Speed 10M V Current LAG Speed Admin Flow Control Disable V	Current Advertisement	Unknown	
Current LAG Speed Admin Flow Control Disable	Neighbor Advertisement	Unknown	
Admin Flow Control Disable	Admin Speed	10M	
·	Current LAG Speed		
Current Flow Control	Admin Flow Control	Disable 💌	
	Current Flow Control		

#### Lag Configuration Settings

The Lag Configuration Settings contains the following fields:

- LAG Displays the LAG Id number.
- **Description** Displays the user-defined port name.
- LAG Type The port types that comprise the LAG.
- Admin Status Enables or disables traffic forwarding through the selected LAG.
- Current LAG Status Indicates if the LAG is currently operating.
- **Reactivate Suspended LAG** Reactivates a port if the LAG has been disabled through the locked port security option.
- **Operational Status** Defines whether the LAG is currently operational or non-operational.
- Admin Auto Negotiation Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.
- Current Auto Negotiation The current Auto Negotiation setting.
- Admin Advertisement Specifies the capabilities to be advertised by the LAG. The possible field values are:
  - Max Capability Indicates that all LAG speeds and Duplex mode settings can be accepted.
  - 10 Half Indicates that the LAG is advertising a 10 mbps speed and half Duplex mode setting.



- 10 Full Indicates that the LAG is advertising a 10 mbps speed and full Duplex mode setting.
- 100 Half —Indicates that the LAG is advertising a 100 mbps speed and half Duplex mode setting.
- 100 Full Indicates that the LAG is advertising a 100 mbps speed and full Duplex mode setting.
- 1000 Indicates that the LAG is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- Neighbor Advertisement The neighbor LAG (the LAG to which the selected interface is connected) advertises its capabilities to the LAG to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- Admin Speed The configured speed at which the LAG is operating.
- Current LAG Speed The current speed at which the LAG is operating.
- Admin Flow Control Enables or disables flow control or enables the auto negotiation of flow control on the LAG.
- Current Flow Control The user-designated Flow Control setting.

### **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 portgroups. Each group is comprised of ports with the same speed. To define LACP:

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

5

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### LACP Page

#### LINKSYS SFE 2000P LACP Help System LACP System Priority Admin Bridging Unit Number 🛛 💌 Port Management Port Settings CAG Management LAG Management LAG Settings Port Port Priority LACP Timeout Edit 1/e1 1 Long 1/e2 Edit - ACP - PoE Settings Long 1/e3 Edit Long 💼 VLAN Manager Spanning Tree Edit 1/e4 Long Multicast Routing Cecurity Suite Edit 1/e5 Long Edit 1/e6 Long Edit 1/e7 Long Edit 1/e8 Long 1/e9 Long Edit 1/e10 Long 1/e11 Long Edit 1/e12 1 Long

The LACP Page contains fields for configuring LACP LAGs.

- LACP System Priority Indicates the global LACP priority value. The possible range is 1-65535. The default value is 1.
- Unit Number Displays the stacking member for which LACP information is defined.
- **Port** Defines the port number to which timeout and priority values are assigned.
- **Port Priority** Defines the LACP priority value for the port. The field range is 1-65535.
- LACP Timeout Administrative LACP timeout. The possible field values are:
  - Short Defines a short timeout value.
  - Long Defines a long timeout value. This is the default value.

#### Modify LACP Parameter Settings

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



#### LACP Parameter Settings Page

SFE 2000P		LINKSYS	
	LACP Parameters Settings		
Port	1/e1 💌		
LACP Port Priority	1		
LACP Timeout	Long 💌		
	Apply		

The LACP Parameter Settings Page contains the following fields:

- Port Defines the port number to which timeout and priority values are assigned.
- LACP Port Priority Defines the LACP priority value for the port. The field range is 1-65535.
- LACP Timeout Administrative LACP timeout. The possible field values are:
  - Short Defines a short timeout value.
  - Long Defines a long timeout value. This is the default value.
- 3. Define the relevant fields.
- 4. Click Apply. The LACP Parameters settings are defined, and the device is updated.

5

Chapter

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

6

# **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

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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.

<b>Properties</b>	Page
-------------------	------

LINKSYS A Division of Court Systems, Inc.						
SFE 2000P	Propert	es				Help
🖻 💼 Admin 🖶 🂼 Statistics		Туре	Authentication			
in an analisius	ID	Name				Guide
Address Tables	10	Static	Enabled	Edit		
Port Management  VLAN Management  Properties  Membership Interface Setting	<b>I</b> 100	Default	Enabled Delete	Edit Add		Logout
GVRP Settings			Back	Next		
⊕ <mark>●</mark> Security Suite ⊕ ● Quality of Service						
						-
						Elisco Frattina alto-anto-

The Properties Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- VLAN Name Displays the user-defined VLAN name.
- **Type** Displays the VLAN type. The possible field values are:
  - Dynamic Indicates the VLAN was dynamically created through GARP.
  - Static Indicates the VLAN is user-defined.
  - Default Indicates the VLAN is the default VLAN.
- Authentication Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - Enable Enables unauthorized users to use the Guest VLAN.
  - Disable Disables unauthorized users from using the Guest VLAN.
- 2. Click the Add button. The Add VLAN Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Add VLAN Page



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

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

#### Modifying VLANs

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

Auth	entication V	/LAN Settings Page
SFE 2000P		
/	Authenticatio	n VLAN Settings
VLAN ID	10	
VLAN Name		
Disable Auther	ntication 🔽	
		Apply

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

- VLAN ID Displays the VLAN ID.
- VLAN Name Displays the VLAN name.
- **Disable Authentication** Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - Enable Enables unauthorized users to use the Guest VLAN.
  - *Disable* Disables unauthorized users from using the Guest VLAN.
- Unit Number Displays the stacking member for which the VLAN parameters are displayed.
- 3. Define the relevant fields.
- 4. Click Apply. The VLAN Settings are defined, and the device is updated.

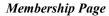
6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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 Christian of Clause Systems, No.		
SFE 2000P	Membership	Help
System     Admin     Source Statistics     Stridging     Address Tables     Port Management	VLAN Name VLAN Type Default	Support Guide
VLAN Management Properties Membership Interface Setting GVRP Settings	C       Ports       Of Unit       1 ▼       C       LAGs         Interface       Interface       Status         1/e1       Untagged       Edit	Logout
Spanning Tree Multicast ⊕ Routing ⊕ Security Suite ⊕ Quality of Service	1/e2     Untagged     Edit       1/e3     Untagged     Edit       1/e4     Untagged     Edit	
	1/e5     Excluded     Edit       1/e6     Untagged     Edit       1/e7     Untagged     Edit	
	1/e9 Untaqged Edit 1/e9 Untaqqed Edit	

The Membership Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- VLAN Name Displays the VLAN name.
- VLAN Type Indicates the VLAN type. The possible field values are:
  - Dynamic -- Indicates the VLAN was dynamically created through GARP.
  - Static Indicates the VLAN is user-defined.
  - Default Indicates the VLAN is the default VLAN.
- **Port** Indicates that ports are indicated in the page.
- LAG Indicates that LAGs are indicated in the page.
- Of Unit Displays the stacking member for which the VLAN parameters are displayed.
- Interface Displays the interface configuration being displayed.
- Interface Status Indicates the interface status. the options areas follows:



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

#### SFE 2000P Edit VLAN Membership VLAN I 100 VLAN Name Interface 1/e1 Interface Status Unflagged V

Edit VLAN Membership Page

The Edit VLAN Membership Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- VLAN Name Displays the VLAN name.
- Interface Displays the port or LAG attached to the VLAN.
- Interface Status Displays the current interface status.
- 3. Define the relevant fields.
- 4. Click Apply. VLAN Membership is modified, and the device is updated.

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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.

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

SFE 2000P	Interfa	ice Setti	ng				Help
💼 System	• Ports	Of Unit 1 💌 🐇	ି LAG	s			Support
Statistics	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering		Guide
Address Tables	1/e1	Trunk	100	Admit All		Edit	
	1/e2	Trunk	100	Admit All	Enable	Edit	Logout
	1/e3	Trunk	100	Admit All	Enable	Edit	
Interface Setting     GVRP Settings	1/e4	Trunk	100	Admit All	Enable	Edit	
Spanning Tree	1/e5	Trunk	100	Admit All	Enable	Edit	
en Routing	1/e6	Trunk	100	Admit All	Enable	Edit	
en Security Suite	1/e7	Trunk	100	Admit All	Enable	Edit	
	1/e8	Trunk	100	Admit All	Enable	Edit	
-	1/e9	Trunk	100	Admit All	Enable	Edit	
	1/e10	Trunk	100	Admit All	Enable	Edit	
	1/e11	Trunk	100	Admit All	Enable	Edit	
)·	1/e12	Trunk	100	Admit All	Enable	Edit	<b>I</b>

Interface Setting Page

The VLAN Interface Setting Page contains the following fields:

- **Port** Indicates that ports are indicated in the page.
- LAG Indicates that LAGs are indicated in the page.
- Of Unit Displays the stacking member for which the VLAN parameters are displayed.
- Interface The port number included in the VLAN.
- Interface VLAN Mode Indicates the port mode. Possible values are:
  - *General* The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - Access The port belongs to a single untagged VLAN. When a port is in Access mode, the
    packet types which are accepted on the port (packet type) cannot be designated. It is also not
    possible to enable/disable ingress filtering on an access port.



- *Trunk* The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
- PVID Assigns a VLAN ID to untagged packets. The possible values are 2 to 4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.
- Frame Type Packet type accepted on the port. Possible values are:
  - Admit Tag Only Indicates that only tagged packets are accepted on the port.
  - Admit All -- Indicates that both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** Enables or disables Ingress filtering on the port. Ingress filtering discards packets which do not include an ingress port.
- 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 VLAN Interface Settings Page opens:

# SFE 2000P VLAN Interface Settings Interface 11/e1 VLAN Mode Trunk PVID 100 Frame Type Admit All Ingress Filtering Enable Apply

VLAN Interface Settings Page

The VLAN Interface Settings Page contains the following fields:

- Interface The port number included in the VLAN.
- VLAN Mode Indicates the port mode. Possible values are:
  - General The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - Access The port belongs to a single untagged VLAN. When a port is in Access mode, the
    packet types which are accepted on the port (packet type) cannot be designated. It is also not
    possible to enable/disable ingress filtering on an access port.
  - *Trunk* The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

Chapter 6:

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **PVID** Assigns a VLAN ID to untagged packets. The possible values are 2 to 4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.
- Frame Type Packet type accepted on the port. Possible values are:
  - Admit Tag Only -- Indicates that only tagged packets are accepted on the port.
  - Admit All Indicates that both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** Enables or disables Ingress filtering on the port. Ingress filtering discards packets which do not include an ingress port.
- 3. Define the relevant fields.
- 4. Click Apply. The VLAN Interface settings are modified, and the device is updated.

6

# **Configuring GVRP Settings**

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

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

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

SFE 2000P	GVRP Settings	Help
System Admin	GVRP Global Status Disable 💌	Suppor
Statistics Bridging Address Tables	Copy From Entry Number To Entry Number(s) (E	Example: 1,3,5-10)
	○ Ports Of Unit	Logout
	# Interface GVRP State Dynamic GVRP VLAN Creation Registration	
GVRP Settings	1 1/e1 Disabled Enabled Enabled Edit	
Multicast Routing	2 1/e2 Disabled Enabled Enabled Edit	
Security Suite Quality of Service	3 1/e3 Disabled Enabled Enabled Edit	
Guanty of Service	4 1/e4 Disabled Enabled Enabled Edit	
	5 1/e5 Disabled Enabled Enabled Edit	
	6 1/e6 Disabled Enabled Enabled Edit	
	7 1/e7 Disabled Enabled Enabled Edit	
	8 1/e8 Disabled Enabled Enabled Edit	

#### **GVRP** Settings Page

The GVRP Settings Page contains the following fields:

- GVRP Global Status Indicates if GVRP is enabled on the device. The possible field values are:
  - Enable -- Enables GVRP on the selected device.
  - Disable Disables GVRP on the selected device.
- Copy from Entry Number Indicates the row number from which GVRP parameters are copied.
- To Entry Number Indicates the row number to which GVRP parameters are copied
- **Port** Indicates the port number on which GVRP is enabled.
- LAGs Indicates the LAG number on which GVRP is enabled.
- Of Unit Displays the stacking member for which the GVRP parameters are displayed.

Chapter 6:

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Interface Displays the interface on which GVRP is enabled.
- GVRP State Indicates if GVRP is enabled on the interface. The possible field values are:
  - Enabled Enables GVRP on the selected interface.
  - Disabled Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - Enable Enables Dynamic VLAN creation on the interface.
  - Disable Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  - Enable Enables GVRP registration on the device.
  - Disable Disables GVRP registration on the device.
- 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 2000P		LINKSYS A Distance of Disco Systems, Inc.
	Edit GVRP	
Interface	⊙ Port 1/e1 ▼ ○ LAG 1 ▼	
GVRP State	Disable 💌	
Dynamic VLAN Creation	Enable 💌	
GVRP Registration	Enable 💌	
	Apply	

The Edit GVRP Page contains the following fields:

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

6

- Enabled Enables GVRP on the selected interface.
- Disabled Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - Enable Enables Dynamic VLAN creation on the interface.
  - Disable Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  - Enable Enables GVRP registration on the device.
  - Disable -- Disables GVRP registration on the device.
- 3. Define the relevant fields.
- 4. Click Apply. GVRP settings are modified, and the device is updated.

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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.

NOTE: This setting is relevant only in Layer 2 mode.

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

SFE 2000	Protocol Group	Help
<ul> <li>System</li> <li>Admin</li> <li>Bridging</li> <li>Address Tables</li> <li>Port Management</li> <li>VLAN Management</li> <li>Membership</li> <li>Interface Settings</li> <li>Protocol Port</li> <li>Spanning Tree</li> <li>Multicast</li> <li>Security Suite</li> <li>Quality of Service</li> </ul>	Frame Type Protocol Value Group ID (Hex) Delete Add	Support Guide Logout

**Protocol Group Page** 

The Protocol Group Page contains the following fields:

- Frame Type Displays the packet type. Possible field values are Ethernet, RFC1042, and LLC Other.
- **Protocol Value** Displays the User-defined protocol name.
- Group ID (Hex) Defines the Protocol group ID to which the interface is added. Range is 1-2147483647.
- 2. Click the Add Button. The Add Protocol Group Page opens:

6

#### Add Protocol Group Page

SFE 2000P		LINKSYS A Dividier of Dave Systems, Inc.
	Add Protocol Group	
Frame Туре	Ethernet 💌	
Protocol Value	Protocol Value     P     F     Ethernet-Based Protocol Value	(Hex Format
Group ID		
		Apply

The *Add Protocol Group Page* provides information for configuring new VLAN protocol groups. The *Add Protocol Group Page* contains the following fields.

- Frame Type Displays the packet type. Possible field values are Ethernet, RFC1042, and LLC Other.
- Protocol Value Displays the User-defined protocol value. The options are as follows:
  - Protocol Value --- The value is entered in Hex format.
  - Ethernet-Based Protocol Value -- The value is selected as either IP, IPX, IPv6., or ARP
- Group ID (Hex)— Defines the Protocol group ID to which the interface is added.
- 3. Define the relevant fields.
- 4. Click Apply. The Protocol Group is added, and the device is updated.

Modifying Protocol Groups

The Edit Protocol Group Page provides information for configuring new VLAN protocol groups

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

#### Edit Protocol Group Page

SFE 2000P			LINKSYS A Dividier of Data Systems, Inc.
	Edit P	Protocol Group	
	Frame Type	Ethernet	
	Protocol Value	a1b1	
	Group ID (Hex)	1	
		Apply	

The Edit Protocol Group Page contains the following fields.

Chapter 6:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Frame Type Displays the packet type. Possible field values are Ethernet, RFC1042, and LLC Other.
- **Protocol Value** Displays the User-defined protocol value.
- Group ID (Hex) Defines the Protocol group ID to which the interface is added.
- 3. Define the relevant fields.
- 4. Click Apply. The Protocol group is modified, and the device is updated.

## **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:

	Protocol Port Page	
LINKSYS A Division of Cisco Systems, Inc.		
SFE 2000 System Admin Statistics Bridging Address Tables Port Management VAN Management VAN Management VAN Management OVER Setting OVER Setting OVER Setting Protocol Forup Protocol Port Spanning Tree Multicast Security Suite Cuality of Service	Protocol Port	Help Support Guide Logout
		Cost brune A

The Protocol Port Page contains the following fields.

- Interface Port or LAG number added to a protocol group.
- **Protocol Group ID** Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- VLAN ID Attaches the interface to a user-defined VLAN ID. Protocol ports can either be attached to a VLAN ID or a VLAN name.
- 2. Click the Add Button. The Add Protocol Port to VLAN Page opens:



The Add Protocol Port to VLAN Page provides information for editing protocol port configurations.

Add Protocol Port to VLAN Page

SFE 2000P			LINKSYS A Divideor of Daco Systems, Inc.
	Add Prote	ocol Port to VLAN	
	Interface Group ID VLAN ID VLAN Name		
		Apply	

The Add Protocol Port to VLAN Page contains the following fields.

- **Interface** Port or LAG number added to a protocol group.
- **Group ID** Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- VLAN ID Attaches the interface to a user-defined VLAN ID.
- VLAN Name Attaches the interface to a user-defined VLAN Name.
- 3. Define the relevant fields.
- 4. Click Apply. The protocol ports are mapped to VLANs, and the device is updated.

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

Chapter 6:

7

# **Configuring IP Information**

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

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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
- Host Mapping

#### **Defining DNS Server**

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:

LINKSYS A Division of Cloud Systems, Inc.		
SFE 2000P System System Management Zoom Stack Management Health Health P Addressing Domain Name System NMP Admin Stack Management Health P Addressing Host Mapping SMMP Admin Statistics Bridging Source Poly Servere Host Mapping Source Source Bridging Source Duality of Service	DNS Servers	Help Support Guide Logout
		Cited Stations

The DNS Servers Page contains the following fields.

- Enable DNS Enables translating the DNS names into IP addresses. The possible field values are:
  - Checked Translates the domains into IP addresses.
  - Unchecked Disables translating domains into IP addresses.
- **Default Domain Name** (1 -158 Characters) Specifies the user-defined DNS server name.

DNS Servers Page



- Type Displays the IP address type. The possible field values are:
  - Dynamic The IP address is dynamically created.
  - Static The IP address is a static IP address.
- **Remove** Removes DNS servers. The possible field values are:
  - Checked Removes the selected DNS server
  - Unchecked Maintains the current DNS server list.
- **DNS Server** Displays the DNS server's IP address.
- Active Server— Specifies the DNS server that is currently active.
- 2. Click the Add button. The Add DNS Server Page opens:

#### Add DNS Server Page

SFE 2000P		LINKSYS A Unider of Disco Spatiana, Inc.
	Add DNS Server	
DNS Server		
DNS Server Currently Active		
Set DNS Server Active		
	Apply	

The *Add DNS Server Page* allows system administrators to define new DNS servers. The Add DNS Server Page page contains the following fields.

- DNS Server Displays the DNS server's IP address.
- DNS Server Currently Active Displays the DNS server which is currently active.
- Set DNS Server Active Indicates the DNS to be server activated.
- 3. Define the relevant fields.
- 4. Click Apply. The DNS server is added, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **Host Mapping**

The *Host Mapping Page* provides information for defining DNS Host Mapping. The *DNS* Host Mapping Page page contains the following fields.

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

Host Mapping Page			
LINKSYS A Dation of Graz Systems, Inc			
SFE 2000P System System Management System Information Stack Management Health Reset Time Damain Name System Host Mapping Stack Mapping Stack Management Host Mapping Stack Ma	Isst Names   P Address   Delote	Help Suppor Guide Logout	
		Kasamatak	

The Host Mapping Page contains the following fields:

- Host Names Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- IP Address Displays the DNS host IP address.
- 2. Click the Add button. The Add DNS Host Page opens:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# 7

#### Add DNS Host Page

SFE 2000P	LINKSYS A Disables of Data Systems, Inc.
Add DNS Ho	st
Host Name	
IP Address	
Apply	

The Add DNS Host page contains the following fields:

- Host Name Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- IP Address Displays the DNS host IP address.
- 3. Define the relevant fields.
- 4. Click Apply. The DNS Host settings are defined, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Configuring Layer 2**

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.

When the system is in stacking mode with a Backup Master present, configure the IP address as a static address. This prevents disconnecting from the network during a Stacking Master switchover.

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:

- IP Interface
- ARP

#### **IP Interface**

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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### IP Interface Page

SGE 2000 System Management System Mormation System Information Back Management Help Support Support Support Support Guide IP Address Management VLAN P Address Management VLAN P Flixters Management VLAN P Flixters Management VLAN P Flixters P Flixters	A Diversion of Calcol Systems, Inc.		
System Management     C Get Dynamic IP from DHCP Server     Guide       J Com     Static IP Address     Guide       Stack Management     Management VLAN     IO       Health     IP Address     IO.6.25149       Time     P In Addressing     Network mask       25256.256.224     Prefix Length       27     Domain Name System	SGE 2000	IP Interface	Help
Admin Statistics Security Suite Quality of Service Apply	System Management 	C       Static IP Address         Management VLAN       100 ▼         IP Address       106.25.149         C       Network mask         255 255 252 24       27         User Defined Default Gateway       106.25.129         Active Default Gateway       108.25.129         Remove User Defined       □	Guide

The IP Interface Page contains the following fields:

- Get Dynamic IP from DHCP Server Retrieves the IP addresses using DHCP.
- Static IP Address Displays the currently configured IP address. IP addresses are either configured on the Default VLAN or are user-defined.
- Management VLAN Sets the management VLAN. The switch uses this VLAN to watch for management packets from Telnet and web browser management sessions.
- IP Address Indicates the IP address.
- Network Mask Displays the currently configured IP address mask.
- **Prefix Length** Specifies the number of bits that comprise the source IP address prefix, or the network source IP address mask.
- User Defined Default Gateway Defines the default gateway IP address.
- Active Default Gateway Indicates if the default gateway is active.
- **Remove User Defined** Removes the selected IP address from the interface. The possible field values are:
  - Checked Removes the IP address from the interface.
  - Unchecked Maintains the IP address assigned to the Interface.

#### 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

Chapter 7:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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:

	ARP Page	
INKSYS Islon of Circo Systems, Inc.		
SGE 2000	ARP	Help
System System Management 	ARP Entry Age Out     60000     (Sec)       Clear ARP Table Entries     None	Support
System Information     Stack Management     Health     Reset	Interface IP Address MAC Address Status     VLAN 100 10.6.25.129 00:00:5e:00:01:1d Dynamic Edit	Guide
Time     P Addressing     P Interface     ARP	□ VLAN 100 10.6.25.130 00:13:20:cb:4d:b0 Dynamic Edit	
Domain Name System	Apply Add	
Statistics Bridging Security Suite Quality of Service		

The ARP Page contains the following fields.

- **ARP Entry Age Out** Defines the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 1 40000000, where zero indicates that entries are never cleared from the cache. The default value is 60,000 seconds.
- Clear ARP Table Entries— Indicates the type of ARP entries that are cleared on all devices. The possible values are:
  - None ARP entries are not cleared.
  - All All ARP entries are cleared.
  - Dynamic Only dynamic ARP entries are cleared.
  - Static Only static ARP entries are cleared.
- Interface Indicates the interface connected to the device.
- **IP Address** Indicates the station IP address, which is associated with the MAC address filled in below.



- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- Status Indicates the ARP Table entry status. Possible field values are:
  - Dynamic Indicates the ARP entry was learned dynamically.
  - Static Indicates the ARP entry is a static entry.
- 2. Click on the Add ARP button. The ARP Settings Page opens:

#### **ARP Settings Page**

No. of Colored	SFE 2000P		LINKSYS A Shidder of Dave Systems, Inc.	
00000000		ARP Settings		
	Interface	© Port 1/e1 🔽 🔿 LAG 1 🔽 🔿 VLAN 10 💌		
	IP Address	0.0.0.0		
	MAC Address			
		Apply		

The ARP Settings Page contains the following fields:

- Interface Indicates the interface connected to the device.
- **IP** Address Indicates the station IP address, which is associated with the MAC address filled in below.
- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- 3. Define the relevant fields.
- 4. Click **Apply.** The ARP Settings are defined, and the device is updated.

#### Modifying ARP Settings

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **ARP Settings Page**

SFE 2000P		LINKSYS A Gindler of Disco Tystems, Inc.
	ARP Settings	
Interface	⊙ Port 3/e1 ▼ ⊖ LAG 1▼ ⊖ VLAN 10 ▼	
IP Address	10.6.25.134 💌	
MAC Address	00:d0:b7:9e:f7:36	
Status	Dynamic 💌	
	Apply	

The ARP Settings Page contains the following fields:

- Interface Indicates the interface connected to the device.
- IP Address Indicates the station IP address, which is associated with the MAC address filled in below.
- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- Status Indicates the ARP Table entry status. Possible field values are:
  - Dynamic Indicates the ARP entry was learned dynamically.
  - Static Indicates the ARP entry is a static entry.
- 3. Define the relevant fields.
  - Click Apply. The ARP Settings are modified, and the device is updated.

7

# **Configuring Layer 3**

In Layer 3 mode, multiple IP addresses can be configured on ports, LAGs or VLANS. This provides greater network flexibility than Layer 2 mode where only a single IP address is configured on ports, LAGs or VLANS. A predefined Default Gateway is not provided in Layer 3. To manage the device remotely, a default route is defined. The Default Route is the route with the next hop of 0.0.0.0. The Default Route is defined in the *IP Routing Page*.

This section provides information for configuring Layer 3 features, and includes the following topics:

- Configuring IP Addressing
- Defining IP Routing

#### **Configuring IP Addressing**

The IP Addressing subsection contains the following pages:

- IP Interface
- ARP Proxy
- UDP Relay
- DHCP Relay
- ARP

#### **IP Interface**

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.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **IP** Interface Page

SFE 2000	IP Interface	Help
System		Suppo
- <del>Ca</del> System Management	□ IP Address Mask Interface Type	
	10.6.25.148 255.255.255.224 VLAN 100 Static Edit	Guide
- Stack Management		
	Delete Add	Logou
- Time		
UDP Relay		
ARP 		

The IP Interface Page contains the following fields.

- IP Address Defines the system IP address.
- Mask Displays the currently configured IP address mask.
- Interface Indicates the interface connected to the device.
- Type Indicates if the IP address has been configured statically or added dynamically.
- Remove Removes the selected IP address from the interface. The possible field values are:
  - Checked Removes the IP address from the interface.
  - Unchecked Maintains the IP address assigned to the Interface.

A table containing the IP Interface configurations is displayed containing the following fields:

- IP Address Defines the system IP address.
- Mask Displays the currently configured IP address mask.
- Interface Displays the interface used to manage the device.
- 2. Click the Add button. The Add IP Interface Page opens:

The Add IP Interface Page allows network managers to create new system IP addresses.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Add IP Interface Page

SFE 2000P		LINKSYS A Dinkier af Disc Spatiene, Inc.
	Add IP	Interface
Interface		C Port 1/e1 C LAG 1 C VLAN 10 V
Static IP Address		
Source IP Address		
Network Mask		
OPrefix Length		
	Apply	

The Add IP Interface Page contains the following fields.

- Interface Defines the system IP address.
- Source IP Address Defines the source IP Address.
- Static IP Address Defines the system IP address.
- Network Mask Displays the currently configured IP address mask.
- **Prefix Length** Specifies the number of bits that comprise the source IP address prefix, or the network source IP address mask.

#### Modifying IP Interfaces

- 1. Click System > System Management > IP Addressing > IP Interface. The *IP Interface Page* opens:
- 2. Click the Edit Button. The IP Interface Settings Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **IP Interface Settings Page**

SFE 2000P		LINKSYS A Unidee of Class Systems, Inc.
	IP Interface Settings	
IP Address	10.6.25.148 💌	
Network Mask	255.255.255.224	
🔿 Prefix Length	/27	
Interface		
Туре	Static	
	Apply	

#### IP Interface Settings

The IP Interface Settings Page contains the following fields:

- IP Address Defines the system IP address.
- Network Mask Displays the currently configured IP address mask.
- **Prefix Length** Specifies the number of bits that comprise the source IP address prefix, or the network source IP address mask
- Interface Defines the system IP address.
- Type Indicates if the IP address has been configured statically or added dynamically.
- 3. Modify the relevant fields.
- 4. Click Update. The IP Interface Settings are modified, and the device is updated.

#### **ARP Proxy**

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. The *ARP Proxy Page* allows network managers to enable ARP Proxy on the switch.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### ARP Proxy Page

LINKSYS A Division of Cisco Systems, Inc.		
SFE 2000	ARP Entry Age Out (Sec) Clear ARP Table Entries None	Help Support Guide
System Information Stack Management Health Reset Time P Addressing P Interface ARP Proxy UDP Relay DHCP Relay	Interface       IP Address       MAC Address       Status         VLAN 100       10.6.25.129       00.00.5e:00.01.1d       Dynamic       Edit         Delete       Add	Logout
Domain Name System		

The ARP Proxy Page contains the following field.

- **ARP Proxy** Enables the device to respond to ARP requests for located nodes. If disabled, the device responds with its own MAC address.
- 2. Enable ARP Proxy.
- 3. Click Apply. Arp Proxy is enabled, and the device is updated.

#### **UDP Relay**

The UDP Relay allows UDP packets to reach other networks. This feature enables browsing from workstations to servers on different networks. The UDP Relay Page contains the following fields.

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

7

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### UDP Relay Page

LINKSYS A Deliser of Clices Systems, Inc.	
System   System Information   System Information   System Information   Stack Management   Health   Reset   Time   IP PAddressing   IP PAdressing   IP Padressing   Dip Relay   Domain Name System   SMMP   Some   Sististics   Sististics	Help Support Guide Logout
	Cisco Systems

The UDP Relay Page contains the following fields:

- **Source IP Interface** Indicates the input IP interface that relays UDP packets. If this field is 255.255.255, UDP packets from all interfaces are relayed. The following address ranges are
  - 0.0.0.0 to 0.255.255.255.
  - 127.0.0.0 to 127.255.255.255.
- **UDP Destination Port** Indicate the destination UDP port ID number of the relayed UDP packets. The following table lists UDP Port allocations.

UDP Port Number	Acronym	Application
7	Echo	Echo
11	SysStat	Active User
15	NetStat	Netstat
17	Quote	Quote of the day
19	CHARGEN	Character Generator
20	FTP-data	FTP Data
21	FTP	FTP
37	Time	Time
42	NAMESERVE	Host Name Server

#### **UDP Port Number**

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



UDP Port Number	Acronym	Application
43	NICNAME	Who is
53	DOMAIN	Domain Name Serve
69	FTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
123	NTP	Network Tim
137	NetBiosNameService	NT Server to StationConnections
138	NetBiosDatagramService	NT Server to StationConnections
139	NetBios SessionServiceNT	Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who	Unix Rwho Daemon
525	timed	Time Daemon
514	syslog	System Log

#### **UDP Port Number**

- **Destination Address** The IP interface that receives UDP packet relays. If this field is 0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.
- 2. Click the Add button. The Add UDP Relay Page opens:

#### Add UDP Relay Page

SFE 2000P			LINKSYS A División of Dava Systems, Inc.
	Add UD	P Relay	
		-	
Source IP Interface	10.6.25.148 💌		
UDP Destination Port	1		
Destination Address	0.0.0.0	(X.X.X.X)	
Apply			

The Add UDP Relay Page contains the following fields:

- Source IP Interface Indicates the input IP interface that relays UDP packets. If this field is 255.255.255, UDP packets from all interfaces are relayed. The following address ranges are
  - 0.0.0.0 to 0.255.255.255.

Chapter 7:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- 127.0.0.0 to 127.255.255.255.
- **UDP Destination Port** Indicate the destination UDP port ID number of the relayed UDP packets. The following table lists UDP Port allocations
- **Destination Address** The IP interface that receives UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255, UDP packets are flooded to all IP interfaces.
- 3. Define the relevant fields.
- 4. Click Apply. The UDP Relay Settings are defined, and the device is updated.

#### **DHCP Relay**

The *DHCP Relay Page* provides information for establishing a DHCP configuration with multiple DHCP servers to ensure redundancy. IP Addresses are controlled and distributed one-by-one to avoid overloading the device

 Click System > System Management > IP Addressing > DHCP Relay. The DHCP Relay Page opens:

LINKSYS Division of Chase Systems, Inc.	DHCP Relay Page	
SFE 2000	DHCP Relay Dealer	Help
System Information Stack Management Health Reset Time P Addressing P Interface ARP Proxy OHCP Relay ARP ARP ARP Relay ARP C OHCP Relay C ARP C C C C C C C C C C C C C C C C C C C	DHCP Server      Delete     Add  Apply	Guide
Admin Bridging		

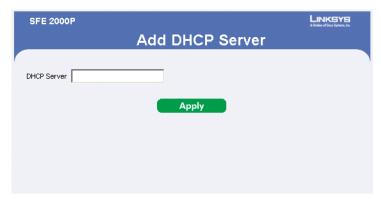
The DHCP Relay Page contains the following fields:

- DHCP Relay— Enable or Disables DHCP on the device.
- **DHCP Server** Adds a DHCP Server to the DHCP Relay Table. The DHCP servers act as a DHCP relay if the parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to respond first.
- 2. Click the Add button. The Add DHCP Server Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Add DHCP Server Page



The Add DHCP Server Page contains the following field:

- **DHCP Server** —Adds a DHCP Server to the DHCP Relay Table. The DHCP servers act as a DHCP relay if the parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to respond first.
- 3. Define the relevant field.
- 4. Click Apply. THe DHCP Server is added, and the device is updated.

#### 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:

7

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### ARP Page

SFE 2000	ARP	Help
System	ARP Entry Age Out 60000 (Sec) Clear ARP Table Entries None	Support
Stack Management Health Reset Time P Addressing P Interface ARP Proxy DUP Relay DUP Relay Duch Relay Consin Name System AMP Admin	Interface     IP Address     MAC Address     Status       VLAN 100     10.6.25.129     00:00:5e:00:01:1d     Dynamic     Edit       Delete     Add	Logout
n 💼 Statistics n 💼 Bridging	a	

The ARP Page contains the following fields.

- **ARP Entry Age Out** Defines the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 1 40000000, where zero indicates that entries are never cleared from the cache. The default value is 60,000 seconds.
- Clear ARP Table Entries— Indicates the type of ARP entries that are cleared on all devices. The possible values are:
  - None ARP entries are not cleared.
  - All All ARP entries are cleared.
  - Dynamic Only dynamic ARP entries are cleared.
  - Static Only static ARP entries are cleared.
- Interface Indicates the interface connected to the device.
- **IP Address** Indicates the station IP address, which is associated with the MAC address filled in below.
- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- Status Indicates the ARP Table entry status. Possible field values are:
  - Dynamic Indicates the ARP entry was learned dynamically.

- *Static* Indicates the ARP entry is a static entry.
- 2. Click on the **Add ARP** button. The *ARP Settings Page* opens:

#### ARP Settings Page

SFE 2000P		LINKSYS A Division of Dace Systems, Inc.
	ARP Settings	
Interface	© Port 1/e1 ▼ C LAG 1 ▼ C VLAN 10 ▼	
IP Address	0.0.0	
MAC Address		
	Apply	

The ARP Settings Page contains the following fields:

- Interface Indicates the interface connected to the device.
- IP Address Indicates the station IP address, which is associated with the MAC address filled in below.
- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- 3. Define the relevant fields.
- 4. Click **Apply.** The ARP Settings are defined, and the device is updated.

#### Modifying ARP Settings

\_

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **ARP Settings Page**

SFE 2000P		LINKSYS A Direktor of Disco Typiteres, Inc.
	ARP Settings	
Interface	⊙ Port 3/e1 ▼ C LAG 1▼ C VLAN 10 ▼	
IP Address	10.6.25.134 💌	
MAC Address	00:d0:b7:9e:f7:36	
Status	Dynamic 💌	
	Apply	

The ARP Settings Page contains the following fields:

- Interface Indicates the interface connected to the device.
- **IP Address** Indicates the station IP address, which is associated with the MAC address filled in below.
- MAC Address Indicates the station MAC address, which is associated in the ARP table with the IP address.
- Status Indicates the ARP Table entry status. Possible field values are:
  - Dynamic Indicates the ARP entry was learned dynamically.
  - Static Indicates the ARP entry is a static entry.
- 3. Define the relevant fields.
- 4. Click Apply. The ARP Settings are modified, and the device is updated.

#### **Defining IP Routing**

Once the switch has been defined as a router, statics routes can be defined. To define IP Routing:

1. Click **Routing** > **IP Routing**. The *IP Routing Page* opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### **IP** Routing Page

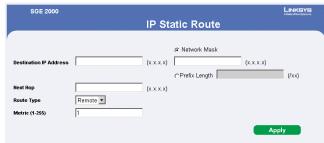
LINKSYS A Debider of Disco Systems, Inc.		
A Budda d' Clas System, sc SGE 2000 System Admin Statistics Bridging Routing Brouting Brouting Brouting Construction Security Suite Construction Security Suite Construction Security Suite	IP Routing	Help Support Guide Logout

The IP Routing Page contains the following fields:

- Dest. IP Address Defines the destination IP address.
- **Prefix Length** Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash (/).
- Next Hop Indicates the next hop's IP address or IP alias on the route.
- **Route Type** Defines the route type. The possible field values are:
  - Reject Rejects the route, and stops routing to the destination network via all gateways.
  - *Remote* Indicates the route is a remote path.
- Metric Indicates the administrative distance to the next hop. The range is 1-255. The default value is 1.
- 2. Click the Add button. The IP Static Route Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **IP Static Route Page**



The IP Static Route Page contains the following fields:

- **Destination IP Address** Defines the destination IP address.
- **Prefix Length** Defines the IP route prefix for the destination IP. The prefix length must be preceded by a forward slash (/).
- Next Hop Indicates the next hop's IP address or IP alias on the route.
- Route Type Defines the route type. The possible field values are:
  - Reject Rejects the route, and stops routing to the destination network via all gateways.
  - *Remote* Indicates the route is a remote path.
- Metric Indicates the administrative distance to the next hop. The range is 1-255. The default value is 1.
- 3. Define the relevant fields.
- 4. Click Apply. The IP Static route is added, and device is updated.

8

# **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

8

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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:

Static Page

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

	5	
LINKSYS A Division of Cisco Systems, Inc.		
SFE 2000P	Static	Help
🗄 🦰 System 🗟 📩 Admin	VLAN ID MAC Address Interface Status	Support
⊕Statistics ⊜Bridging ↓Address Tables	Delete Add	Guide
Static		Logout
Port Management     VLAN Management     Spanning Tree		
Multicast B Conting B Courity Suite		
🗄 💼 Quality of Service		
		Cost System

The Static Page contains the following fields:

- VLAN ID Displays the VLAN ID number to which the entry refers.
- MAC Address Displays the MAC address to which the entry refers.
- Interface Displays the interface to which the entry refers:
  - Port The specific port number to which the forwarding database parameters refer.
  - LAG The specific LAG number to which the forwarding database parameters refer.
- Status Displays how the entry was created. The possible field values are:
  - Permanent The MAC address is permanent.
  - Delete on Reset The MAC address is deleted when the device is reset.
  - Delete on Timeout The MAC address is deleted when a timeout occurs.
  - Secure The MAC Address is defined for locked ports.

8

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

Add Static MAC Address Page

SFE 2000P		LINKSYS A Unider of Dace Systems, Inc.
	Add Static MAC Address	
Interface	œPort 1/e1 ▼ CLAG 1▼	
MAC Address		
ⓒ VLAN ID	10 💌	
© VLAN Name	V	
Status	Permanent	
	Арріу	

The Add Static MAC Address Page contains the following fields:

- Unit Number Indicates the stacking member for which the Static address is defined.
- Interface Displays the interface to which the entry refers:
  - Port The specific port number to which the forwarding database parameters refer.
  - LAG The specific LAG number to which the forwarding database parameters refer.
- MAC Address Displays the MAC address to which the entry refers.
- VLAN ID Displays the VLAN ID number to which the entry refers.
- VLAN Name Displays the VLAN name to which the entry refers.
- Status Displays how the entry was created. The possible field values are:
  - Permanent The MAC address is permanent.
  - Delete on Reset The MAC address is deleted when the device is reset.
  - Delete on Timeout The MAC address is deleted when a timeout occurs.
  - Secure The MAC Address is defined for locked ports.
- 3. Define the relevant fields.
- 4. Click Apply. The Static MAC Address is added, and the device is updated.

8

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Defining Dynamic Addresses**

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

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

	Dynamic Page	
LINKSYS A Division of Divis Systems, No.		
SFE 2000P	Aging Interval       000       (Gec)         Clear Table       (Gec)       (Gec)         Cuery by:       (Gec)       (Gec)         Interface       @ Port Int III @ LAO IIII       (Gec)         MAC Address       (Gec)       (Gec)         VLAN ID       (Gec)       (Gec)         Address Table Sort Key       (MAN IN)       (Gec)	Help Support Guide Logout
	VLAN ID         MAC         Interface           Internal Use         00005600011d         3/41           Internal Use         0000560243.0         3/41           Internal Use         000320cbd88         3/41           Internal Use         001320cbd400         3/41           Internal Use         001320cbd400         3/41           Internal Use         001320cbd400         3/41           Internal Use         001320cbd405         3/41           Internal Use         0000b79ef733         3/41           Internal Use         0000b79ef733         3/41           Internal Use         0000b79ef733         3/41	

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

The Dynamic Page contains the following fields:

- Aging Interval (secs) Specifies the amount of time the MAC address remains in the Dynamic MAC Address table before it is timed out, if no traffic from the source is detected. The default value is 300 seconds.
- Clear Table If checked, clears the MAC address table.
- Interface Specifies the interface for which the table is queried. There are two interface types from which to select.

8

- MAC Address Specifies the MAC address for which the table is queried.
- VLAN ID Specifies the VLAN ID for which the table is queried.
- Address Table Sort Key Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.
- 2. Define the relevant fields.
- 3. Click Apply. Dynamic addressing is defined, and the device is updated.

8

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

Chapter 8:

9

# **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:

9

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **IGMP Snooping Page**

SFE 2000P	IGMP	Snoop	oing						Help
System Admin Statistics	Enable IG	MP Snoopir	ng Status						Suppo
Bridging Address Tables Port Management	VLAN ID	IGMP Snooping Status	Host Timeout	MRouter Timeout	Leave Timeout				Guide
VLAN Management Spanning Tree	10	Disabled	260	300	10	Edit	Ĵ.		
Comparing Compar	100 App	Disabled	260	300	10	Edit	I		

The IGMP Snooping Page contains the following fields:

- Enable IGMP Snooping Status Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
  - Enable -- Enables IGMP Snooping on the device.
  - Disable -- Disables IGMP Snooping on the device.
  - VLAN ID Specifies the VLAN ID.
  - **IGMP Snooping Status** Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
    - Enable Enables IGMP Snooping on the VLAN.
    - Disable Disables IGMP Snooping on the VLAN.
- **Host Timeout** Indicates the amount of the time the Host waits to receive a message before it times out. The default value is 260 seconds.
- **MRouter Timeout** Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- Leave Timeout Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout

9

occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.

- 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:

SFE 2000P		Linksys
	Edit IGMP Snooping	in venue in used spinoria, in.
VLAN ID	10 💌	
IGMP Status Enable	Disable 💌	
Auto-Learn	Enable 💌	
Host Timeout	260	
MRouter Timeout	300	
Leave Timeout	@ 10	
	🔿 Immediate Leave	
	Apply	

#### Edit IGMP Snooping Page

The Edit IGMP Snooping Page contains the following fields:

- VLAN ID Specifies the VLAN ID.
- **IGMP Status Enable** Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
  - Enable Enables IGMP Snooping on the VLAN.
  - Disable Disables IGMP Snooping on the VLAN.
- Auto Learn Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device. The possible field values are:
  - Enable -- Enables auto learn
  - *Disable* Disables auto learn.
  - **Host Timeout** Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
  - **MRouter Timeout** Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.

Chapter 9:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- 9
- Leave Timeout Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.
- 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 attached to the Multicast service group in the Ports and LAGs tables. 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 > Bridge Multicast> Multicast Groups. The Multicast Group Page opens:

SFE 2000P	Multicast Group	Help
n System Admin Statistics	Enable Bridge Multicast Filtering	Support
Bridging Address Tables	VLAN ID 1 💌	Guide
	Bridge Multicast Address 010005e010101	Logout
e Spanning Tree Multicast IGMP Snooping	Delete Add	
Multicast Group     Forward     Routing	C Ports Of Unit I ▼ C LAGs	
en Security Suite Cuality of Service	Interface Interface Status	
	1/e1 Non Edit	
	1/e2 Forbidden Edit	
	1/e3 Non Edit	
	1/e4 Non Edit	
	1/e5 Non Edit	
	1/e6 Non Edit	
	1/e7 Non Edit	

#### Multicast Group Page

The Multicast Group Page contains the following fields:

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

9

- Unchecked Disables IGMP Snooping on the device.
- VLAN ID Specifies the VLAN ID.
- Bridge Multicast Address Identifies the Multicast group MAC address/IP address.
- **Ports** Indicates the port number on which Multicast service is configured.
- LAGs Indicates the LAG number on which Multicast service is configured.
- **Of Unit** Displays the stacking member for which the Multicast service parameters are displayed.
- Interface Displays the interface on which the Multicast service is configured.
- Interface Status Displays the interface status. The options are as follows:
  - Static Attaches the port to the Multicast group as static member in the Static Row. The
    port/LAG has joined the Multicast group statically in the Current Row.
  - Forbidden Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
  - Non The port is not part of a Multicast group.
- 2. Click the Add button. The Add Multicast Group Page opens:

Ada Multicast	Oroup Tuge

. . . . . . . .

SFE 2000P		
	Add Multicast Group	
VLAN ID	100 💌	
Bridge IP Multicast		
Bridge Mac Multicast		
	Apply	

The Add Multicast Group Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- Bridge Multicast IP Address Displays the IP address attached to the Multicast Group.
- Bridge Multicast MAC Address Displays the MAC address attached to the Multicast Group.

#### To Modify 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

Chapter 9:

9

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Edit Multicast Group Page

SFE 2000P		LINKSYS A Disable of Data Systems, Inc.
	Edit Multicast Group	
VLAN ID	1	
Bridge IP Multicast	224-239.129 1.1.1	
Bridge Mac Multicast	01005e010101	
Interface	1/e3	
Interface Status	Non 💌	
	Apply	

The Edit Multicast Group Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- Bridge Multicast IP Address Displays the IP address attached to the Multicast Group.
- Bridge Multicast MAC Address Displays the MAC address attached to the Multicast Group.
- Interface Displays the port attached to the Multicast Group.
- Interface Status Displays the interface status. The options are as follows:
  - *Static* Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
  - *Forbidden* Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
  - *Excluded* The port is not part of a Multicast group.
  - Dynamic Attaches the port to the Multicast group as dynamic member.
- 3. Define the Multicast Group Port Settings.
- 4. Click Apply. The Multicast group parameters are saved, and the device is updated.

9

# **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:

#### Multicast Forward Page

LINKSYS A Dividuar of Circle Systema, Inc.		
SFE 2000P		Help
	C Ports Of Unit T ⊆ C LAGs	Guide
- Management	Interface Interface Status	Logout
- Spanning Tree 	1/e1 Excluded Edit	
IGMP Snooping	1/e2 Excluded Edit	
Multicast Group	1/e3 Excluded Edit	
🖮 💼 Routing 🖮 💼 Security Suite	1/e4 Excluded Edit	
Quality of Service	1/e5 Excluded Edit	
	1/e6 Excluded Edit	
	1/e7 Excluded Edit	
	1/e8 Excluded Edit	· · ·
	1/e9 Excluded Edit	
	1/e10 Excluded Edit	
	1/e11 Excluded Edit	
	1/e12 Excluded Edit	
		Constanting of the second s

The Multicast Forward Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- Ports Indicates the port number on which Multicast service is configured.
- LAGs Indicates the LAG number on which Multicast service is configured.
- Of Unit Displays the stacking member for which the Multicast service parameters are displayed.
- Interface Displays the port attached to the Multicast Group.
- Interface Status Displays the interface status. The options are as follows:
  - Static Attaches the port to the Multicast group as static member.
  - *Forbidden* Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.

Chapter 9:

9

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- *Excluded* The port is not part of a Multicast group.
- Dynamic Attaches the port to the Multicast group as dynamic member.

#### 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:

SFE 2000P		LINKSYS A Divider of Data Patiena, Inc.
	Edit Multicast Forward All	
VLAN ID	10	
Interface	1/e13	
Interface Status	Excluded -	
•	Apply	

#### Edit Multicast Forward All Page

The Edit Multicast Forward All Page contains the following fields:

- VLAN ID Displays the VLAN ID.
- Interface Displays the port or LAG attached to the Multicast Group.
- Interface Status Displays the interface status.
- 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 on Interfaces
- Defining Interface Settings
- Defining Rapid Spanning Tree
- Defining Multiple Spanning Tree

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **Defining STP on Interfaces**

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

LINKSYS A Denixel of Close Systema, Inc.			
SFE 2000P	Clobal Settings Spanning Tree Start STP Operation Mod BPDU Handling Path Cost Default V Bridge Settings Priority © Hello Time © Max Age © Forward Delay	Classic STP      Flooding	Help Support Guide Logout
	Designated Root Bridge ID Root Bridge ID Root Port Root Path Cost Topology Changes Last Topology Chan		r

The STP Properties Page contains the following fields:

The Global Settings area contains the following fields:

- Spanning Tree State Indicates if STP is enabled on the device. The possible field values are:
  - Enable Enables STP on the device. This is the default value.
  - Disable Disables STP on the device.
- **STP Operation Mode** Indicates the STP mode by which STP is enabled on the device. The possible field values are:
  - Classic STP --- Enables Classic STP on the device. This is the default value.
  - Rapid STP Enables Rapid STP on the device.
  - Multiple STP Enables Multiple STP on the device.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



- **BPDU Handling** Determines how BPDU packets are managed when STP is disabled on the port/ device. BPDUs are used to transmit spanning tree information. The possible field values are:
  - Filtering Filters BPDU packets when spanning tree is disabled on an interface. This is the default value.
  - Flooding Floods BPDU packets when spanning tree is disabled on an interface.
- **Path Cost Default Values** Specifies the method used to assign default path costs to STP ports. The possible field values are:
  - Short Specifies 1 through 65,535 range for port path costs. This is the default value.
  - Long Specifies 1 through 200,000,000 range for port path costs. The default path costs assigned to an interface varies according to the selected method.

The Bridge Settings area contains the following fields:

- **Priority** Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc. The range is 0 to 65535.
- **Hello Time** Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.
- Max Age Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds. The range is 6 to 40 seconds.
- Forward Delay Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.

The Designated Root area contains the following fields:

- Bridge ID Identifies the Bridge ID and MAC address.
- Root Bridge ID— Identifies the Root Bridge priority and MAC address.
- **Root Port** Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root. The default is zero.
- **Root Path Cost** The cost of the path from this bridge to the root.
- **Topology Changes Counts** Indicates the total amount of STP state changes that have occurred.
- Last Topology Change Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format, for example, 2 days 5 hours 10 minutes and 4 seconds:
- 2. Define the relevant fields.

Chapter 10:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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:

SFE 2000P	Inte	rface	Setti	ngs									Help
System Admin Statistics	⊙ Po	nts Of U	nit 🔳 🤇	ି LAGs								-	Support
Bridging Address Tables	Port	STP	Port Fast	Root Guard	Port State	Port Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions	Guide
Port Management	1/e1	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	Logout
- en VLAN Management	1/e2	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
	1/e3	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
Interface Settings RSTP	1/e4	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
MSTP Multicast	1/e5	Enable	Disabled	Disable	N/A	Disable	2000000	128	N/A	N/A	N/A	N/A	
Routing	1/e6		Disabled						N/A	N/A	N/A	N/A	
E Security Suite													
addancy of Dervice	1/e7		Disabled						N/A	N/A	N/A	N/A	
	1/e8	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
1	1/e9	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	-
	1/e10	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
	1/e11	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
	1/e12	Enable	Disabled	Disable	Disabled	Disable	2000000	128	N/A	N/A	N/A	N/A	
			Disabled						N/A	N/A	N/A	N/A	
			Disabled						N/A	N/A	N/A		

Interface Settings Page

The STP Interface Settings Page contains the following fields:

- Ports Indicates the port number on which Spanning Tree is configured.
- LAGs Indicates the LAG number on which Spanning Tree is configured.
- Of Unit Displays the stacking member for which the Spanning Tree parameters are displayed.
- **Port** Indicates the port or LAG on which STP is enabled.
- STP Indicates if STP is enable on the port. The possible field values are:
  - Enable -- Indicates that STP is enabled on the port.
  - Disables -- Indicates that STP is disabled on the port.
- **Port Fast** Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link



optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.

- **Root Guard** Prevents devices outside the network core from being assigned the spanning tree root.
- **Port State** Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - Disabled Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - Blocking Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
  - *Listening* Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - Forwarding Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role** Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* Provides the lowest cost path to forward packets to the root switch.
  - Designated The port or LAG through which the designated switch is attached to the LAN.
  - *Alternate* Provides an alternate path to the root switch from the root interface.
  - Backup Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
  - *Disabled* The port is not participating in the Spanning Tree.
- **Path Cost** Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Priority** Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is provided in increments of 16.
- **Designated Bridge ID** Indicates the bridge priority and the MAC Address of the designated bridge.
- Designated Port ID Indicates the selected port's priority and interface.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Designated Cost** Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- Forward Transitions Indicates the number of times the port has changed from the Blocking state to Forwarding state.
- LAG Displays the LAG of which this port is a member, if relevant. If a port is a member of a LAG, the LAG settings override the port settings.
- 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 Interface Settings Page opens:

#### Interface Settings Page

SFE 2000P		LINKSYS A Unities of Classe Systems, Inc.
	Interface Settings	
	The second s	
Port	1/e1 💌	
STP	Enable 💌	
Port Fast	Disabled 💌	
Enable Root Guard		
Port State	Disabled	
Speed	100M	
Path Cost	2000000	
Default Path Cost		
Priority	128	
Designated Bridge ID	N/A	
Designated Port ID	N/A	
Designated Cost	N/A	
Forward Transitions	N/A	
LAG		
	Apply	

The Interface Settings Page contains the following fields:

- Ports Indicates the port number on which Spanning Tree is configured.
- STP Indicates if STP is enable on the port. The possible field values are:
  - Enable Indicates that STP is enabled on the port.
  - Disable Indicates that STP is disabled on the port.
- **Port Fast** Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link



optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.

- Enable Root Guard Enable the prevention of a devices outside the network core from being assigned the spanning tree root.
- **Port State** Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - Disabled Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - Blocking Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
  - *Listening* Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - Forwarding Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- Speed Indicates the speed at which the port is operating.
- **Path Cost** Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- Default Path Cost Indicates the default path cost.
- **Priority** Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is provided in increments of 16.
- **Designated Bridge ID** Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** Indicates the selected port's priority and interface.
- **Designated Cost** Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- Forward Transitions Indicates the number of times the port has changed from the Blocking state to Forwarding state.
- LAG Displays the LAG of which this port is a member, if relevant. If a port is a member of a LAG, the LAG settings override the port settings.
- 3. Define the relevant fields.
- 4. Click Apply. The interface settings are modified, and the device is updated.

Chapter 10:



# **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:

).										
SFE 2000P	RSTP									Help
System		_							-	Support
Admin Statistics	Ports	Of Unit  1	<u> </u>	LAGs						
Bridging Address Tables	Interface	Role	Mode	Fast Link	Port Status	Point-to-Point Operational Status	Activate Protocol Migration			Guide
- Port Management - Mulan Management	1/e1	Disable	STP	Disable	Disabled	Enable	Activate	Edit		Logout
📥 Spanning Tree	1/e2	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
Properties	1/e3	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
RSTP	1/e4	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
MSTP Multicast	1/e5	N/A	STP	N/A	N/A	N/A	Activate	Edit		
Routing Security Suite	1/e6	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
Quality of Service	1/e7	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
	1/e8	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
	1/e9	Disable	STP	Disable	Disabled	Enable	Activate	Edit		
	1/e10	Disable		Disable	Disabled		Activate	Edit		
	1/e11	Disable		Disable	Disabled		Activate	Edit		
				Disable			Activate	Edit		
	1/e12	Disable			Disabled			Edit		
	1/e13	Disable	SIP	Disable	Disabled	Enable	Activate	Edif		

**RSTP** Page

The RSTP Page contains the following fields:

- Ports Indicates the port number on which RSTP is configured.
- LAGs Indicates the LAG number on which RSTP is configured.
- Of Unit Displays the stacking member for which the RSTP parameters are displayed.
- Interface Displays the port or LAG on which Rapid STP is enabled.
- **Role** Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - Root Provides the lowest cost path to forward packets to root switch.
  - Designated Indicates that the port or LAG via which the designated switch is attached to the LAN.

Chapter 10:



- Alternate Provides an alternate path to the root switch from the root interface.
- Backup Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
- *Disabled* Indicates the port is not participating in the Spanning Tree.
- **Mode** Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the *Global STP* page. The possible field values are:
  - Classic STP Indicates that Classic STP is enabled on the device.
  - *Rapid STP* Indicates that Rapid STP is enabled on the device.
  - *Multiple STP* Indicates that Multiple STP is enabled on the device.
- Fast Link Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- Port Status Indicates if RSTP is enabled on the interface. The possible field values are:
  - Enable Indicates that RSTP is enabled on the port.
  - Disable Indicates that RSTP is disabled on the port.
- Point-to-Point Operational Status Indicates the Point-to-Point operating state.
- Activate Protocol Migration Runs a Protocol Migration Test. The test sends Link Control Protocol (LCP) packets to test if a data link is enabled.
- 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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SFE 2000P		
Edit	Rapid Spanning Tree	
Interface	💿 Port 1/e1 🔽 🔿 LAG 1 🔽	
Role	Disable	
Mode	STP	
Fast Link Operational Status	Disable	
Port State	Disabled	
Point to Point Admin Status	Auto	
Point to Point Operational Status	Enable	
Activate Protocol Migration Test		
	Apply	

#### Edit Rapid Spanning Tree Page

The Edit Rapid Spanning Tree Page contains the following fields:

- Interface Displays the port or LAG on which Rapid STP is enabled.
- **Role** Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - Root Provides the lowest cost path to forward packets to root switch.
  - Designated Indicates that the port or LAG via which the designated switch is attached to the LAN.
  - *Alternate* Provides an alternate path to the root switch from the root interface.
  - Backup Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - Disabled Indicates the port is not participating in the Spanning Tree.
- **Mode** Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the *Global STP* page. The possible field values are:
  - Classic STP Indicates that Classic STP is enabled on the device.
  - *Rapid STP* Indicates that Rapid STP is enabled on the device.
  - *Multiple STP* Indicates that Multiple STP is enabled on the device.
- **Fast Link Operational Status** Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Port State** Indicates if RSTP is enabled on the interface. The possible field values are:
  - Enable Indicates that RSTP is enabled on the port.



- Disable Indicates that RSTP is disabled on the port.
- **Point-to-Point Admin Status** Indicates if a point-to-point links is established, or permits the device to establish a point-to-point link. The possible field values are:
  - Enable Enables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.
  - Disable Disables point-to-point link.
- Point-to-Point Operational Status Indicates the Point-to-Point operating state.
- Activate Protocol Migration Test— Runs a Protocol Migration Test. The test sends Link Control Protocol (LCP) packets to test if a data link is enabled.
- 3. Define the relevant fields.
- 4. Click Apply. The Rapid Spanning Tree Settings are modified, and the device is updated.

10

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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
- Instance to VLAN
- Instance Settings
- Interface Settings

10

# **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:

SFE 2000P	Properties	Help
System Statistics Bridging Address Tables Fort Management Spanning Tree Forperties For Management Spanning Tree Forperties For MSTP Forperties MSTP Forperties Fortics MSTP Forperties Fortics Security Suite Guality of Service	Region Name       50:25:67:02:90:00         Revision       0         Max Hops       20         IST Master       32768-00:25:67:02:90:00	Support Guide Logout

#### **MSTP** Properties Page

The MSTP Properties Page contains the following fields:

- Region Name Provides a user-defined STP region name.
- **Revision** Defines unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration. The possible field range 0-65535.
- Max Hops Indicates the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.
- IST Master Identifies the Spanning Tree Master instance. The IST Master is the specified instance root.
- 2. Define the relevant fields.
- 3. Click Apply. The MSTP properties are defined, and the device is updated.

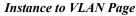
Chapter 10:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

### **Instance to VLAN**

The VLAN screen enables mapping VLANs to MSTP Instances.

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



SFE 2000P	Instand	e To VL	AN						Help
E System									- Support
Admin Statistics	VLAN	Instance ID (0-15)	Guide						
en Bridging	VLAN 1	0	VLAN 17	0	VLAN 33	0	VLAN 49	0	Guide
Port Management	VLAN 2	0	VLAN 18	0	VLAN 34	0	VLAN 50	0	Logout
Spanning Tree	VLAN 3	0	VLAN 19	0	VLAN 35	0	VLAN 51	0	
	VLAN 4	0	VLAN 20	0	VLAN 36	0	VLAN 52	0	
	VLAN 5	0	VLAN 21	0	VLAN 37	0	VLAN 53	0	
- en MSTP	VLAN 6	0	VLAN 22	0	VLAN 38	0	VLAN 54	0	
Instance To VLAN	VLAN 7	0	VLAN 23	0	VLAN 39	0	VLAN 55	0	
Instance Settings	VLAN 8	0	VLAN 24	0	VLAN 40	0	VLAN 56	0	
Multicast	VLAN 9	0	VLAN 25	0	VLAN 41	0	VLAN 57	0	
E Security Suite	VLAN 10	0	VLAN 26	0	VLAN 42	0	VLAN 58	0	
Cuality of Service	VLAN 11	0	VLAN 27	0	VLAN 43	0	VLAN 59	0	
	VLAN 12	0	VLAN 28	0	VLAN 44	0	VLAN 60	0	
	VLAN 13	0	VLAN 29	0	VLAN 45	0	VLAN 61	0	
	VLAN 14	0	VLAN 30	0	VLAN 46	0	VLAN 62	0	
	VLAN 15	0	VLAN 31	0	VLAN 47	0	VLAN 63	0	
٦	VLAN 16	0	VLAN 32	0	VLAN 48	0	VLAN 64	0	-

The Instance to VLAN Page contains the following fields:

- VLAN Indicates the VLAN for which the MSTP instance ID is defined.
- Instance ID Indicates the MSTP instance ID assigned to the VLAN.

#### **Instance Settings**

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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### MSTP Instance Settings Page

LINKSYS A dhaara of Gace System, Inc.			
SFE 2000P	Instance Settin	ngs	Help
i	Instance ID		Support
Statistics     Bridging     Port Management     VLAN Management     Spanning Tree     Properties	Included VLAN		Guide Logout
	Bridge Priority	32768	
	Designated Root Bridge ID	D 32768-00.25.67.02.90.00	
Properties	Root Port	0	
Instance Settings	Root Path Cost	0	
Interface Settings	Bridge ID	32768-00.25:67:02.90:00	
n Enviring	Remaining Hops	20	
B ■ Security Suite B ■ Quality of Service	Apply		
			Cince Statist

The MSTP Instance Settings Page contains the following fields:

- Instance ID Defines the VLAN group to which the interface is assigned.
- Included VLAN Maps the selected VLAN to the selected instance. Each VLAN belongs to one instance.
- Bridge Priority Specifies the selected spanning tree instance device priority. The field range is 0-61440
- **Designated Root Bridge ID** Indicates the ID of the bridge with the lowest path cost to the instance ID.
- **Root Port** Indicates the selected instance's root port.
- Root Path Cost Indicates the selected instance's path cost.
- **Bridge ID** Indicates the bridge ID of the selected instance.
- **Remaining Hops** Indicates the number of hops remaining to the next destination.

#### **Interface Settings**

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

Chapter 10:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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

SFE 2000P	Interface Set	lings	Help
System Admin	Instance ID		Support
Statistics Bridging	Interface	© Port 1/e1 ▼ C LAG 1 ▼	Guide
Address Tables	Port State	N/A	
-en Port Management	Туре	N/A	Logout
Spanning Tree	Role	N/A	
Interface Settings	Mode	N/A	
🖹 RSTP 	Interface Priority	128	
Properties	Path Cost	2000000 🔲 Use Default	
- 🔄 Instance Settings	Designated Bridge ID	N/A	
Multicast	Designated Port ID	N/A	
Routing	Designated Cost	N/A	
Security Suite Quality of Service	Forward Transitions	N/A	
	Remain Hops	N/A	
	Apply	rface Table	
	(app)		

MSTP Interface Settings Page

The MSTP Instance Settings Page contains the following fields:

- Instance ID Lists the MSTP instances configured on the device. Possible field range is 0-15.
- Interface Displays the interface for which the MSTP settings are displayed. The possible field values are:
  - Port Specifies the port for which the MSTP settings are displayed.
  - LAG Specifies the LAG for which the MSTP settings are displayed.
- **Port State** Indicates whether the port is enabled for the specific instance. The possible field values are:
  - Enable Enables the port for the specific instance.
  - Disable Disables the port for the specific instance.
  - Forwarding Enables forwarding all multicast packets on a port.
- **Type** Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:



- Boundary Port Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
- Master Port Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
- Internal Indicates the port is an internal port.
- **Role** Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* Provides the lowest cost path to forward packets to root device.
  - *Designated* Indicates the port or LAG via which the designated device is attached to the LAN.
  - Alternate Provides an alternate path to the root device from the root interface.
  - Backup Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - Disabled Indicates the port is not participating in the Spanning Tree.
- **Mode** Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the *Global STP* page. The possible field values are:
  - *Classic STP* Indicates that Classic STP is enabled on the device.
  - *Rapid STP* Indicates that Rapid STP is enabled on the device.
  - *Multiple STP* Indicates that Multiple STP is enabled on the device.
- Interface Priority Defines the interface priority for specified instance. The default value is 128.
- **Path Cost** Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Designated Bridge ID** Indicates that the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** Indicates that the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- Forward Transitions Indicates the number of times the port has changed from Forwarding state to Blocking state.
- **Remaining Hops** Indicates the hops remaining to the next destination.

Chapter 10:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Interface State Indicates whether the port is enabled or disabled in the specific instance.
- 2. Click the Interface Table button. The Interface Table Page opens:

#### Interface Table Page

	SFE 20	000P									INS .
						Interfa	ice 1	Table			
Ins	tance 1	œ l	Ports C	)f Unit	1 <b>.</b> o u	AGs					
#	Interface	Role	Mode	<b>.</b>	Port	Path	Port	Designated	Designated	Designated	Remain
#	пцептасе	Role	mode	Туре	Priority	Cost	State	Cost	Bridge ID	Port ID	Hops
1	1/e1	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
2	1/e2	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
3	1/e3	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
4	1 <i>/</i> e4	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
5	1/e5	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A

The Interface Table Page contains the following fields:

- Instance ID Defines the VLAN group to which the interface is assigned.
- Interface Displays the interface for which the MSTP settings are displayed. The possible field values are:
  - Port Specifies the port for which the MSTP settings are displayed.
  - LAG Specifies the LAG for which the MSTP settings are displayed.
- **Role** Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* Provides the lowest cost path to forward packets to root device.
  - Designated Indicates the port or LAG via which the designated device is attached to the LAN.
  - *Alternate* Provides an alternate path to the root device from the root interface.
  - Backup Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - Disabled Indicates the port is not participating in the Spanning Tree.
- Mode Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the Global STP page. The possible field values are:
  - Classic STP Indicates that Classic STP is enabled on the device.

- *Rapid STP* Indicates that Rapid STP is enabled on the device.
- *Multiple STP* Indicates that Multiple STP is enabled on the device.
- **Type** Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
  - Boundary Port Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
  - Master Port Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
  - Internal -- Indicates the port is an internal port.
- Port Priority Defines the interface priority for specified instance. The default value is 128.
- **Path Cost** Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Port State** Indicates whether the port is enabled for the specific instance. The possible field values are:
  - Enable Enables the port for the specific instance.
  - Disable Disables the port for the specific instance.
  - Forwarding Enables forwarding all multicast packets on a port.
- **Designated Cost** Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Designated Bridge ID** Indicates that the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** Indicates that the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Remaining Hops** Indicates the hops remaining to the next destination.
  - *Static* Attaches the port to the Multicast group as static member in the Static Row. The port/LAG has joined the Multicast group statically in the Current Row.
  - *Forbidden* Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
  - Non The port is not part of a Multicast group.

Chapter SFE2000/SI

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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 the following traps:

- Copy trap
- Stacking traps

The SNMP section contains the following sections:

- Configuring SNMP Security
- Defining Trap Management

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **Configuring SNMP Security**

The Security section contains the following pages:

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

### **Defining 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**

SEE 200F         System         Syst	LINKSYS A Division of Class Systems, Doc		
	System System Management SMMP Security Security Views Groups Communities Trap Management Statistics Statistics Statistics Statistics Security Views Communities Statistics Statistics Security Views Security Views Securit	Local Engine ID (19.64 Hex Characters) EngineD not Configured Use Default	Support Guide

The Engine ID Page contains the following fields.

• Local Engine ID (10-64 Hex characters) — Indicates the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings consists of two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. For stand-alone devices, select a default Engine ID that is comprised of Enterprise number and the default MAC address. For a stackable system configure the Engine ID, and verify



that the Engine ID is unique for the administrative domain. This prevents two devices in a network from having the same Engine ID.

- Use Default Uses the device generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
  - *First 4 octets* first bit = 1, the rest is IANA Enterprise number.
  - Fifth octet Set to 3 to indicate the MAC address that follows.
  - Last 6 octets MAC address of the device.

#### **Defining SNMP Views**

SNMP Views provide access or block access to device features or feature aspects. For example, a view can be defined that states that SNMP Group A has Read Only (R/O) access to Multicast groups, while SNMP Group B has Read-Write (R/W) access to Multicast groups. Feature access is granted via the MIB name, or MIB Object ID. To define SNMP views:

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

A Dense of Case System, Str.	Views	
ESystem ■ System Management ■ SNMP	View Name Default	[
	□ Object ID Subtree	View Type
	□ 1	Included
Groups	1.3.6.1.6.3.13	Excluded
Communities	1.3.6.1.6.3.16	Excluded
Trap Management	1.3.6.1.6.3.18	Excluded
🗄 🌰 Statistics	□ 1.3.6.1.6.3.12.1.2	Excluded
Bridging     Brouting	□ 1.3.6.1.6.3.12.1.3	Excluded
i in Security Suite	1.3.6.1.6.3.15.1.2	Excluded
in envice	□ 1.3.6.1.4.1.3955.89.2	.7.2 Excluded
	Delete	Add
	Delete	Add

#### **SNMP** Views Page

The SNMP Views Page contains the following fields:

- View Name Displays the user-defined views. The options are as follows:
  - Default Displays the default SNMP view for read and read/write views.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- DefaultSuper Displays the default SNMP view for administrator views.
- **Object ID Subtree** Indicates the device feature OID included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
  - Select from List Select the Subtree from the list provided.
  - Insert Enables a Subtree not included in the Select from List field to be entered.
- View Type Indicates if the defined OID branch will be included or excluded in the selected SNMP view.
- 2. Click the Add button. The Add SNMP View Page opens:

SFE 2000P							
		Add S	NMP	View			
View Name	<b></b>						
Subtree ID Tree		system interfaces ip icmp tcp		Up Down	C Insert	1.3.6.1.2.1.1	
View Type	Included 💌	, .	_				
						Apply	

#### Add SNMP View Page

The *Add SNMP View Page* contains parameters for defining and configuring new SNMP view. The *Add SNMP View Page* contains the following fields:

- View Name Displays the user-defined views. The options are as follows:
  - Default Displays the default SNMP view for read and read/write views.
  - DefaultSuper Displays the default SNMP view for administrator views.
- Subtree ID Tree Indicates the device feature OID included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
  - Select from List Select the Subtree from the list provided.
  - Up/Down Allows you to determine the priority by moving the selected subtree up or down in the list.
  - Insert Enables a Subtree not included in the Select from List field to be entered.
- View Type Indicates if the defined OID branch will be included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
  - Included Includes the defined OID branch.
  - Excluded Excludes the defined OID branch.

- 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:

System System System System System Management System System Carlos System System Carlos System Carlos System System Carlos System Carlos Corups Compute Comput	Users User Name Group Name Engine ID Authentication Delete Add	Help Support Guide Logout
Duality of Service		

**SNMP** Users Page

The SNMP Users Page contains the following fields.

- User Name Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- Group Name Displays the user-defined group to which access control rules are applied.
- Engine ID Indicates the local device engine ID.
- Authentication Indicates the Authentication method used.
- 2. Click the Add button. The Add SNMP Group Membership Page opens:

Chapter 11:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add SNMP Group Membership Page

SFE 2000		LINKSYS
Ad	d SNMP Group Membership	
User Name		
Engine ID	CLocal CRemote	
Group Name		
Authentication Method	None	
Password		
Authentication Key		
Privacy Key		
	Ар	ply

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

- User Name Provides a user-defined local user list.
- Engine ID Indicates either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database.
  - Local Indicates that the user is connected to a local SNMP entity.
  - *Remote* Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.
- **Group Name** Contains a list of user-defined SNMP groups. SNMP groups are defined in the SNMP Group Profile page.
- Authentication Method— Indicates the Authentication method used. The possible field values are:
  - MD5 Key Users are authenticated using the HMAC-MD5 algorithm.
  - SHA Key Users are authenticated using the HMAC-SHA-96 authentication level.
  - MD5 Password The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - SHA Password Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
  - No Authentication No user authentication is used.
- **Password** Define the local user password. Local user passwords can contain up to 159 characters.
- Authentication Key Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined.



Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.

• **Privacy Key** — Defines the Privacy Key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

## **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 2000 System System Management SNMP Security Security Supers Composition Communities Trap Management Admin Bridging Routing Routing	Groups Group Name Security Model S test SNMPv1 N	Security Level Operation Read Write Notify No Authentication Default Edit Delete Add	Help Support Guide Logout
Quality of Service			

#### SNMP Groups Profile Page

The SNMP Groups Profile Page contains the following fields:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- *SNMPv3* SNMPv3 is defined for the group.
- Security Level Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
  - No Authentication Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
  - Privacy Encrypts SNMP message.
- **Operation** Defines the group access rights. The possible field values are:
  - *Read* The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - Write The management access is read-write and changes can be made to the assigned SNMP view.
  - Notify Sends traps for the assigned SNMP view.
- 2. Click the Add button. The Add SNMP Group Profile Page opens:

SNMPv1 -

No Authentication 🔽

Read Default

SFE

Group Name

Security Model

Security Level

Oneration

	Lin
Add SNMP Group Profile	
	Add SNMP Group Profile

KSYS

-

Apply

🔽 🗖 Notify 🛛 Default

#### Add SNMP Group Profile Page

The Add SNM	P Group Profile	Page allows netw	ork managers to	define new	SNMP Gro	up profiles.	The
Add SNMP Gr	oup Profile Page	e contains the foll	owing fields:				

🗾 🗖 Write Default

- Group Name Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- Security Model Defines the SNMP version attached to the group.
- Security Level Defines the security level attached to the group. Security levels apply to SNMPv3 only.
- **Operation** Defines the group access rights. The options for each operation Read, Write and Notify are as follows:

- Default Defines the default group access rights.
- DefaultSuper Defines the default group access rights for administrator.

#### Modifying SNMP Group Profile Settings

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

#### SNMP Group Profile Settings Page

SFE 2000		LINKSYS	
	SNMP Group Profile Settings		
Group Name	test 💌		
Security Model	SNMPv1		
Security Level	No Authentication		
Operation	🔽 Read Default 🔄 🗖 Write Default 🔄 🗖 Notify D	)efault 🗾 💌	
		Apply	

The SNMP Group Profile Settings Page contains the following fields:

- Group Name Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- Security Model Defines the SNMP version attached to the group.
- Security Level Defines the security level attached to the group. Security levels apply to SNMPv3 only.
- **Operation** Defines the group access rights. The options for each operation Read, Write and Notify are as follows:
  - Default Defines the default group access rights.
  - DefaultSuper Defines the default group access rights for administrator.

#### **Defining SNMP Communities**

The Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c. The SNMP Communities Page contains two areas, the Basic Table and the Advanced Table. To define SNMP Communities:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **SNMP** Communities Page

LINKSYS A Division of Clicce Systems, Inc.		
SFE 2000 System System Management System Management Sourity Security Groups Statistics Bridging Security Suite Ouality of Service	Basis Table   124000   12   Read Only   Default   Edit   Delete	Help Support Guide Logout
		core

The SNMP Communities Page is divided into the following tables:

- SNMP Communities Basic Table
- SNMP Communities Advanced Table

The SNMP Communities Basic Table area contains the following fields:

- Management Station Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** Displays the password used to authenticate the management station to the device.
- Access Mode Displays the access rights of the community.
- View Name Displays the user-defined SNMP view.

The SNMP Communities Advanced Table area contains the following fields:

- **Management Station** Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** Displays the password used to authenticate the management station to the device.
- Group Name Displays advanced SNMP communities group name.

186



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

#### Add SNMP Community Page

SFE 2000				LINKSYS A Database of Dana Typesena, Inc.
	A	dd SNMP (	Communi	ty
SNMP Manager Community Str	( 	5 All (0.0.0.0)	(X.X.X)	
Basic	Access Mode	Read Only	🔲 View Name	Default 🔽
C Advanced	Group Name	test 💌		
				Apply

The *Add SNMP Community Page* allows network managers to define and configure new SNMP communities. The *Add SNMP Community Page* contains the following fields:

- **SNMP Management Station** Defines the management station IP address for which the advanced SNMP community is defined. There are two definition options: Define the management station IP address.
- Select All, which includes all management station IP addresses.
- **Community String** Defines the password used to authenticate the management station to the device.
- **Basic** Enables SNMP Basic mode for a selected community and contains the following fields:
- Access Mode Defines the access rights of the community. The possible field values are:
  - *Read Only* Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* Management access is read-write and changes can be made to the device configuration, but not to the community.
  - SNMP Admin User has access to all device configuration options, as well as permissions to modify the community.
- View Name Contains a list of user-defined SNMP views.
- Advanced Enables SNMP Advanced mode for a selected community and contains the following fields:
- Group Name Defines advanced SNMP communities group names.

#### 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:

Chapter 11:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Edit SNMP Community Page

SFE 2000				LINKSYS A Unities of Class Typitama, Inc.
	SNN	IP Commu	nity Setti	ngs
SNMP Manager Community Str		•		
<ul> <li>Basic</li> <li>Advanced</li> </ul>	Access Mode Group Name	Read Only 💌	🔽 View Name	Default
				Apply

The Edit SNMP Community Page contains the following fields:

- **SNMP Management** Defines the management station IP address for which the advanced SNMP community is defined.
- **Community String** Defines the password used to authenticate the management station to the device.
- **Basic** Enables SNMP Basic mode for a selected community and contains the following fields:
- Access Mode Defines the access rights of the community. The possible field values are:
  - *Read Only* Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* Management access is read-write and changes can be made to the device configuration, but not to the community.
  - SNMP Admin User has access to all device configuration options, as well as permissions to modify the community.
- View Name Contains a list of user-defined SNMP views.
- Advanced Enables SNMP Advanced mode for a selected community and contains the following fields:
  - Group Name Defines advanced SNMP communities group names.
- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Community settings are defined, and the device is updated.

11

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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**

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

Trap Settings Page

LINKSYS A Desize of Cloco Systems, Inc.			
SFE 2000	Trap Settings		Help
System System Management SNMP Trap Seturity Trap Seturity Trap Seturity Station Management Station Management Filter Settings Roding Roding Security Suite Quality of Service	Enable SNMP Notifications Enable Authentication Notifications Apply	2	Support Guide Logout
			C003 97 11*

The Trap Settings Page contains the following fields:

- Enable SNMP Notification Specifies whether the device can send SNMP notifications. The possible field values are:
  - Enable Enables SNMP notifications.
  - Disable Disables SNMP notifications.
- Enable Authentication Notification Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:

Chapter 11:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Enable Enables the device to send authentication failure notifications.
- Disable Disables the device from sending authentication failure notifications.

## **Configuring Station Management**

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

Station Management Page

SFE 2000 System System Management SNMP Trap Management Trap Settings Station Management Statistics Bridging Routing Scurity Suite Cousity of Service	Station Management         StMPY1 2. Nutrification Recipient       Motification Community Nutrification UDP Filter Inneout Retries         1       210.0.00       Traps       1       SNMPV1       162       Edit         StMPV3 Mutrification Recipient       Inneout Retries       Inneout Retries       Inneout Retries         #       #       Popping       Name Level       Popt Name       Timeout Retries	Help Support Guide Logout
ľ		

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

The SNMPv1,2 Notification Recipient table area contains the following fields:

- **Recipients IP** Indicates the IP address to whom the traps are sent.
- Notification Type Defines the notification sent. The possible field values are:
  - Trap Indicates traps are sent.
  - Inform Indicates informs are sent.
- Community String Identifies the community string of the trap manager.
- Notification Version Determines the trap type. The possible field values are:
  - SNMP V1 Indicates SNMP Version 1 traps are sent.

- SNMP V2 Indicates SNMP Version 2 traps are sent.
- **UDP Port** Displays the UDP port used to send notifications. The default is 162.
- Filter Name Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.

The SNMPv3 Notification Recipient table area contains the following fields:

- Recipients IP Indicates the IP address to whom the traps are sent.
- Notification Type Defines the notification sent. The possible field values are:
  - Trap Indicates traps are sent.
  - Inform Indicates informs are sent.
- User Name Displays the SNMP Communities.
  - Security Level Defines the means by which the packet is authenticated. The possible field values are:
  - No Authentication Indicates the packet is neither authenticated nor encrypted.
  - Authentication Indicates the packet is authenticated.
  - *Privacy* Indicates the packet is both authenticated and encrypted.
- UDP Port Displays the UDP port used to send notifications. The default is 162.
- Filter Name Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- Timeout Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- 2. Click the Add button. The Add SNMP Notification Recipient Page opens

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add SNMP Notification Recipient Page

Add SNMP Notification Recipient	
Recipient IP	
Notification Type Traps 💌	
© SNMPv1,2 Community String Notification Version SNMPv1 -	
CSNMPv3 User Name Security Level NoAuthentication	
UDP Port 162	
Timeout 15 (sec) Retries 3	

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

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

The Add SNMP Notification Recipient Page contains the following fields:

- Recipient IP Indicates the IP address to whom the traps are sent.
- Notification Type Defines the notification sent. The possible field values are:
  - Trap Indicates traps are sent.
  - Inform -- Indicates informs are sent.

The SNMPv1,2 Notification Recipient area contains the following fields:

- SNMPv1,2 Enables SNMPv1,2 as the Notification Recipient. Either SNMPv1,2 or SNMPv3 can be enabled at any one time, but not both at the same time. If SNMPv1,2 is enabled, the Community String and Notification Version fields are enabled for configuration:
- **Community String** Identifies the community string of the trap manager.



- Notification Version Determines the trap type. The possible field values are:
  - SNMP V1 Indicates SNMP Version 1 traps are sent.
  - SNMP V2 Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

- SNMPv3 Enables SNMPv3 as the Notification Recipient. Either SNMPv1,2 or SNMPv3 can be enabled at any one time, but not both at the same time. If SNMPv3 is enabled, the User Name and Security Level fields are enabled for configuration:
- User Name Defines the user to whom SNMP notifications are sent.
- Security Level Defines the means by which the packet is authenticated. The possible field values are:
  - No Authentication Indicates the packet is neither authenticated nor encrypted.
  - Authentication Indicates the packet is authenticated.
  - *Privacy* Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** Displays the UDP port used to send notifications. The default is 162.
- Filter Name Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Recipient settings are defined, and the device is updated.

#### Modify SNMP Notifications

The *SNMP Notification Receiver Page* allows system administrators to define notification settings. The *SNMP Notification Receiver 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 SNMP Notification Receiver Page opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### SNMP Notification Receiver Page

SFE 2000		LINKSYS A Dividior of Docor Tyrelama, Inc.
	SNMP Notification Reciever	
Recipient IP	210.0.0.0 -	
Notification Typ	e Traps 💌	
€SNMPv1,2		
Community Stri	ing 1	
Notification Ver	sion SNMPv1 -	
CSNMPv3		
User Name	Y	
Security Level	NoAuthentication	
UDP Port	162	
Filter Name	<b>x</b>	
Timeout	15	
Retries	З	
	Apply	

The SNMP Notification Receiver Page contains the following fields:

- Recipients IP Indicates the IP address to whom the traps are sent.
- Notification Type Defines the notification sent. The possible field values are:
  - Trap Indicates traps are sent.
  - Inform -- Indicates informs are sent.

The SNMPv1,2 Notification Recipient area contains the following fields:

- SNMPv1,2 Enables SNMPv1,2 as the Notification Recipient. Either SNMPv1,2 or SNMPv3 can be enabled at any one time, but not both at the same time. If SNMPv1,2 is enabled, the Community String and Notification Version fields are enabled for configuration:
- Community String (SNMP v1, 2) Identifies the community string of the trap manager.
- Notification Version (SNMP v1, 2) Determines the trap type. The possible field values are:
  - SNMP V1 Indicates SNMP Version 1 traps are sent.
  - SNMP V2 Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

• SNMPv3 — Enables SNMPv3 as the Notification Recipient. Either SNMPv1,2 or SNMPv3 can be enabled at any one time, but not both at the same time. If SNMPv3 is enabled, the User Name and Security Level fields are enabled for configuration:

- User Name Defines the user to whom SNMP notifications are sent.
- Security Level (SNMP v3) Defines the means by which the packet is authenticated. The possible field values are:
  - No Authentication Indicates the packet is neither authenticated nor encrypted.
  - Authentication Indicates the packet is authenticated.
  - *Privacy* Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- UDP Port Displays the UDP port used to send notifications. The default is 162.
- Filter Name Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Receivers are defined, and the device is configured.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **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.

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

Filter Settings Page

LINKSYS A theore of Case Systems, Inc.		
SFE 2000 System System Management Situry Trap Settings Statistics Biging Statistics Biging Statistics Discurt Suite Quality of Service	Filter Settings Filter Name  Delete Add Apply	Help Support Guide Logout
		Constanting of the second seco

The Filter Settings Page contains the following fields:

- Filter Name Contains a list of user-defined notification filters.
- **Object ID Subtree** Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the Select from List or the Object ID List. there are two configuration options:
  - Select from List Select the OID from the list provided.
  - Up/Down Allows you to determine the priority by moving the selected subtree up or down in the list.
  - Object ID Enter an OID not offered in the Select from List option.
- Filter Type Indicates whether informs or traps are sent regarding the OID to the trap recipients.
  - Excluded Restricts sending OID traps or informs.

11

- Included Sends OID traps or informs.
- 2. Click the Add button. The Add SNMP Notification Filter Page opens:

Add SNMP Notification Filter Page

SFE 2000							LINKSYS A Distator of Data Systems, Inc.
	Ad	d SNMP	Not	ificat	tion Filt	er	
Filter Name							
New Object Identifier Tree	Select from List	system interfaces ip icmp tcp		Up Down	C Object ID	[	
Filter Type	Included 💌						
						Ар	ply

The Add SNMP Notification Filter Page contains the following fields:

- Filter Name Contains a list of user-defined notification filters.
- New Object Identifier Subtree Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the Select from List or the Object ID List. there are two configuration options:
  - Select from List Select the OID from the list provided.
  - Object ID Enter an OID not offered in the Select from List option.
- Filter Type Indicates whether informs or traps are sent regarding the OID to the trap recipients.
  - Excluded Restricts sending OID traps or informs.
  - Included Sends OID traps or informs.
- 3. Define the relevant fields.
- 4. Click Apply. The SNMP Notification Filter is added to the list, and the device is updated.

11

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

Chapter 11:

# **Configuring Quality of Service**

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

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

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

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

The QoS facility involves the following elements:

- Access Control Lists (ACLs) Used to decide which traffic is allowed to enter the system, and which is to be dropped. Only traffic that meets this criteria are subject to CoS or QoS settings. ACLs are used in QoS and network security.
- **Traffic Classification** Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.
- Assignment to Hardware Queues Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong, as defined by the classification mechanism.
- Traffic Class-Handling Attributes Applies QoS/CoS mechanisms to different classes, including: Bandwidth Management

The Quality of Service section contains the following section:

Chapter 12:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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

The section also contains the following pages:

• Configuring Policy Table

# **Defining General Settings**

The QoS General Settings section contains the following pages:

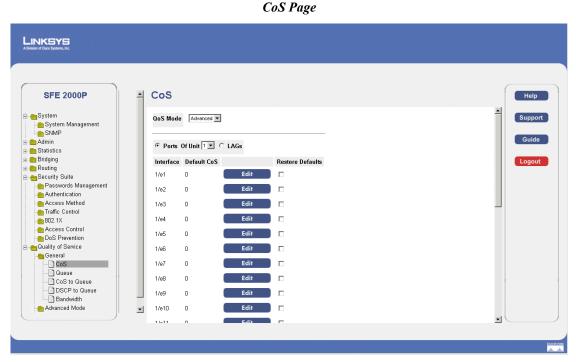
- Defining CoS
- Defining Queue
- Mapping CoS to Queue
- Mapping DSCP to Queue
- Configuring Bandwidth



## **Defining CoS**

The *CoS Page* contains fields for enabling or disabling CoS. In addition, the Trust mode can be selected. The Trust mode relies on predefined fields within the packet to determine the egress queue settings.

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



The CoS Page contains the following fields:

- **QoS Mode** Indicates if QoS is enabled on the interface. The possible values are:
  - Advanced Enables Advanced mode QoS on the interface.
  - Basic Enables QoS on the interface.
  - Disable Disables QoS on the interface.
- **Ports** Displays the ports CoS configuration.
- LAGs Displays the LAGs CoS configuration.
- Of Unit Displays the stacking member for which the CoS parameters are displayed.
- Interface Indicates the interface for which the CoS information is displayed.
- **Default CoS** Displays the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.
- Restore Defaults- Restores the factory CoS default settings to the selected port.

Chapter 12:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Checked Restores the factory QoS default settings to ports.
- Unchecked— Maintains the current QoS settings.

#### 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 2000P	LINKSYS A Debler of Dave Typeteres, Inc.
Edit Interface Priority	
Interface © Port 1/e1 I C LAG 1	
Set Default User Priority	
Apply	

The Edit Interface Priority Page contains the following fields:

- Interface Indicates the port or LAG name.
- Set Default User Priority— Defines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.
- 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:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Queue Page

LINKSYS Division of Cloco Systems, Inc.				
SFE 2000P	∸ Que ⊙ stri	LLE ct Priority <sup>©</sup> WRR		Help Support
SIMP CAdmin Catalistics Catali	Queue	Scheduling WRR % of WRR Weight Bandwidth		Guide Logout
Authentication     Access Method	1 2 3	1 2 3		
Traffic Control  302.1X  Access Control  DoS Prevention  Guality of Service	4	4		
General CoS CoS CoS to Queue DSCP to Queue Bandwidth Advanced Mode				

The Queue Page contains the following fields:

- Strict Priority Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
- WRR Indicates that traffic scheduling for the selected queue is based strictly on the WRR.
- **Queue** Displays the queue for which the queue settings are displayed. The possible field range is 1 4.
- WRR Weight Displays the WRR weights to queues.
- % of WRR Bandwidth Displays the amount of bandwidth assigned to the queue. These values are fixed and are not user defined.
- 2. Define the queues.
- 3. Click Apply. The queues are defined, and the device is updated.

LINKSYS

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## Mapping CoS to Queue

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

Cos to	Queue	Page	

A Division of Cisco Systems, Inc.		
System System System ShMP Admin ShMP Bridging B	CoS to Queue  Restore Defaults  Class of Service  O  1  Class of Service  O  1  Class of Service  O  Cueue  O  1  A  Cueue  O  1  A  Cueue  Cueue Cueue Cueue  Cueue  Cueue  Cueue  Cueue  Cueue  Cueue Cueue Cueue  Cueue Cueue Cueue Cueue Cueue Cue	Help Support Guide Logout

The Cos to Queue Page contains the following fields:

- **Restore Defaults** Restores all queues to the default CoS settings.
- Class of Service Specifies the CoS VLAN (CoS) priority tag values, where zero is the lowest and 8 is the highest.
- **Queue** Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported, where Queue 4 is the highest and Queue 1 is the lowest.
- 2. Define the relevant fields.
- 3. Click Apply. Cos to queues are mapped, and the device is updated.

12

## **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 2000P	DSCP						
SFE 2000P	DSCP	10 Q	ueue				Help
System	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	Suppo
System Management	0	1 -	25	2 -	50	4 -	
Admin	1	1 🔻	26	2 🔻	51	4	Guid
Statistics	2	1 -	27	2 💌	52	4 💌	
Bridging Routing	3	1 💌	28	2 -	53	4	Logou
Security Suite	4	1 💌	29	2 -	54		
- Passwords Management	5	1	30	2 -	55	4	
Access Method	6	1 -	31	2 -	56	4	
Traffic Control	7	1		2 -			
B02.1X			32		57	4	
DoS Prevention	8	1 💌	33	3 💌	58	4	
Quality of Service	9	1 💌	34	3 💌	59	4	
	10	1 💌	35	3 💌	60	4	
	11	1 💌	36	3 💌	61	4 💌	
- CoS to Queue	12	1 💌	37	3 💌	62	4	
Bandwidth	J 13	1 💌	38	3 💌	63	4 💌	
💼 Advanced Mode 📃 💌	] 14	1 💌	39	3 💌			
	15	1 -	40	3 -			

DSCP to Queue Page

The DSCP to Queue Page contains the following fields:

- DSCP In Indicates the Differentiated Services Code Point value in the incoming packet.
- Queue Maps the DSCP value to the selected queue.
- 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 a specified egress interface. Modifying queue scheduling affects the queue settings globally. The *Bandwidth* page is not used with the Service mode, as bandwidth settings are based on services.

Queue shaping can be based per queue and/or per interface. Shaping is determined by the lower specified value. The queue shaping type is selected in the *Bandwidth Page*.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Bandwidth Page

SFE 2000P	Bandwidth	Help
- <del>es</del> System	● Ports Of Unit 1 ▼ ○ LAGs	Support
💼 System Management	Interface Ingress Rate Limit Egress Shaping Rates	
SNMP	Status Rate Limit Egress Snaping Rates	Guide
en Admin En Statistics		Culto
Bridging	1/e1 Edit	Logout
Routing	1/e2 Edit	Logout
escurity Suite		
- 💼 Passwords Management	1/e3 Edit	
- en Authentication	1/e4 Edit	
Traffic Control	1/e5 Edit	
- 602.1X	1/es	
Access Control	1/e6 Edit	
- en DoS Prevention	1/e7 Edit	
Cuality of Service		
	1/e8 Edit	
- Queue	1/e9 Edit	
CoS to Queue		-
- DSCP to Queue	1/e10 Edit	
Bandwidth	1/e11 Edit	
- 💼 Advanced Mode		

The Bandwidth Page contains the following fields:

- Port Indicates the port for which the bandwidth settings are displayed.
- LAG Indicates the LAG for which the bandwidth settings are displayed.
- **Of Unit** Displays the stacking member for which the bandwidth settings are displayed.
- Ingress Rate Limit Status Indicates if rate limiting is defined on the interface. The possible field values are:
  - Enable Enables ingress rate limiting on the interface.
  - Disable Disables ingress rate limiting on the interface.
- Rate Limit Defines the amount of bandwidth assigned to the interface. The possible field values are 62-1000000 Kbps.
- Committed Information Rate (CIR) Defines CIR as the queue shaping type. The possible field value is 64-1,000,000 Kbs.
- Committed Burst Size (CbS) Defines CBS as the queue shaping type. The possible field value is 4096-16,769,020 bits.

Note This field is not supported on FE ports.

#### Modifying Bandwidth Settings

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



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

SFE 2000P		LINKSY A Distance of Data Space	
Edit Bandwidth			
nterface 💿 Port 🚺 🔽 🔿 LAV	G 1 🗾		
Enable Egress Shaping Rate	<b>—</b>		
Committed Information Rate (CIR)	undefined		
0	128000		
Committed Burst Size (CBS)			
Committed Burst Size (CBS) Enable Ingress Rate Limit			

The Edit Bandwidth Page contains the following fields:

- Interface Indicates the interface for which the queue shaping information is displayed. The possible field values are:
  - *Port* Indicates the port for which the bandwidth settings are displayed.
  - LAG Indicates the LAG for which the bandwidth settings are displayed.
- Egress Shaping Rate on Selected Port Indicates if rate limiting is enabled on the interface.
- Committed Information Rate (CIR) Defines CIR as the queue shaping type. The possible field value is 4096 1,000,000 Kbs.

Note This field is not supported on FE ports.

- Committed Burst Size (CbS) Defines CBS as the queue shaping type. The possible field value is 4096-16,769,020 bits.
- Ingress Rate Limit Status Indicates if rate limiting is defined on the interface. The possible field values are:
  - Enable Enables ingress rate limiting on the interface.
  - Disable -- Disables ingress rate limiting on the interface.
- Ingress Rate Limit Defines the amount of bandwidth assigned to the interface. The possible field values are 62-1000000 Kbps.
- 3. Modify the relevant fields.
- 4. Click Apply. The bandwidth settings are modified, and the device is updated.



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# **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 DSCP values from incoming packets to DSCP values in outgoing packets.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



## **DSCP** Mapping Page

DSCP					
	Mappi	ng			Hel
DSCD In	DSCD Out	DSCD In	DSCD Out	DSCD In	DSCP Out
					50 V
					Gui
					51
2		27		52	52 V
3	3 💌	28	28 💌	53	53 💌
4	4 💌	29	29 💌	54	54 💌
5	5 💌	30	30 💌	55	55 💌
6	6 💌	31	31 💌	56	56 💌
					57 💌
					58 💌
9	9 💌	34	34 💌	59	59 💌
10	10 💌	35	35 💌	60	60 💌
11	11 💌	36	36 💌	61	61 💌
12	12 💌	37	37 💌	62	62 💌
	13 💌	38	38 💌	63	63 💌
	0 1 2 3 4 5 6 7 8 9 10 11	0 0 × 1 1 × 2 2 × 3 3 × 4 4 × 5 5 × 6 8 × 7 7 × 8 8 × 9 9 × 10 10 × 11 11 ×	0     0     25       1     1     26       2     2     27       3     3     28       4     4     29       5     5     30       6     6     31       7     7     32       8     8     33       9     9     34       10     10     36       11     11     36       12     12     12	0       0       ×       25       25         1       1       ×       26       26         2       2       ×       27       27         3       3       28       26       ×         4       4       29       29       ×         5       5       30       30       ×         6       6       31       31       ×         7       7       32       32       ×         8       8       33       33       ×         9       9       34       34       ×         10       10       25       55       ×         11       11       36       38       ×	1       1       1       26       26       51         2       2       27       27       52         3       3       28       28       53         4       4       29       28       54         5       5       30       30       55         6       6       31       31       56         7       7       32       32       57         8       8       33       33       58         9       9       34       34       59         10       10       35       35       60         11       11       36       36       61         12       12       37       37       37       62

The DSCP Mapping Page contains the following fields:

- DSCP In Indicates the Differentiated Services Code Point value in the incoming packet.
- DSCP Out Indicates the Differentiated Services Code Point value in the outgoing packet.

## **Defining Class Mapping**

The Defining Class Mapping page enables mapping DSCP values from incoming packets to DSCP values in outgoing packets.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **Class Mapping Page**

LINKSYS A Dinken of Chest Systems, No.		
SFE 2000P	Class Mapping Class: Map ACL 1 Match ACL 2 Delete Add	Help Support Guide Logout

The Class Mapping Page contains the following fields:

- Class Map Name Selects an existing Class Map by name.
- ACL1 Contains a list of the user-defined ACLs.
- Match Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
  - And Both the MAC-based and the IP-based ACL must match a packet.
  - Or Either the MAC-based or the IP-based ACL must match a packet.
- ACL2 Contains a list of the user-defined ACLs.
- 2. Click he Add button. The Add QoS Class Map Page opens:

#### Add QoS Class Map Page

SFE 2000P		LINKSYS A Bridler of Case Typiters, Inc.
	Add Qos Class Map	
Class Map Name		
Preferred ACL	IP Based ACL	
F IP ACL	<b>•</b>	
Match	And 💌	
MAC ACL	<b>Y</b>	
	Apply	

The Add QoS Class Map Page contains the following fields.

• Class Map Name — Defines a new Class Map name



- Preferred ACL Indicates if packets are first matched to an IP based ACL or a MAC based ACL. The possible field values are:
  - *IP Based ACLs* Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.
  - MAC Based ACLs Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.
- IP ACL Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.
- Match Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
  - And Both the MAC-based and the IP-based ACL must match a packet.
  - Or Either the MAC-based or the IP-based ACL must match a packet.
- MAC ACL Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.
- 3. Define the relevant fields.
- 4. Click Apply. QoS mapping is added, and the device is updated.

## **Defining Aggregate Policer**

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

SFE 2000P   System   Admin   Admin   Statistics   Bridging   Security Suite   Orallay of Service   Advanced Mode   DSCP Mapping   Advanced Mode   DSCP Mapping   Policy Table   Policy Table   Basic Mode	LINKSYS A Delader of Data Systems, Inc.		
Admin     A	SFE 2000P	Aggregate Policer	Help
	Admin  Admin  Statistics  Finding  Routing  Guerral  Advanced Mode  Advanced Mode  Aspring  Policy Table  Policy Table Po	pol_agg 10000 10000 Remark DSCP Edit	Guide

Aggregate Policer Page

The Aggregate Policer Page contains the following fields.

Chapter 12:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Aggregate Policer Name— Specifies the Aggregate Policer Name
- Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is Single.
- Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is Single.
- **Exceed Action** Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - Drop Drops packets exceeding the defined CIR value.
  - Remark DSCP Remarks packet's DSCP values exceeding the defined CIR value.
  - None Forwards packets exceeding the defined CIR value.
- 2. Click the Add button. The Add QoS Aggregate Policer Page opens:

#### Add QoS Aggregate Policer Page

SFE 2000P		LINKSYS
Add QoS	Aggregate P	olicer
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

The Add QoS Aggregate Policer Page contains the following fields.

- Aggregate Policer Name— Specifies the Aggregate Policer Name
- Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is Single.
- Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is Single.
- Exceed Action Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - Drop Drops packets exceeding the defined CIR value.
  - Remark DSCP Remarks packet's DSCP values exceeding the defined CIR value.
  - None Forwards packets exceeding the defined CIR value.
- 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 2000P		LINKSYS A Biblier of Oter Systems, Inc.
Edit QoS	Aggregate Po	licer
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

The Edit QoS Aggregate Policer Page contains the following fields.

- Aggregate Policer Name— Specifies the Aggregate Policer Name
- Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is Single.
- Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is Single.
- **Exceed Action** Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - Drop Drops packets exceeding the defined CIR value.
  - Remark DSCP Remarks packet's DSCP values exceeding the defined CIR value.
  - None Forwards packets exceeding the defined CIR value.
- 3. Modify the relevant fields.
- 4. Click Apply. QoS aggregate policer settings are modified, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **Configuring Policy Table**

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

SFE 2000P System Admin Statistics Bridging Routing Security Suite Quality of Service General Advanced Mode	Policy Table  Policy Name pol1 Edit Delete Add	Help Support Guide Logout
- Class Mapping - Aggregate Policer - Policy Table - Policy Binding Basic Mode		

The Policy Table Page contains the following fields:

- **Policy Name** Displays the user-defined policy name.
- 2. Click the Add button. The Add QoS Policy Profile Page opens:

## Add QoS Policy Profile Page

SFE 2000P			
	Add QoS Pol	icy Profile	
New Policy Name			
🗖 Class Map	cls1 💌		
	@Trust CoS-DSCP		
Action	CSet DSCP New	v Value 🛛	(0 - 63)
V Police			,
Туре	Aggregate 💌		
Aggregate Policer	pol_agg 💌		
Ingress Committed Information Rate (CIR)(3-12,582,912)	10000	(Kbits per Second)	
Ingress Committed Burst Size (CBS)(3,000-19,173,960)	10000	(Bytes)	
Exceed Action	None	]	
			Apply

The Add QoS Policy Profile Page contains the following fields.

- New Policy Name— Displays the user-defined policy name.
- Class Map Displays the user-defined class maps which can be associated with the policy.



- Action Defines the action attached to the rule. The possible field values are:
  - Trust CoS-DSCP Enables Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.
  - Set Manually configures the Trust.
- **Police** Enables Policer functionality.
- **Type** Policer type for the policy. Possible values are:
  - Aggregate Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
  - Single Configures the class to use manually configured information rates and exceed actions.
- Aggregate Policer Specifies the Aggregate Policer Name
- Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is Single.
- Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is Single.
- **Exceed Action** Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - Drop Drops packets exceeding the defined CIR value.
  - Remark DSCP Remarks packet's DSCP values exceeding the defined CIR value.
  - None Forwards packets exceeding the defined CIR value.
- 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

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SFE 2000P		
	Edit Qos Policy Profile	
Policy Name		
🗌 Class Map		
C Action	C Trust CoS-DSCP	
	C Set DSCP Y New Value	(0 - 63)
Police		
Туре		
Aggregate Policer		
Ingress Committed Information Rate (CIR)	(Kbits per Second)	
Ingress Committed Burst Size (CBS)	(Bytes)	
Exceed Action	None	
Class-Map Trust Set Attribute S	Policer Name	
	Delete	
	Ar	ply

#### Edit QoS Policy Profile Page

The Edit QoS Policy Profile Page contains the following fields.

- New Policy Name— Displays the user-defined policy name.
- Class Map Displays the user-defined name of the class map.
- Action Defines the action attached to the rule. The possible field values are:
  - Trust CoS-DSCP Enables Trust Mode for the class. This command is used to distinguish
    the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism
    maps a packet to a queue using the received or default value and the relevant map, as
    defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic
    with certain DSCP values.
  - Set Manually configures the Trust.
- **Police** Enables Policer functionality.
- **Type** Policer type for the policy. Possible values are:
  - Aggregate Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
  - Single Configures the class to use manually configured information rates and exceed actions.
- Aggregate Policer Specifies the Aggregate Policer Name
- Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is Single.



- Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is Single.
- **Exceed Action** Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - Drop Drops packets exceeding the defined CIR value.
  - Remark DSCP Remarks packet's DSCP values exceeding the defined CIR value.
  - None Forwards packets exceeding the defined CIR value.
- 2. Define the relevant fields.
- 3. Click Apply. The QoS policy profile is defined, and the device is updated.

## **Defining Policy Binding**

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

#### **Policy Binding Page**

SFE 2000P	Policy Binding Interface Policy Name Delete Add	Help Support Guide Logout

The Policy Binding Page contains the following fields:

- Interface Displays the interface to which the entry refers.
- **Policy Name** Displays a Policy name configured to the interface.
- 2. Click the Add button. The Add QoS Policy Binding Page opens:

Chapter 12:



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add QoS Policy Binding Page



The Add QoS Policy Binding Page contains the following fields.

- Interface Displays the interface to which the entry refers.
- **Policy Name** Displays a Policy name configured to the interface.
- 3. Define the relevant fields.
- 4. Click Apply. The QoS Policy Binding is defined, and the device is updated.

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:

SFE 2000P		LINKSYS A Dividior of Doce Tyritema, Inc.
	Edit Qos Policy Binding	
Interface 1		
Policy Name 💽		
Apply		

## Edit QoS Policy Binding Page

The Edit QoS Policy Binding Page contains the following fields.

- **Interface** Displays the interface to which the entry refers.
- **Policy Name** Displays a Policy name configured to the interface.
- 3. Define the relevant fields.
- 4. Click Apply. The QoS policy binding is defined, and the device is updated.

# (12)

## **Defining QoS Basic Mode**

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

LINKSYS Atomat i Gas System, IX.	Basic Mode Page	
SFE 2000P	Trust state disable while the system is not in the QoS Basic model   Trust Mode   Image: Comparison of the co	Help Support Guide Logout

The Basic Mode Page contains the following fields:

- **Trust Mode** Displays the trust mode. If a packet's CoS tag and DSCP tag, and TCP/UDP mapping are mapped to different queues, the Trust Mode determines the queue to which the packet is assigned. Possible values are:
  - CoS Sets trust mode to CoS on the device. The CoS mapping determines the packet queue
  - DSCP Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue.
- 2. Click the **DSCP Rewrite** button. The *DSCP Mapping Page* opens:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

			DSCP	Mappi	ing Pag	е	
	SFE 2000P						LINKSYS A Distance of Disco Typesona, Inc.
			DSC	P M	appin	a	
						3	
DSC	P In DSCP Out	DSCP Ir	DSCP Out	DSCP In	DSCP Out	DSCP I	n DSCP Out
0	1 -	16	1 -	32	1 -	48	1 -
1	1 -	17	1 -	33	1 -	49	1 -
2	1 -	18	1 👻	34	1 🗸	50	1 -
3	1 -	19	1 -	35	1 -	51	1 -
4	1 🚽	20	1 🗸	36	1 🗸	52	1 -
5	1 -	21	1 -	37	1 -	53	1 -
6	1 -	22	1 -	38	1 -	54	1 -
7	1 -	23	1 -	39	1 -	55	1 -
8	1 -	24	1 -	40	1 -	56	1 -
9	1 🗾	25	1 👻	41	1 🗸	57	1 -
10	1 -	26	1 -	42	1 -	58	1 -
11	1 -	27	1 -	43	1 -	59	1 -
12	1 -	28	1 -	44	1 -	60	1 -
13	1 -	29	1 -	45	1 -	61	1 -
14	1 -	30	1 🗸	46	1 🗸	62	1 -
15	1 -	31	1 -	47	1 -	63	1 -
						-	
							Apply

The *DSCP Mapping Page* enables mapping DSCP values from incoming packets to DSCP values in outgoing packets. The *DSCP Mapping Page* contains the following fields:

- DSCP In Indicates the Differentiated Services Code Point value in the incoming packet.
- DSCP Out Indicates the Differentiated Services Code Point value in the outgoing packet.
- 3. Define the DSCP mappings.
- 4. Click Apply. The DSCP mappings are defined, and the device is updated.

# **Managing System Files**

## **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.

The File Management section contains the following pages:

- Firmware Upgrade
- Save Configuration
- Copy Files
- Active Image



## **Firmware Upgrade**

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

Firmware Upgrade Page

LINKSYS A Designer of Check Systems, Inc.		
SCE 2000 System Admin File Management Save Configuration Copy Files Diagnostics Statistics Statistics Bridging Scurity Suite Courly Suite Courly Suite Courly Suite Courly Suite Courly Suite	Firmware Upgrade     © UPGRADE © BACKUP     File Type        FIP Server        Source File        Destination File     Verter Active Image	Help Support Guide Logout

The Firmware Upgrade Page contains the following fields:

- Upgrade Specifies the firmware upgrade is an upgrade function.
- Backup Specifies the firmware upgrade is a backup function.
- File Type Specifies the destination file type to which to the file is downloaded. The possible field values are:
  - Software Image Downloads the Image file.
  - Boot Code Downloads the Boot file.
- TFTP Server Specifies the TFTP Server IP Address from which files are downloaded.
- Source File Specifies the file to be downloaded.
- Destination File Specifies the downloaded file name.
- 2. Define the relevant fields.
- 3. Click Apply. Firmware upgrade is defined, and the device is updated.

## **Save Configuration**

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

LINKSYS A Unitari of Cases Systems, Inc.		
SGE 2000 System Admin File Management Copy Files Active Image Diagnostics Statistics Security Suite Quality of Service	Save Configuration	Help Support Guide Logout
		Case Section

The Save Configuration Page contains the following fields:

- Upgrade Specifies the firmware upgrade is an upgrade function.
- Backup Specifies the firmware upgrade is a backup function.
- File Type Specifies the Configuration file to be saved.
- TFTP Server Specifies the TFTP Server IP Address from which file is downloaded.
- Source File Specifies the file to be downloaded.
- Destination File— Specifies the saved file name.
- 2. Define the relevant files.
- 3. Click Apply. The save configuration is defined, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **Copy Files**

All software images on the stack must be identical to ensure proper operation of the stack. There are two different ways to update images across the stack:

- Image can be updated prior to connecting a unit to the stack. (This is the recommended method.)
- Upgrade master and copy master image to units across the stack.

These steps can be done from the Menu-Based CLI or from the web interface.

- a. Copy image from TFTP to master
- b. Change active image on master
- c. Reboot master
- d. Copy from master to rest of units
- e. Change active of rest of units
- f. Reload only rest of units and not master.

**NOTE:** If there is a backup master in the stack, it takes over as master of the stack following step (c) above. In such a case steps (a) - (c) should be run on the (old backup) new master unit.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



## Copy Files Page

LINKSYS		
SCE 2000 System Admin File Management Save Configuration Copy Files Active Image Diagnostics Bridging Routing Bridging Routing Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Copy Files Diagnostics Copy Files Diagnostics Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Copy Files Diagnostics Diagnostics Bridging Copy Files Diagnostics Bridging Copy Files Diagnostics Copy Files Diagnostics Diagnostics Copy Files Diagnostics Di	escere Configuration Factory Defaults   • Cary Master Firmware   Surce   • Cary Configuration   • Cary Configuration   Surce File Name   • Configuration   • Configuration   • Cary Configuration	Help Support Guide Logout

The Copy Files Page contains the following fields:

- **Restore Configuration Factory Defaults** Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When not selected, the device maintains the current Configuration file.
- **Copy Master Firmware** Indicates the Stacking Master configuration file to copy. The possible field values are:
  - Source Copies the current Stacking Master's firmware.
  - Destination Unit Defines the stacking member to which the firmware is downloaded.
- Copy Configuration Indicates the device configuration to be copied.
- Source File Name Indicates the configuration file copied.
  - Destination File Name Defines the stacking member to which the configuration file is downloaded.
- 2. Define the relevant fields.
- 3. Click Apply. Copy Files is configured, and the device is updated.

## **Active Image**

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

Chapter 13:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Active Image Page

SGE 2000 System Admin File finanagement Save Configuration Copy Files Active Image	Active Image Unit No. Active Image After Reset 1 Image 1 Image 1 2 Image 1 Image 1 3 Image 1 Image 1 Apply	Help Support Guide Logout
Diagnostics     Statistics     Bridging     Routing     Security Suite     Quality of Service		

The Active Image Page contains the following fields:

- Unit No. Indicates the unit number for which the Image file is selected.
- Active Image Indicates the Image file which is currently active on the unit.
- After Reset The Image file which is active on the unit after the device is reset. The possible field values are:
  - Image 1 Activates Image file 1 after the device is reset.
  - Image 2 Activates Image file 2 after the device is reset.
- 2. Define the relevant fields.
- 3. Click Apply. Active image is define, and the device is updated.

14

# **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**

The *Log Settings Page* contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. The Severity log messages are listed from the highest severity to the lowest. To define Log Global Parameters:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Log Settings Page

Admin     File Management     Severity     Console     Memory Logs     Log Flash       Isog Settings     Emergency     IV     IV     IV       File Management     Emergency     IV     IV     IV       Bridging     Alart     IV     IV     IV       Objerosities     Critical     IV     IV     IV       Statistics     Error     IV     IV     IV       Southy Suite     Waming     IV     IV     IV       Quality of Service     Informational     IV     IV     IV	System Admin File Management	Enable Loggi					He
Severity     Console     Memory Logs     Log Flash       Memory     Filash     Filash     Filash     Filash       Delagnestics     Critical     Filash     Filash       Statistics     Firor     Filash     Filash       Routing     Karning     Filosh     Filosh       Security Suite     Notice     Filosh     Filosh       Debug     Filosh     Filosh     Filosh		Lilable Luggi	ing 🗹				Sup
Emergency     Image: Construction       Flash       Remote Log Servers       Depositics       Diagnostics       Statistics       Error       Image: Construction       Varing       Varing       Notice       Informational       Image: Construction		Severity	Console	Memory Logs	Log Flash		Gui
Alert     IF     IF     IF       Bennete Log Servers     Critical     IF     IF       Diagnostics     Critical     IF     IF       Statistics     Error     IF     IF       Browning     Warning     IF     IF       Security Suite     Notice     IF     IF       Duality of Service     Informational     IF     IF	Memory	Emergency	•	<b>V</b>	V		Log
Diagnostics     Critical     IP     IP       Statistics     Error     IP     IP       Statistics     Error     IP     IP       Routing     Warning     IP     IP       Security Suite     Notice     IP     IP       Quality of Service     Informational     IP     IP		Alert		•	V		
Statistics     Error     I     I       Bridging     Warning     I     I       Routing     Varning     I     I       Becurity Suite     Notice     I     I       Duality of Service     Informational     I     I	Remote Log Servers     Diagnostics	Critical	V	•	V		
Routing Warning V Arice V C Security Suite Notice V F Duality of Service Debug Debug	Statistics	Error	•	V	V		
Security Suite Notice II Informational II II IIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Warning	~	V			
Debug	Security Suite	Notice	V	•			
	Quality of Service	Informational	V	V			
Apply		Debug					
		Apply					
		Apply					

The Log Settings Page contains the following fields:

- Enable Logging Indicates if device global logs for Console, Memory Logs, and Log Flash.
- Severity The following are the available severity logs:
  - Emergency The system is not functioning.
  - Alert The system needs immediate attention.
  - Critical The system is in a critical state.
  - Error A system error has occurred.
  - Warning A system warning has occurred.
  - Notice The system is functioning properly, but system notice has occurred.
  - Informational Provides device information.
  - Debug Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.
- Console Provides information about logs saved to the console.
- Memory Logs Defines all system logs in a chronological order that are saved in RAM (Cache)
- Log Flash Defines the minimum severity level from which logs are sent to the Message Log kept in FLASH memory.

14

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

## Viewing the Device Memory Logs

The *Memory Log Page* contains all system logs in a chronological order that are saved in RAM (Cache). To open the *Memory Page*:

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

SGE 2000	Memory	/			Help
System Admin	Log Index	Log Time	Severity	Description	Suppor
File Management	2147483371	01-Jan-2000 19:09:06	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	
Logs	2147483372	01-Jan-2000 18:42:00	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	Guide
Log Settings	2147483373	01-Jan-2000 18:41:55	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.E	
	2147483374	01-Jan-2000 18:30:13	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	Logout
Remote Log Servers	2147483375	01-Jan-2000 18:00:30	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	
💼 Diagnostics	2147483376	01-Jan-2000 18:00:25	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.6	
Statistics	2147483377	01-Jan-2000 17:34:34	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	
Bridging Routing	2147483378	01-Jan-2000 03:41:43	Informational	%AAA-I-DISCONNECT: User CLI session for user admin over consc	
Security Suite	2147483379	01-Jan-2000 03:23:55	Informational	%AAA-I-CONNECT: User CLI session for user admin over console ,	
Quality of Service	2147483380	01-Jan-2000 03:21:23	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.E	
	2147483381	01-Jan-2000 03:20:16	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10	
	2147483382	01-Jan-2000 03:00:17	Informational	%AAA-I-DISCONNECT: User CLI session for user admin over consc	
	2147483383	01-Jan-2000 02:50:14	Informational	%AAA-I-CONNECT: User CLI session for user admin over console ,	
	2147483384	01-Jan-2000 02:29:11	Informational	%AAA-I-DISCONNECT: User CLI session for user admin over consc	
		01-Jan-2000 02:19:41	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.6	
	•			Distancial Distance in the second sec	
				Clear Logs	

The *Memory Page* contains all system logs in a chronological order that are saved in RAM (Cache). The *Memory Page* contains the following fields:

- Log Index Displays the log number.
- Log Time Displays the time at which the log was generated.
- Severity Displays the log severity.
- **Description** Displays the log message text.

### **Clearing Message Logs**

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

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

Chapter 14:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

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 log 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

Log Index       Log Time       Severity       Description       Image: Severity       Support         File Management       2147229975       01-Jan-2000 01:10:22       Alert       %TFIP-A-ThtpRxERROR: An error message was received: 1 <file no<="" td="">       Guid         Log Settings       214723099       01-Jan-2000 01:03:17       Alert       %Box-AFAN-STAT-CHING: FAN#2 status is - not operational.       Guid</file>	SGE 2000	Flash				Help
Admin         Log Index         Memory         Index         Statistics         214723029         01-Jan-2000 01:01:37         Alert         %Box-AFAN-STAT-CHNG: FAM#2 status is - not operational.         Guida           Image: Index         Log Settings         2147231204         01-Jan-2000 01:01:33         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpsLmTransLog2Phy: no suct         Log           Image: Index         Lag 2000 01:00:133         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpsLmTransLog2Phy: no suct         Log           Image: Index         11/Jan-2000 01:00:133         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpsLmTransLog2Phy: no suct         Log           Image: Index         214723229         01-Jan-2000 01:05:07         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Log           Statistics         214723289         01-Jan-2000 01:05:03         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Log         Log         Log         Log         Log         Log         Log         Log		ridon				
File Management         214722997         01-Jan-2000 01:10:22         Alet         % TFTP-A-TtpPA:ERROR: An enror message was received: 1 <file no<="" td="">           Logos         214722909         01-Jan-2000 01:01:22         Alet         % DTP-A-TtpPA:ERROR: An enror message was received: 1 <file no<="" td="">           Logos         214722909         01-Jan-2000 01:01:37         Alet         % Box-AFAN-STAT-CHNS: FAM#2 status is - not operational.         Could           Memory         214723209         01-Jan-2000 01:01:38         Emergency         % SYSLOG-F-OSFATAL: Spm Ernor: dpssLmTransLog2Phy: no suct         Logos           Diagnostics         214723229         01-Jan-2000 01:05:07         Alet         % Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Logos           Statistics         214723249         01-Jan-2000 01:05:07         Alet         % Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Logos           Bridging         214723259         01-Jan-2000 01:05:07         Alet         % Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Logos           Bridging         214723259         01-Jan-2000 01:05:07         Alet         % Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Logos           Bridging         214723269         01-Jan-2000 01:05:07         Alet         % Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Logos</file></file>		Log Index	Log Time	Severity	Description	Suppo
214723029       01-Jan-2000 01:03:17       Alert       %Box-Ar-FAN-STAT-CHNG: FAN#2 status is - not operational.       Guidal         Log Settings       2147231204       01-Jan-2000 01:01:33       Emergency       %SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no suct       Log         Memory       214723229       01-Jan-2000 01:01:33       Emergency       %SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no suct       Log         Diagnostics       214723229       01-Jan-2000 01:05:7       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Log         Statistics       214723269       01-Jan-2000 01:05:5       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Log         Bridging       214723289       01-Jan-2000 01:05:5       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Log         Statistics       214723289       01-Jan-2000 01:05:5       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Statistics         Bridging       214723289       01-Jan-2000 01:05:3       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Log         Routing       214723289       01-Jan-2000 01:04:31       Alert       %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       Life         Quality of Service       214723289       01-Jan-2000 01:04:31			•			
Log Settings         2147231204         01-Jan-2000 01:01:33         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no suct         Log           Memory         2147232209         01-Jan-2000 01:01:33         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no suct         Log           Diagnostics         2147232209         01-Jan-2000 01:00:133         Emergency         %SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no suct         Log           Statistics         2147232239         01-Jan-2000 01:05:16         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           Statistics         214723289         01-Jan-2000 01:05:16         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           Statistics         214723289         01-Jan-2000 01:05:13         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           Security Suite         01-Jan-2000 01:05:13         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           214723289         01-Jan-2000 01:05:13         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           Security Suite         01-Jan-2000 01:04:14         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)         Here           2147233289		2147230099	01-Jan-2000 01:03:17	Alert		Guide
Flash       214/232203       01-Jan-2000 01:03:33       Emergency       %SYSL0GF-/OSFATAL: Spm Error. dpscImfraneLog2PP): no such         Privation       Permote Log Servers       214/23223       01-Jan-2000 01:06:07       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         Statistics       214/232349       01-Jan-2000 01:05:05       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         Bridging       214/23289       01-Jan-2000 01:05:55       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         Bridging       214/23289       01-Jan-2000 01:05:55       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         Security Suite       214/23289       01-Jan-2000 01:05:03       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         Ouality of Service       214/23289       01-Jan-2000 01:04:03       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         214/23289       01-Jan-2000 01:04:15       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         214/233299       01-Jan-2000 01:04:15       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         214/233299       01-Jan-2000 01:03:43       Alert       %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)         214/233299       01-Jan-2000 01:03:43       Alert       %	Log Settings	2147231204	01-Jan-2000 01:01:33	Emergency	%SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no such	
Remote Log Servers         214723329         01-Jan-2000 01:06.07         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Statistics         214723329         01-Jan-2000 01:05.05         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Statistics         214723329         01-Jan-2000 01:05.05         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Bridging         214723289         01-Jan-2000 01:05.05         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Bridging         214723289         01-Jan-2000 01:05.05         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Brouting         214723289         01-Jan-2000 01:05.05         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Security Suite         214723289         01-Jan-2000 01:04.07         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723349         01-Jan-2000 01:04.17         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723349         01-Jan-2000 01:04.17         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723349         01-Jan-2000 01:03.15         Alet         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723349         01-Jan-2000 01:03.27 <td></td> <td>2147232209</td> <td>01-Jan-2000 01:01:33</td> <td>Emergency</td> <td>%SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no such</td> <td>Logou</td>		2147232209	01-Jan-2000 01:01:33	Emergency	%SYSLOG-F-OSFATAL: Spm Error: dpssLmTransLog2Phy: no such	Logou
Diagnostics         214723249         01-Jan-2000 01:05:51         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Bridging         214723268         01-Jan-2000 01:05:55         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Bridging         214723268         01-Jan-2000 01:05:55         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Bridging         214723289         01-Jan-2000 01:05:55         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Brodging         214723289         01-Jan-2000 01:05:05         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           Boulaity of Service         214723329         01-Jan-2000 01:04:47         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723319         01-Jan-2000 01:04:47         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723319         01-Jan-2000 01:04:47         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723329         01-Jan-2000 01:04:47         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233192         01-Jan-2000 01:03:45         Alert         %Box-A:TEMP-RISING-ALARM: Over temperature (sensor 1)           214723309         01-Jan-2000 01:03:37         Alert </td <td></td> <td>2147232329</td> <td>01-Jan-2000 01:06:07</td> <td>Alert</td> <td>%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)</td> <td></td>		2147232329	01-Jan-2000 01:06:07	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
Bridging         2147.23280         01/347.23000         01/347.23000         01/347.23000         01/347.23000         01/347.23000         01/347.23000         01/347.23080		2147232449	01-Jan-2000 01:05:51	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
Routing         214/223698         01-Jan-2000 01:05:19         Alert         %Box-A-1EMP-RISING-ALARM: Over temperature (sensor 1)           Security Suite         2147232089         01-Jan-2000 01:05:03         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           Ouality of Service         214723209         01-Jan-2000 01:04:07         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723309         01-Jan-2000 01:04:47         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723309         01-Jan-2000 01:04:47         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233299         01-Jan-2000 01:04:57         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233299         01-Jan-2000 01:04:57         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233299         01-Jan-2000 01:04:57         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233299         01-Jan-2000 01:03:59         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233299         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233599         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)<		2147232569	01-Jan-2000 01:05:35	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
Security Suite         2147233209         01-Jan-2000 01:05:03         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           Ouality of Service         2147233293         01-Jan-2000 01:04:47         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233293         01-Jan-2000 01:04:47         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723369         01-Jan-2000 01:04:31         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723369         01-Jan-2000 01:03:51         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723369         01-Jan-2000 01:03:59         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723369         01-Jan-2000 01:03:43         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723359         01-Jan-2000 01:03:43         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723359         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723359         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147232689	01-Jan-2000 01:05:19	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
Quality of Service         214723292         01-Jan-2000 01:04:47         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723304         01-Jan-2000 01:04:17         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233169         01-Jan-2000 01:04:17         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233169         01-Jan-2000 01:03:15         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233269         01-Jan-2000 01:03:26         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723369         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723359         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           214723359         01-Jan-2000 01:03:27         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147232809	01-Jan-2000 01:05:03	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
2147233169         D1-Jan-2000         D1-Jan-2000         O1-Jan-2000         O1-Jan-2000         Mark         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233289         D1-Jan-2000         D1-Jan-2000         Alet         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233499         D1-Jan-2000         D1-Jan-2000         Alet         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233599         D1-Jan-2000         D1-Jan-2000         Alet         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233599         D1-Jan-2000         D1-Jan-2000         Alet         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147232929	01-Jan-2000 01:04:47	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
2147233289         D1-Jan-2000         D1-33:59         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233499         D1-Jan-2000         D1-33:43         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233599         D1-Jan-2000         D1-32:7         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)           2147233529         D1-Jan-2000         D1-32:7         Alert         %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147233049	01-Jan-2000 01:04:31	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
2147233409     D1-Jan-2000     D1-03:43     Alert     %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)       2147233529     D1-Jan-2000     D1-03:27     Alert     %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147233169	01-Jan-2000 01:04:15	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
2147233529 D1-Jan-2000 01:03:27 Alert %Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)		2147233289	01-Jan-2000 01:03:59	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
		2147233409	01-Jan-2000 01:03:43	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	
		2147233529	01-Jan-2000 01:03:27	Alert	%Box-A-TEMP-RISING-ALARM: Over temperature (sensor 1)	1
		•			Þ	
Clear Logs					Clear Logs	

The Flash Page contains the following fields:

- Log Index Displays the log number.
- Log Time Displays the time at which the log was generated.
- Severity Displays the log severity.
- **Description** Displays the log message text.

## **Clearing Message Logs**

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

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

230

14

## **Viewing Remote Logs**

The *Remote Log Servers Page* contains information for viewing and configuring the Remote Log Servers. New log servers can be defined, and the log severity sent to each server.

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

#### **Remote Log Servers Page**

A Denixer of Choce Systems, Inc.		
SGE 2000 System Admin File Management Cos Cos Flash Flash Flash Flash Bridging Routing Generative Bridging Bridging Brid Bridging Brid Brid Bridging Brid Bri	Server       UDP Port       Facility       Description       Minimum Severity         192.188.1.10       514       Local 7       Informational       Edit         Delete       Add	Help Support Guide Logout
		Case Strikes

The Remote Log Servers Page contains the following fields:

- Server Specifies the server IP address to which logs can be sent.
- UDP Port Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 Local 7**.
- **Description** Provides a user-defined server description.
- Minimum Severity Indicates the minimum severity from which logs are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.
- 2. Click the Add button. The Add Syslog Server Page opens:

Chapter 14:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add Syslog Server Page

SGE 2000		LINKSYS A Dataset of Class Systems, Inc.
	Add Syslog Serve	r
Log Server IP Address		
UDP Port	514	
Facility	Local 7 💌	
Description	×	
Minimum Severity	Informational 💌	
	Apply	

The *Add Syslog Server Page* contains information for viewing and configuring the Remote Log Servers. New log servers can be defined, and the log severity sent to each server.

The Add Syslog Server Page contains the following fields:

- Log Server IP Address Specifies the server to which logs can be sent.
- **UDP Port** Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 Local 7**.
- Description Provides a user-defined server description.
- **Minimum Severity** Indicates the minimum severity from which logs are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.
- 3. Define the relevant fields.
- 4. Click **Apply.** The *Add Syslog Server Page* closes, the syslog server is added, and the device is updated.

#### Modify Syslog Server Settings

- 1. Click Admin > Logs > Remote Log Servers. The Remote Log Servers Page opens:
- 2. Click the Edit button. The Syslog Server Settings Page opens:



#### Syslog Server Settings Page

SGE 2000		LINKSYS A Unider of Disco Typiteres, Inc.
	Syslog Server Settings	
Server	192.168.1.10 💌	
UDP Port	514	
Facility	Local 7 💌	
Description		
Severity To Include	Informational 💌	
	Apply	

The Syslog Server Settings Page contains the following fields:

- Server Specifies the server to which logs can be sent.
- UDP Port (1-65535) Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 Local 7**.
- **Description** Provides a user-defined server description.
- Severity to Include Indicates the minimum severity from which logs are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.
- 3. Define the relevant fields.
- 4. Click Apply. The Syslog Server settings are modified, and the device is updated.

14

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

Chapter 14:

15

# **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 different system time aspects, including:

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



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

## **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:

SGE 2000	Sustan Tin		Help
5GE 2000	System Time	3	нер
System - System Management	Clock Source	C Local Settings C SNTP	Support
	Local Settings		Guide
- 🔄 Stack Management	Date	01/Jan/00 (DDMMM/YY)	
Health	Local Time	20.02.52 (HH:MM:SS)	Logout
Time	Time Zone Offset	GMT 💌	
SNTP Settings	🗖 Daylight Saving	🕼 USA 🌑 European 🖷 Other	
👝 IP Addressing	Time Set Offset	80 (Min)	
en Domain Name System System	From	(DDAMMMYY) (HH:MM)	
Admin Statistics	То	(DDMMM/YY) (HH:MM)	
Bridging Routing	Recurring		
Security Suite	From	Day Sun 💌 Week First 🛒 Month Jan 💌 Time 00000 (HH:MM)	
Quality of Service	То	Day Sun 🗹 Week First 🗾 Month Jan 💌 Time 00.00 (HH:MM)	
	Apply		

System Time Page

The System Time Page contains the following fields:

- Clock Source Indicates the source used to set the system clock. The possible field values:
  - SNTP Sets the system time is set via an SNTP server.
  - Local Settings Sets that the system time is not set by an external source. This is the default value.
- Date Indicates the system date. The field format is Day:Month:Year, for example, 04 May 2050.
- Local Time Indicates the system time. The field format is HH:MM:SS, for example, 21:15:03.
- **Time Zone Offset** Indicates the difference between *Greenwich Mean Time* (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GMT -5. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area.



- Daylight Savings Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:
  - USA The device switches to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.
  - *European* The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.
  - Other The DST definitions are user-defined based on the device locality. If Other is selected, the From and To fields must be defined.
- **Time Set Offset (1-1440)** For non USA and European countries, Indicates the amount of time for DST can be set in minutes. The default time is 60 minutes. Day:Month:Year in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25Oct07 and 5:00. The possible field values are:
  - Date The date at which DST begins. The possible field range is 1-31.
  - Month The month of the year in which DST begins. The possible field range is Jan-Dec.
  - Year The year in which the configured DST begins.
  - *Time* The time at which DST begins. The field format is Hour:Minute, for example, 05:30.
- To Indicates the time that DST ends in countries other than USA or Europe in the format DayMonthYear in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23Mar08 and 12:00. The possible field values are:
  - Date The date at which DST ends. The possible field range is 1-31.
  - Month The month of the year in which DST ends. The possible field range is Jan-Dec.
  - Year— The year in which the configured DST ends.
  - *Time* The time at which DST starts. The field format is Hour: Minute, for example, 05:30.
- **Recurring** Indicates the time that DST starts in countries other than USA or European where the DST is constant year to year. The possible field values are:
- From Indicates the time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:
  - *Day* The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
  - Week The week within the month from which DST begins every year. The possible field range is 1-5.
  - Month The month of the year in which DST begins every year. The possible field range is Jan.-Dec.

Chapter 15:

237

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- *Time* The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.
- To Indicates the recurring time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:
  - Day The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
  - Week The week within the month at which DST ends every year. The possible field range is 1-5.
  - Month The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
  - *Time* The time at which DST ends every year. The field format is Hour:Minute, for example, 05:30.
- 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* provides information for defining SNTP parameters globally. To define SNTP global parameters:

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

SCE 200   System Management   Orgen   Stack Management   Stack Management <td></td>	

**SNTP Settings Page** 

The SNTP Settings Page contains the following fields:



- Enable SNTP Broadcast Enables polling the selected SNTP Server for system time information, when enabled.
- SNTP Server Indicates the user-defined SNTP server IP address. Up to eight SNTP servers can be defined
- **Poll Interval** Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. By default, the poll interval is 1024 seconds.
- Encryption Key ID Indicates the Key Identification used to communicate between the SNTP server and device. The range is 1 4294967295
- **Preference** The SNTP server providing SNTP system time information. The possible field values are:
  - Primary The primary server provides SNTP information.
  - Secondary The backup server provides SNTP information.
  - In progress The SNTP server is currently sending or receiving SNTP information.
  - *Unknown* The progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.
- Status The operating SNTP server status. The possible field values are:
  - Up The SNTP server is currently operating normally.
  - Down Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
- Last Response Indicates the last time a response was received from the SNTP server.
- Offset Indicates the Timestamp difference between the device local clock and the acquired time from the SNTP server.
- Delay Indicates the amount of time it takes to reach the SNTP server.
- 2. Click the Add button. The Add SNTP Server Page opens:



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add SNTP Server Page

SGE 2000		LINKSYS A Direlfor of Disco Systems, Inc.
	Add SNTP Server	
SNTP Server		
🥅 Enable Poll Interval		
Encryption Key ID	<b>V</b>	
	Apply	

The Add SNTP Server Page contains the following fields:

- SNTP Server Defines user-defined SNTP server IP address.
- Enable Poll Interval Indicates whether or not the device polls the selected SNTP server for system time information.
- Encryption Key ID Indicates the Key Identification used to communicate between the SNTP server and device. The range is 1 4294967295
- 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 defining the means by which the SNTP server is authenticated.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



### SNTP Authentication Page

SCE 2000   System Management   System Information   Domain Name System   Domain Name System   System Information   System System   Domain Name System   System Information   System Information	LINKSYS A Division of Clause Systems, No.		
	System System Management System Information System Information System Information Health Reset Time SNTP Settings NTP Addinetication P Addmin SNTP Addination SNMP Admin Source	Enable SNTP Authentication	Support Guide

The SNTP Authentication Page contains the following fields:

- Enable SNTP Authentication Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:
  - Checked Authenticates SNTP sessions between the device and SNTP server.
  - Unchecked Disables authenticating SNTP sessions between the device and SNTP server.
- Encryption Key ID Defines the Key Identification used to authenticate the SNTP server and device. The field value is up to 4294967295 characters.
- Authentication Key Displays the key used for authentication.
- **Trusted Key** Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.
- 2. Click the Add button. The Add SNTP Authentication Page opens:



SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Add SNTP Authentication Page

SGE 2000		LINKSYS A Unities of Case Systems, Inc.
	Add SNTP Authenticati	on
Encryption Key ID		
Authentication Key		
Trusted Key		
	Apply	

The Add SNTP Authentication Page contains the following fields:

- Encryption Key ID Defines the Key Identification used to authenticate the SNTP server and device. The field value is up to 4294967295 characters.
- Authentication Key Displays the key used for authentication.
- **Trusted Key** Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.
- 3. Define the relevant fields.
- 4. Click Apply. The SNTP Authentication is defined, and the device is updated.

16

## **Viewing Statistics**

This section provides 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:

 $\mathbf{b}$ 

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Interface Page

SGE 2000	Interface	Help
System	Interface  • Port 1/g1  • C LAG 1	Support
Admin Statistics	Refresh Rate No Refresh 💌	Guide
	Receive Statistics	
	Total Bytes (Octets) 0	Logout
mon	Unicast Packets 0	
💼 Bridging 💼 Routing	Multicast Packets 0	
Security Suite	Broadcast Packets 0	
Guainty of Service	Packets with Errors 0	
	Transmit Statistics	
	Total Bytes (Octets) 0	
	Unicast Packets 0	1
	Multicast Packets 0	
	Broadcast Packets 0	
	Clear Counters	

The Interface Page contains the following fields:

The General Information area contains the following fields:

- Interface Indicates the device for which statistics are displayed. The possible field values are:
  - Port Defines the specific port for which Ethernet statistics are displayed.
  - LAG Defines the specific LAG for which Ethernet statistics are displayed.
- **Refresh Rate** Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - 15 Sec Indicates that the Ethernet statistics are refreshed every 15 seconds.
  - 30 Sec Indicates that the Ethernet statistics are refreshed every 30 seconds.
  - 60 Sec Indicates that the Ethernet statistics are refreshed every 60 seconds.
  - No Refresh Indicates that the Ethernet statistics are not refreshed.

The Receive Statistics area contains the following fields:

- Total Bytes (octets) Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- Unicast Packets Displays the number of good Unicast packets received on the interface since the device was last refreshed.



- **Multicast Packets** Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **Broadcast Packets** Displays the number of good broadcast packets received on the interface since the device was last refreshed.
- Packets with Errors Displays the number of packets with errors.

The Transmit Statistics area contains the following fields:

- **Total Bytes (octets)** Displays the number of octets transmitted on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- Unicast Packets Displays the number of good Unicast packets transmitted on the interface since the device was last refreshed.
- **Multicast Packets** Displays the number of good Multicast packets transmitted on the interface since the device was last refreshed.
- **Broadcast Packets** Displays the number of good broadcast packets transmitted on the interface since the device was last refreshed.

#### **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:

 $\mathbf{h}$ 

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Etherlike Page

- Admin	Interface @ Port 191 V C LAG 1 V	Help
Bang System Can Admin Can Statistics Can Ethernet		Suppo
	Refresh Rate No Refresh	Guide
GVRP	Frame Check Sequence (FCS) Errors	Logou
EAP RMON	Single Collision Frames 0	
en Bridging		
e 💼 Routing e 💼 Security Suite	Excessive Collisions 0 Oversize Packets 0	
a 💼 Quality of Service		
	Internal MAC Receive Errors 0	
	Received Pause Frames 0	
	Transmitted Pause Frames 0	
	Clear Counters	

The Etherlike Page contains interface statistics. The Etherlike Page contains the following fields:

- Interface Indicates the device for which statistics are displayed. The possible field values are:
  - Port Defines the specific port for which Etherlike statistics are displayed.
  - LAG Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - 15 Sec Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - 30 Sec Indicates that the Etherlike statistics are refreshed every 30 seconds.
  - 60 Sec Indicates that the Etherlike statistics are refreshed every 60 seconds.
  - No Refresh Indicates that the Etherlike statistics are not refreshed.
- Frame Check Sequence (FCS) Errors Displays the number of FCS errors received on the selected interface.
- Single Collision Frames Displays the number of single collision frames received on the selected interface.
- Late Collisions Displays the number of late collision frames received on the selected interface.



- Excessive Collisions Displays the number of excessive collisions received on the selected interface.
- **Oversize Packets** Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- Internal MAC Receive Errors Displays the number of internal MAC received errors on the selected interface
- Receive Pause Frames Displays the number of received paused frames on the selected interface.
- **Transmitted Pause Frames** Displays the number of paused frames transmitted from the selected interface.

#### **Resetting Etherlike Statistics Counters**

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

#### **Viewing GVRP Statistics**

The GVRP Page contains device statistics for GVRP. To view GVRP statistics:

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

6

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **GVRP** Page LINKSYS SGE 2000 **GVRP** System Refresh Rate No Refresh 💌 Statistics Ethernet Guide Attribute (Counter) Received Transmitted Interface Join Empty Etherlike GVRP Empty EAP RMON Leave Empty Bridging Join In Becurity Suite Quality of Service Leave In Leave All GVRP Error Statistics Invalid Protocol ID Invalid Attribute Type Invalid Attribute Value Invalid Attribute Length Invalid Event Clear Counters

The *GVRP Page* contains device statistics for GVRP. The *GVRP Page* is divided into two areas, GVRP Statistics Table and GVRP Error Statistics Table.

The following fields are relevant for both tables:

- Interface—Specifies the interface type for which the statistics are displayed.
  - Port Indicates port statistics are displayed.
  - LAG Indicates LAG statistics are displayed.
- **Refresh Rate**—Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
  - 15 Sec Indicates that the GVRP statistics are refreshed every 15 seconds.
  - 30 Sec Indicates that the GVRP statistics are refreshed every 30 seconds.
  - 60 Sec Indicates that the GVRP statistics are refreshed every 60 seconds.
  - No Refresh Indicates that the GVRP statistics are not refreshed.

The GVRP Received Transmitted Table contains the following fields:

- Join Empty Displays the device GVRP Join Empty statistics.
- **Empty** Displays the device GVRP Empty statistics.

16

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Leave Empty Displays the device GVRP Leave Empty statistics.
- Join In Displays the device GVRP Join In statistics.
- Leave In Displays the device GVRP Leave in statistics.
- Leave All— Displays the device GVRP Leave all statistics.

The GVRP Error Statistics Table contains the following fields:

- Invalid Protocol ID Displays the device GVRP Invalid Protocol ID statistics.
- Invalid Attribute Type Displays the device GVRP Invalid Attribute ID statistics.
- Invalid Attribute Value Displays the device GVRP Invalid Attribute Value statistics.
- Invalid Attribute Length Displays the device GVRP Invalid Attribute Length statistics.
- Invalid Events Displays the device GVRP Invalid Events statistics.

#### **Resetting GVRP Statistics Counters**

- 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.

h

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### EAP Page LINKSYS SGE 2000 Help EAP 💼 System Support 1/g1 💌 Port en Statistics Refresh Rate No Refresh V Guide en Ethernet - 🗋 Interface - 🗋 Etherlike Logout Frames Receive 0 Frames Transmit 0 RMON Start Frames Receive e Bridging ia en Routing ia en Security Suite Log off Frames Receive **Respond ID Frames Receive** 🛓 💼 Quality of Service Respond Frames Receive Request ID Frames Transmit n Request Frames Transmit n Invalid Frames Receive 0 Length Error Frames Receive 0 0 Last Frame Version Last Frame Source 00:00:00:00:00:00

The *EAP Page* contains information about EAP packets received on a specific port. The EAP Page page contains the following fields:

- Unit Number Indicates the stacking member for which the EAP statistics are displayed.
- **Port** Indicates the port, which is polled for statistics.
- **Refresh Rate** Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - 15 Sec Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - 30 Sec Indicates that the Etherlike statistics are refreshed every 30 seconds.
  - 60 Sec Indicates that the Etherlike statistics are refreshed every 60 seconds.
  - No Refresh Indicates that the Etherlike statistics are not refreshed.
- Frames Receive Indicates the number of valid EAPOL frames received on the port.
- Frames Transmit Indicates the number of EAPOL frames transmitted via the port.
- Start Frames Receive Indicates the number of EAPOL Start frames received on the port.
- Log off Frames Receive Indicates the number of EAPOL Logoff frames that have been received on the port.



- **Respond Frames Receive** Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Request ID Frames Transmit** Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** Indicates the number of EAP Request frames transmitted via the port.
- Invalid Frames Receive Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- Length Error Frames Receive Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- Last Frame Version Indicates the protocol version number attached to the most recently received EAPOL frame.
- Last Frame Source Indicates the source MAC address attached to the most recently received EAPOL frame.

16

SFE2000/SFE2000P Gigabit Ethernet Switch Reference 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

16

## **Viewing RMON Statistics**

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device. To view the RMON statistics:

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

#### **RMON Statistics Page**

LINKSYS Andrien of Cisco Systems, Inc.			
SGE 2000	Statistics		Неір
💼 System 🍋 Admin	Interface	● Port 1/g1 ▼ C LAG 1 ▼	Suppor
Statistics	Refresh Rate	No Refresh 💌	Guide
	Received Bytes (Octets)	0	Logout
	Received Packets	0	
Alarms	Broadcast Packets Received	0	
Bridging Routing	Multicast Packets Received	0	
Security Suite	CRC & Align Errors	0	
Quality of Service	Undersize Packets	0	
	Oversize Packets	0	
	Fragments	0	
	Jabbers	0	
-	Collisions	0	
	Frames of 64 Bytes	0	
	Frames of 65 to 127 Bytes	0	_
	Frames of 128 to 255 Bytes	0	
	Frames of 256 to 511 Bytes	0	
)'	Eramoe of 512 to 1023 Rutoe		-

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device. The *RMON Viewing RMON Statistics* page contains the following fields:

- Interface Indicates the device for which statistics are displayed. The possible field values are:
  - Port Defines the specific port for which RMON statistics are displayed.
  - LAG Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - 15 Sec Indicates that the RMON statistics are refreshed every 15 seconds.
  - 30 Sec Indicates that the RMON statistics are refreshed every 30 seconds.
  - 60 Sec Indicates that the RMON statistics are refreshed every 60 seconds.
  - No Refresh Indicates that the RMON statistics are not refreshed.

Chapter 16:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Received Bytes (Octets)** Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- Multicast Packets Received Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- CRC & Align Errors Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- Undersize Packets Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- Jabbers Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- Collisions Displays the number of collisions received on the interface since the device was last refreshed.
- Frames of xx Bytes Number of xx-byte frames received on the interface since the device was last refreshed.
- 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.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

# 16

# **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 Diviser of Caso System, Bo		
SGE 2000 System Admin Statistics History Vertes Aarms Satistics History Aarms Satistics Bardyng Scurty Suite Securty Suite Securty Suite	History       Source       Sampling       Current Number       Owner         I       1/g1       1800       50       50       Adam       Edit         History Table       Delete       Ada	Help Support Guide Logout
		Cost 3 THE

**RMON History Control Page** 

The RMON History Control Page contains the following fields:

- History Entry No. Number automatically assigned to the table entry number.
- Source Interface Displays the interface from which the history samples were taken. The possible field values are:
  - Port Specifies the port from which the RMON information was taken.
  - LAG Specifies the port from which the RMON information was taken.

Chapter 16:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Sampling Interval** Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- Sampling Requested Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- Current Number of Samples Displays the current number of samples taken.
- Owner Displays the RMON station or user that requested the RMON information. The field
  range is 0-20 characters.
- 3. Click the Add button. The Add RMON History Page opens:

SGE 2000		LINKSYS A Under of Dece Systems, Inc.
	Add RMON History	
New History Entry	1	
Source Interface	💿 Port 1/g1 🔽 🔿 LAG 1 🗾	
Owner		
Max No. of Samples to Keep	50	
Sampling Interval	1800	
	Apply	

#### Add RMON History Page

The Add RMON History Page contains the following fields:

- New History Entry Number automatically assigned to the table entry number.
- Source Interface Displays the interface from which the history samples were taken. The possible field values are:
  - Port Specifies the port from which the RMON information was taken.
  - LAG Specifies the port from which the RMON information was taken.
- Owner Displays the RMON station or user that requested the RMON information. The field
  range is 0-20 characters.
- Max No. of Samples to Keep Indicates the number of samples to save.
- **Sampling Interval** Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- 4. Define the relevant fields.
- 5. Click Apply. The entry is added to the RMON History Control Page, and the device is updated.

16

Modify History Control Settings

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

#### History Control Settings Page

SGE 2000		LINKSYS
Hi	story Control Settings	
History Entry No.	1 -	
Source Interface	⊙ Port 1/g1 🔽 C LAG 1 🔽	
Owner	Adam	
Max No. of Samples to Keep	50	
Sampling Interval	1800	
	Apply	

The History Control Settings Page contains the following fields:

- History Entry Number Displays the entry number for the History Control Table page.
- Source Interface Displays the interface from which the history samples were taken. The possible field values are:
  - Port Specifies the port from which the RMON information was taken.
  - LAG Specifies the port from which the RMON information was taken.
- **Owner** Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- Max No. of Samples to Keep Indicates the number of samples to save.
- **Sampling Interval** Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- 3. Define the relevant fields.
- 4. Click Apply. The history control settings are defined, and the device is updated.

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Viewing the RMON History Table

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

**RMON History Table Page** 

SFE 2000	Histo	<b>ry</b> Entry No.	T								Help Support
Construction     Construction	No.	e Drop Events ce Table	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragment	Guide
										Þ	

The RMON History Table Page contains the following fields:

- History Entry No. Displays the entry number for the History Control Table page.
- **Owner** Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- Sample No. Indicates the sample number from which the statistics were taken.
- **Drop Events** Indicates the number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number dropped packets, but rather the number of times dropped packets were detected.
- **Received Bytes (Octets)** Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** Displays the number of good Multicast packets received on the interface since the device was last refreshed.



- **CRC Align Errors** Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- Undersize Packets Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- Jabbers Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- Collisions Displays the number of collisions received on the interface since the device was last refreshed.
- Utilization Displays the percentage of the interface utilized.

## **Configuring RMON Events**

This section includes the following topics:

- Defining RMON Events Control
- Viewing the RMON Events Logs

#### **Defining RMON Events Control**

The RMON Events Page contains fields for defining RMON events. To view RMON events:

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

 $\mathbf{b}$ 

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **RMON Events Page**

SGE 2000	Events	Help
💼 System 💼 Admin	Event Entry Community Description Type Time Owner	Support
en Statistics	Delete	Guide
- <del>C</del> RMON	Events Log	Logout
Bridging		
Routing Security Suite Quality of Service		
Quality of Service		

The *RMON Events Page* contains fields for defining RMON events. The *RMON RMON Events Page* page contains the following fields:

- Event Entry Displays the event.
- **Community** Displays the community to which the event belongs.
- **Description** Displays the user-defined event description.
- **Type** Describes the event type. Possible values are:
  - None Indicates that no event occurred.
  - Log —Indicates that the event is a log entry.
  - Trap Indicates that the event is a trap.
  - Log and Trap Indicates that the event is both a log entry and a trap.
- Time Displays the time that the event occurred.
- **Owner** Displays the device or user that defined the event.

The Add to List button adds the configured RMON event to the Event Table at the bottom of the page.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### Add RMON Events Page

SGE 200	00	LINKSYS A Divider of Disco Pystema, Inc.
	Add RMON Events	
Event Entry	2	
Community	Default Community	
Description	Default Description	
Туре	None	
Owner		
	Apply	

The Add RMON Events Page contains the following fields:

- Event Entry Displays the event.
- **Community** Displays the community to which the event belongs.
- **Description** Displays the user-defined event description.
- **Type** Describes the event type. Possible values are:
  - None Indicates that no event occurred.
  - Log —Indicates that the event is a log entry.
  - Trap Indicates that the event is a trap.
  - Log and Trap Indicates that the event is both a log entry and a trap.
- **Owner** Displays the device or user that defined the event.
- 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 Modify Event Control Settings Page opens:

I

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

SGE 2000		LINKSYS A Diselect of Data Systems, Inc.
	Event Control Settings	
Event Entry No.	1	
Community	Default Community	
Description	Default Description	
Туре	None	
Owner		
	Apply	

#### Modify Event Control Settings Page

The Modify Event Control Settings Page contains the following fields:

- Event Entry Displays the event.
- **Community** Displays the community to which the event belongs.
- **Description** Displays the user-defined event description.
- **Type** Describes the event type. Possible values are:
  - None --- Indicates that no event occurred.
  - Log —Indicates that the event is a log entry.
  - Trap Indicates that the event is a trap.
  - Log and Trap Indicates that the event is both a log entry and a trap.
- **Owner** Displays the device or user that defined the event.
- 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 page contains fields for defining RMON events.

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



#### **Events** Page

LINKSYS A Division of Cisco Systems, Inc.		
SFE 2000	Events Event Log No. Log Time Description	Help
System     Statistics     Statistics     Ethement     RMON     Statistics     History     History     Airms     Statistics	Event Log No. Log Time Description	Support Guide Logout
⊕		

The Events Page contains the following fields:

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

#### **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:

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

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### **RMON** Alarms Page

SGE 2000	Ala	arms								ſ	Help
System		Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	F	Suppor
		1	Total Bytes (Octets)- Receive	1/g1	0	Absolute	100	1 - Default Description	20	1	Guide

The RMON Alarms Page contains the following fields:

- Alarm Entry Indicates a specific alarm.
- Counter Name Displays the selected MIB variable.
- Interface Displays the interface for which RMON statistics are displayed. The possible field v values are:
  - Port Displays the RMON statistics for the selected port.
  - LAG Displays the RMON statistics for the selected LAG.
- Counter Value Displays the current counter value for the particular alarm.
- Sample Type Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - Delta Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - Absolute Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.



- **Rising Event** Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the RMON Events page.
- **Falling Threshold** Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the RMON Events page.
- **Startup Alarm** Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
- Interval Defines the alarm interval time in seconds.
- **Owner** Displays the device or user that defined the alarm.
- 2. Click the Add button. The Add RMON Alarm Page opens:

#### Add RMON Alarm Page

SGE 2000		LINKSYS
	Add RMON Alarm	
Alarm Entry	2	
Interface	© Port 1/g1 💌 🔿 LAG 1 🔽	
Counter Name	Total Bytes (Octets)- Receive 💌	
Sample Type	Absolute -	
<b>Rising Threshold</b>	100	
<b>Rising Event</b>	1 - Default Description 💌	
Falling Threshold	20	
Falling Event	1 - Default Description 💌	
Startup Alarm	Rising and Falling 💌	
Interval	100	
Owner		
	Apply	

The Add RMON Alarm Page contains the following fields:

- Alarm Entry Indicates a specific alarm.
- Interface Displays the interface for which RMON statistics are displayed. The possible field v values are:
  - Port Displays the RMON statistics for the selected port.
  - LAG Displays the RMON statistics for the selected LAG.
- Counter Name Displays the selected MIB variable.

Chapter 16:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



- **Sample Type** Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - *Delta* Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - *Absolute* Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the RMON Events page.
- **Falling Threshold** Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the RMON Events page.
- **Startup Alarm** Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
- Interval Defines the alarm interval time in seconds.
- **Owner** Displays the device or user that defined the alarm.
- 3. Define the relevant fields.
- 4. Click Apply. The RMON alarm is added, and the device is updated.

#### 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 2000P		LINKSYS A Unider of Data Systems, Inc.
	Edit RMON Alarm	
Alarm Entry	1 -	
Interface	🔿 Port 💌 @ LAG 💌	
Counter Name	Total Bytes (Octets)- Receive	
Counter Value		
Sample Type	Absolute -	
<b>Rising Threshold</b>		
<b>Rising Event</b>	1 - Default Description 💌	
Falling Threshold		
Falling Event	•	
Startup Alarm	Rising Alarm	
Interval (Sec)		
Owner		
	Apply	
	Арріу	

The Edit RMON Alarms Page contains the following fields:

- Alarm Entry Indicates a specific alarm.
- Interface Displays the interface for which RMON statistics are displayed. The possible field v values are:
  - Port Displays the RMON statistics for the selected port.
  - LAG Displays the RMON statistics for the selected LAG.
- Counter Name Displays the selected MIB variable.
- **Counter Value** Displays the current counter value for the particular alarm.
- Sample Type Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - Delta Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - Absolute Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the RMON Events page.

Chapter 16:

16

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Falling Threshold** Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the RMON Events page.
- **Startup Alarm** Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
- Interval Defines the alarm interval time in seconds.
- **Owner** Displays the device or user that defined the alarm
- 3. Define the relevant fields.
- 4. Click Apply. The RMON alarms are modified, and the device is updated.

# **Managing Device Diagnostics**

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

- Viewing Integrated Cable Tests
- Performing Optical Tests
- Configuring Port Mirroring
- 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 120 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:

LINKSYS Division of Class Systems, Inc.		
SFE 2000P	Copper Ports Unit Number II	Help Support
Logs	Port Test Result Cable Fault Distance Last Update Cable Length 1/e1 Test	Guide
Copper Ports	1/c2 Test	Logout
Port Mirroring CPU Utilization	1/e3	
💼 Statistics 💼 Bridging	1/e4 Test	
en Routing Security Suite	1/e5 Test	
Quality of Service	1/e6 Test	
	1/e7 Test	
	1/e8 Test	
	1/e9 Test	
	1/e10 Test	
	1/e11 Test	
	1/e12 Test	

**Copper Ports Page** 

The Copper Ports Page contains the following fields:

• Unit No. — Indicates the unit number on which the tests are performed.

Chapter 17:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- **Port** Specifies port to which the cable is connected.
- Test Result Displays the cable test results. Possible values are:
  - No Cable Indicates that a cable is not connected to the port.
  - Open Cable Indicates that a cable is connected on only one side.
  - Short Cable Indicates that a short has occurred in the cable.
  - OK Indicates that a cable passed the test.
- Cable Fault Distance Indicates the distance from the port where the cable error occurred.
- Last Update Indicates the last time the port was tested.
- **Cable Length** Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.
- 2. Click the Advanced button. The Copper Cable Extended Feature Page opens:

#### Copper Cable Extended Feature Page

SFE 200	OP							LINKSYS
		C	opper C	able	Exte	nded F	eature	
Cable Status	Bad Ca	ble						
Speed	1000 M	B/s						
Link Status	Up							
Pair Distance	e to Fault	Status	Cable Length	Channel	Polarity	Pair Skew		
1-2			78M	в	Normal	8 ns		
3-6			73M	А	Normal	8 ns		
4-5			75M	D	Normal	8 ns		
7-8			75M	с	Normal	0 ns		
						Done		
						Done		

The Copper Cable Extended Feature Page contains the following fields.

- Cable Status Displays the cable status.
- Speed Indicates the speed at which the cable is transmitting packets.
- Link Status Displays the current link status.
- **Pair** The pair of cables under test.
- Distance to Fault Indicates the distance from the port where the cable error occurred.
- Status Displays the cable status.

- Cable length Displays the cable length.
- Channel Displays the cable's channel.
- **Polarity** Automatic polarity detection and correction permits on all RJ-45 ports for automatic adjustment of wiring errors.
- **Pair Skew** Reaction or transmission time in nanoseconds for the selected cable pair and given cable length.
- 3. Define the relevant fields.
- 4. Click Apply. The advanced copper cable settings are defined, and the device is updated.

#### **Performing Optical Tests**

The *Optical Test Page* allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present. During the port test, the port moves to a down state.

**Optical Test Page** 

SFE 200P   System   File Management   Dignostice   Dignostice   Optical Test   On Mirrongo   Statistice   Dignostice   Statistice   Dignostice   Optical Test   On Mirrongo   Statistice   Pouling Statistice Ouling of Senice Image description of Senice	LINKSYS A Diesen of Claus Systems, No.		
	System     Admin     File Management     Ogper Ports     Opper Ports     Optical Test     Optical Test	Unit Number 1 💌	Support

The Optical Test Page contains the following fields:

- **Port** Displays the port IP address on which the cable is tested.
- **Temperature** Displays the temperature (C) at which the cable is operating.
- Voltage Displays the voltage at which the cable is operating.

Chapter 17:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

- Current Displays the current at which the cable is operating.
- **Output Power** Indicates the rate at which the output power is transmitted.
- Input Power Indicates the rate at which the input power is transmitted.
- Transmitter Fault Indicates if a fault occurred during transmission.
- Loss of Signal Indicates if a signal loss occurred in the cable.
- Data Ready Indicates the data status.

## **Configuring Port Mirroring**

Configuring 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 Configuring Port Mirroring Page opens:

LINKSYS A Diador of Choic Systems, Inc.		
SFE 2000P	Port Mirroring Destination Port Ive Source Port Type Status 1/e1 TxOnly NatReady Edit Delete Add	Help Support Guide Logout

#### **Configuring Port Mirroring Page**

The Configuring Port Mirroring Page contains the following fields:

• Source Port — Defines the port from which traffic is mirrored.

- **Destination Port** Defines the port to which traffic is mirrored.
- **Type** Indicates the port mode configuration for port mirroring. The possible field values are:
  - *RxOnly* Defines the port mirroring on receiving ports. This is the default value.
  - *TxOnly* Defines the port mirroring on transmitting ports.
  - Tx and Rx— Defines the port mirroring on both receiving and transmitting ports.
- Status Indicates if the port is currently monitored. The possible field values are:
  - Active Indicates the port is currently monitored.
  - notReady Indicates the port is not currently monitored.
- 2. Click the Add button. The Add Port Mirroring Page opens:

#### Add Port Mirroring Page

SFE 200	0P		LINKSYS A Dialize of Dice Tystems, Inc.
		Add Port Mirror	ing
Source Port	•		
Туре	Tx Only 💌		
	Apply		

The Add Port Mirroring Page contains the following fields:

- Source Port Defines the port to which traffic is mirrored.
- **Type** Indicates the port mode configuration for port mirroring. The possible field values are:
  - *RxOnly* Defines the port mirroring on receiving ports. This is the default value.
  - *TxOnly* Defines the port mirroring on transmitting ports.
  - *Tx and Rx* Defines the port mirroring on both receiving and transmitting ports.
- 3. Define the relevant fields.
- 4. Click Apply. Port mirroring is added, and the device is updated.

#### Modifying Port Mirroring

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

Chapter 17:

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

#### Edit Port Mirroring Page

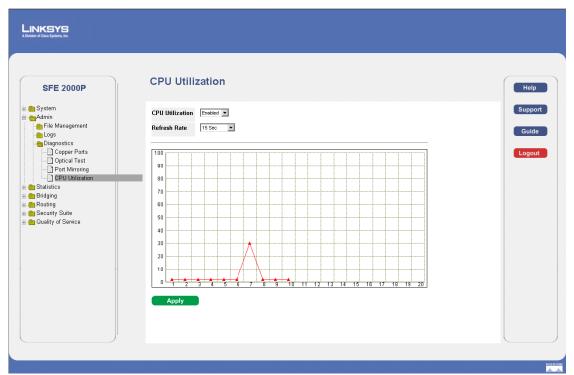
LINKSYS A Dividior of Data Systems, Inc.		SFE 2000P
	Edit Port Mirroring	
		Source Port 1/e1
		Type Tx Only
	)	Apply
	)	

The Edit Port Mirroring Page contains the following fields:

- Source Port Defines the port to which traffic is mirrored.
- Type Indicates the port mode configuration for port mirroring. The possible field values are:
  - RxOnly Defines the port mirroring on receiving ports. This is the default value.
  - *TxOnly* Defines the port mirroring on transmitting ports.
  - *Tx and Rx* Defines the port mirroring on both receiving and transmitting ports.
- 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.



**CPU Utilization Page** 

The CPU Utilization Page contains the following fields:

- CPU Utilization Displays CPU resource utilization information. The possible field values are:
  - Enabled Enables viewing CPU utilization information. This is the default value.
  - Disabled Disables viewing the CPU utilization information.
- Refresh Rate Amount of time that passes before the statistics are refreshed.
- Usage Percentages Indicates the percentage of the CPU's resources consumed by the device.
- Time Indicates the time, in 15 second intervals, the usage samples are taken.

17

Chapter

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide



# **Linksys One Contact Information**

Need to contact Linksys One?

Visit us online for information on the latest products and updates to your existing products at:

http://www.linksys.com/international

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Czech Republic	support.cz@linksys.com
Denmark	support.dk@linksys.com
Finland	support.fi@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Greece	support.gr@linksys.com (English only)
Hungary	support.hu@linksys.com
Ireland	support.ie@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Poland	support.pl@linksys.com
Portugal	support.pt@linksys.com
Russia	support.ru@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com

Chapter A:

# Appendix

A

SFE2000/SFE2000P Gigabit Ethernet Switch Reference Guide

In Europe	E-mail Address
United Kingdom	support.uk@linksys.com
	T
Outside of Europe	E-mail Address
Asia Pacific	asiasupport@linksys.com (English only)
Latin America	support.portuguese@linksys.com or support.spanish@linksys.com
Middle East & Africa	support.mea@linksys.com (English only)
South Africa	support.ze@linksys.com (English only)
UAE	support.ae@linksys.com (English only)
U.S. and Canada	support@linksys.com

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com