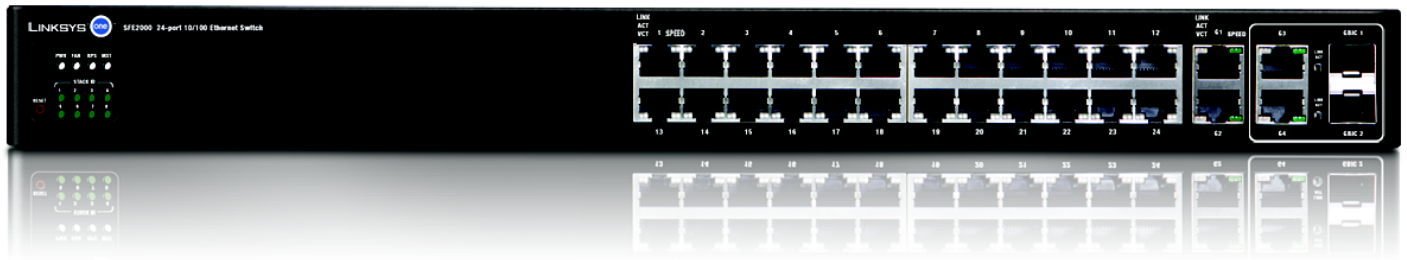
LINKSYS®
A Division of Cisco Systems, Inc.



Release 1.0

Linksys SFE2000/SFE2000P Fast Ethernet Switch Administration Guide

CISCO SYSTEMS

Contents

Chapter 1

Introduction

Welcome

Thank you for choosing a Linksys Ethernet switch. This Ethernet switch allows you to quickly and easily expand your Linksys One system. It delivers non-blocking, wire speed switching for your network clients, plus multiple options for connecting to your network backbone. Twenty four ports wire up your workstations or connect to other Linksys switches or devices. LED indicators provide power, link, and activity status.

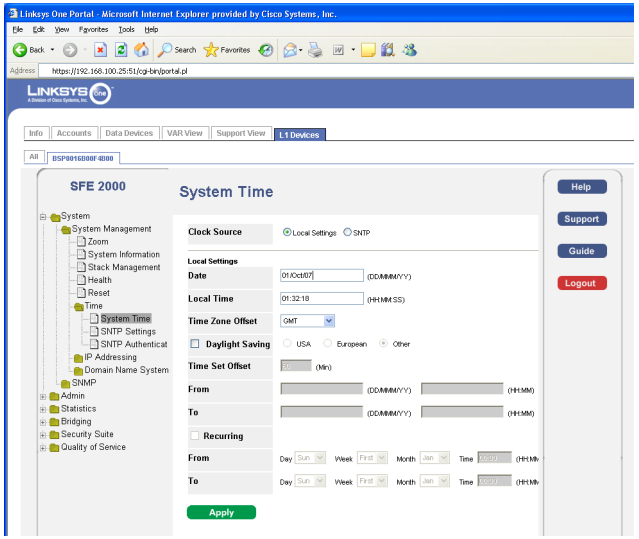
The Ethernet switch features monitoring and configuration via the Linksys One Portal, your web browser, or the console interface. If your Ethernet switch is part of a Linksys One system, the easiest way to manage it is with the Linksys One Portal — available only on the Linksys One Services Router. Refer to the *Linksys One Customer Premises Equipment Administration Guide* for more details on the Linksys One Portal.

The Ethernet switch supports numerous security features including the Remote Authorization and Authentication (RADIUS) and Terminal Access Controller Access Control System (TACACS+) protocols. With Simple Network Time Protocol (SNTP), the Ethernet switch can synchronize its clock with a time server available on one of its attached networks.

The system is fully manageable using a combination of a database of MIB (Management Information Base) variables, whose combined values represent all facets of the system state, and the Simple Network Management Protocol (SNMP) protocol.

The "P" model of the Ethernet switch supports Power over Ethernet (PoE) which eliminates the need to run 110/220 VAC power to wireless network, IP telephony, or other PoE powered devices on the Linksys network. Use of a PoE system allows greater flexibility in locations of network devices, and significantly decreasing installation costs. The entire PoE system can be centrally powered by uninterruptible power supplies if necessary.

Linksys One Portal



What's in this User Guide?

This user guide covers the steps for setting up and using the Ethernet switch. Use the instructions in this guide to help you connect the switch, set it up, and configure it to your Linksys network. These instructions should be all you need to get the most out of your Ethernet switch.

This user guide contains the following chapters:

Chapter 1, "Introduction"

This chapter describes the Ethernet switch applications and provides an overview of the content of this administration guide.

Chapter 2, "Getting to Know the Switch"

This chapter describes the physical features of the Ethernet switch.

Chapter 3, "Connecting the Switch"

This chapter explains how to install and connect the Ethernet switch.

Chapter 4, "Console Configuration"

This chapter describes how to use the console interface when you configure the Ethernet switch.

Chapter 5, "Web Utility Configuration"

This chapter shows you how to configure the Ethernet switch using the Web-based Utility.

Chapter 2

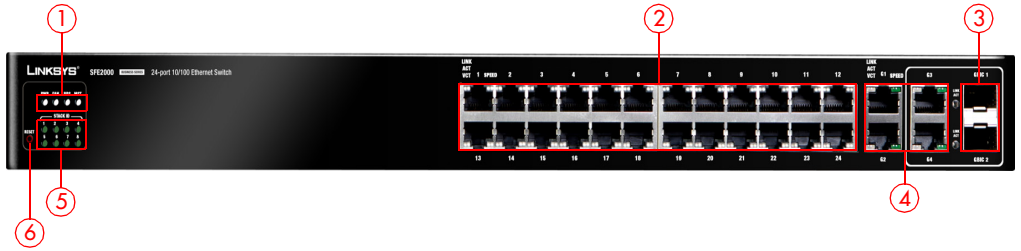
Getting to Know the Switch

Overview

The SFE2000 and SFE2000P models are 24-port, layer-2 Ethernet switches that expand the capability of the Linksys system. These two versions are functionally identical except the SFE2000P model offers Power-over-Ethernet (PoE) which can be used to supply power to various Linksys products over Ethernet cable.

The Front Panel

The Switch's LEDs and Ethernet ports are located on the front panel.



1	**System Status LEDs**. Four LEDs indicate the status of the Ethernet switch power, fan, RPS connectivity, and stack master. For more details, refer to "System Status LEDs," on page 4.
2	**LAN Ports**. Twenty four 10/100 BaseT LAN ports provide connectivity to other Linksys devices. For more details, refer to "LAN Ports," on page 5.
3	**Gigabit Interface Converter (mini-GBIC) Uplink Ports**. Two mini-GBIC ports provide uplink ports which support network speeds of 10Mbps, 100Mbps, and 1000Mbps. For more details, refer to "Uplink Ports," on page 6.
4	**Uplink Ports**. Four 10/100/1000 Uplink ports. Ports G3 and G4 are shared with ports mini-GBIC 1 and mini-GBIC 2 respectively. These ports can also be used for stacking multiple units. For more details, refer to "Uplink Ports," on page 6.
5	**Stack ID**. If stacking is active, indicates the ID number of the stack. For more details, refer to "Stack ID LEDs," on page 5.
6	**RESET Switch**. Resets the SFE2000/SFE2000P Ethernet switch. For more details, refer to "Reset Switch," on page 5.

Front Panel LEDs

The Switch uses Light Emitting Diodes (LEDs) to indicate the status of numerous functions. These functions are listed below.

System Status LEDs

PWR	A green PWR LED lights to indicate that the Ethernet switch is powered by internal power supplies. If the Ethernet switch is powered by a remote power supply (RPS), this LED blinks red.
FAN	A green FAN LED lights to indicate that the cooling fan is operating properly. A blinking red FAN LED indicates that the cooling fan has failed.
RPS	A green RPS LED lights to indicate that RPS is connected and operating properly. A blinking red RPS LED indicates an RPS fault.
MST	A green MST LED indicates that this Ethernet switch is a stack master.

LAN Port LEDs

Act/Link	The green Act/Link LEDs light to indicate a functional network link through the corresponding port with an attached device. The Act (Activity) LEDs flash to indicate that the Ethernet switch is actively sending or receiving data over that port. • On the SFE2000, a green Link LED indicates that the port is linked to a 10/100Mbps device. • On the SFE2000P, a green Link LED indicates that PoE is active on that port.

Uplink Port LEDs

Act/Link	The green Act/Link LEDs light to indicate a functional network link through the corresponding port with an attached device. The Act (Activity) LEDs flash to indicate that the Ethernet switch is actively sending or receiving data over that port.
Gigabit	The Gigabit LED lights indicate a Gigabit connection on the corresponding port.

Stack ID LEDs

Stack ID	A green Stack ID LED indicates that this Switch is stacked and the corresponding number indicates its stack ID. Range is 1 to 8.

Reset Switch

The Ethernet switch can be reset by inserting a pin or paper clip into the RESET opening. If the reset switch is held for 10 seconds or longer, the Ethernet switch will be reset to its default settings.

CAUTION: All user-defined settings are lost when you hold the Reset button for 10 seconds or longer; the Ethernet switch reverts to its default settings.

When a unit is reset to its default setting, the unit restarts in stackable mode using default stacking ports with autonumbering enabled. Pressing the reset button on the master unit of a stack resets all units in the stack.

LAN Ports

The Ethernet switch is equipped with 24 Ethernet ports.

1-24	The Switch is equipped with 24 auto-sensing, Ethernet (IEEE 802.3) network ports, which use RJ-45 connectors. The Fast Ethernet ports support network speeds of 10Mbps or 100Mbps. They can operate in half and full-duplex modes. Auto-sensing technology enables each port to automatically detect the speed of the device connected to it, and adjust its speed and duplex accordingly.

Uplink Ports

The Switch is equipped with 4 uplink ports and 2 mini-GBIC uplink ports.

G1-G4	Ports G1-G4 are Ethernet (IEEE 802.3ab) uplink ports which support network speeds of 10Mbps, 100Mbps, and 1000Mbps. Ports G3 and G4 are shared with GBIC1 and GBIC2 ports, respectively. If shared ports pairs are both connected, then the mini-GBIC port takes priority. In stacking mode, two ports are used for stacking. Use only ports G1/G2 for stacking. In standalone mode, all four ports can be used as uplinks.
GBIC1/2	The Switch provides two mini-GBIC ports. The mini-GBIC port is a connection point for a mini-GBIC expansion module, so the Switch can be uplinked via fiber or copper to another switch. Each mini-GBIC port provides a link to a high-speed network segment or individual workstation at speeds of up to 1000Mbps. Use the Linksys MGBT1, MGBSX1, or MGBLH1 mini-GBIC modules with the Switch. The MGBSX1 and the MGBLH1 require fiber cabling with LC connectors, while the MGBT1 requires a Category 5e Ethernet cable with an RJ-45 connector.

The Back Panel

The power port is located on the back panel of the Ethernet switch.

1	**Power Port**. The Power port is where you will connect the power cord. For more details, refer to "Power Port," on page 7.
2	**Console Port**. The Console port is where you can connect a serial cable to a PC's serial port for configuration. For more details, refer to "Console Port," on page 7.
3	**RPS Port**. Redundant Power Supply (RPS) port. For more details, refer to "RPS Port," on page 7.

Power Port

The 100-240 VAC power cord is connected to the Power port.

CAUTION: Only use the power cord that is supplied with the Ethernet switch. The unit may be damaged if the incorrect power cord is used.

Console Port

The Console port is where you connect a serial cable to a PC's serial port for configuration using your PC's HyperTerminal program. Refer to "Configuring the HyperTerminal Application," on page 33 for more information.

NOTE: Many modern laptop computers are not supplied with serial ports. You may use a USB-to-Serial adapter on your laptop to connect to the console serial port.

RPS Port

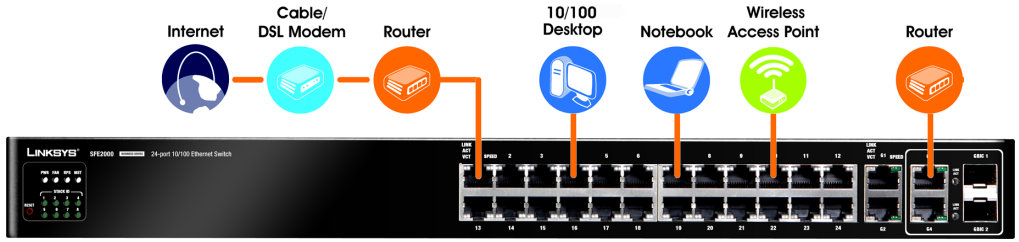
An optional Redundant Power Supply (RPS) is connected to the RPS port. An RPS enhances the reliability of the Ethernet switch and it can keep the unit running if a power failure occurs. Only use a Linksys RPS1000 Redundant Power Supply unit and a proper RPS cable (RPSCBL1) with the Ethernet switch.

WARNING: Do not remove the cover from the RPS port unless an RPS unit is connected to the Ethernet switch. Keep the RPS port covered when not in use.

Connecting the Switch

Overview

This chapter will explain how to connect network devices to the Ethernet switch. For an example of a possible network configuration, see the application diagrams shown below.



Before You Install the Switch...

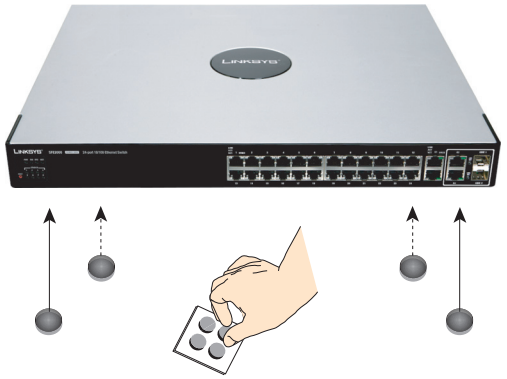
When you choose a location for the Ethernet switch, observe the following guidelines:

- Make sure that the Ethernet switch will be accessible and that the cables can be easily connected.
- Keep cabling away from sources of electrical noise, power lines, and fluorescent lighting fixtures.
- Position the Ethernet switch away from water and moisture sources.
- To ensure adequate air flow, be sure to provide a minimum clearance of two inches (50 mm) around the air intake and exhaust ports on the sides of the Ethernet switch.
- Do not stack free-standing Ethernet switches more than four units high. The stacking configuration, described in "Stacking Multiple Switches," on page 12, allows up to eight units to be logically stacked together. It is recommended that multiple Ethernet switches be mounted in a rack when installed in this manner. Ethernet switches can be physically placed at different locations; they do not have to be stacked at the same location.

Chapter 3

Placement Options

Before connecting cables to the Ethernet switch, first you will physically install the Ethernet switch. Either set the Ethernet switch on its four rubber feet for desktop placement, mount it in a standard-sized, 19-inch wide for rack-mount placement, or mount it on a wall with the wall-mount brackets provided.



NOTE: The four supplied mounting brackets can be used for either wall mount or rack mount installations.

Desktop Placement

1. Attach the rubber feet to the recessed areas on the bottom of the Ethernet switch.
2. Place the Ethernet switch on a desktop near an AC power source.

CAUTION: Keep enough ventilation space for the Ethernet switch so it does not exceed the environmental restrictions mentioned in the specifications.

Rack-Mount Placement

To mount the Ethernet switch in any standard-sized, 19-inch wide, (each Ethernet switch requires 1RU of space in the rack), follow these instructions:

1. Remove the four front screws on one side of the Ethernet switch. Retain the screws for re-installation.
2. Place one of the supplied spacers on the side of the Ethernet switch so the four holes align to the screw holes.
3. Place a rack mount bracket next to the spacer and reinstall the four screws (removed in step 1).

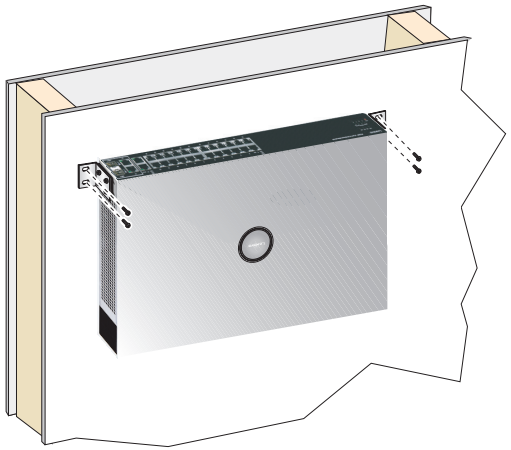
4. Repeat steps 2 through 3 for the other side of the Ethernet switch.
5. Attach the Ethernet switch to the rack using the supplied screws.

Wall-Mount Placement

1. On one of the side corners, remove the four front screws on of the Ethernet switch. Retain the screws for re-installation.

NOTE: The Ethernet switch, shown below, is mounted with the ports located on top. When the switch is mounted to a wall, the ports can be oriented in any direction.

2. Place one of the supplied spacers on the side of the Ethernet switch so the four holes align to the screw holes.
3. Place a rack mount bracket next to the spacer and reinstall the four screws (removed in step 1). The wall mount brackets should point towards the bottom of the Ethernet switch.
4. Repeat steps 1 through 3 for the other corners of the Ethernet switch.
5. Attach the Ethernet switch to a wall with appropriate screws (not supplied).



CAUTION: Ensure that the Ethernet switch is securely attached to the wall.

Connecting the Cables

To connect network devices to the Ethernet switch, follow these instructions:

1. For 10/100Mbps devices, connect a Category 5 Ethernet network cable to one of the numbered ports on the Ethernet switch. For a 1000Mbps device, connect a Category 5e Ethernet network cable to one of the uplink ports on the Ethernet switch.
2. Connect the other end to a PC or other network device.

NOTE: If connecting an Ethernet switch to an SVR3000 router, connect it to a Cascade port on the SVR3000.

3. Repeat steps 2 and 3 to connect additional devices.
4. If you are using the mini-GBIC port, then insert the mini-GBIC module to the mini-GBIC port. For detailed instructions, refer to the documentation supplied with the mini-GBIC module.

CAUTION: Observe the orientation of the mini-GBIC module before inserting it into a mini-GBIC port. The bottom mini-GBIC ports are upside down in relation to the top mini-GBIC ports.

5. If you use the console interface to configure the Ethernet switch, then connect the supplied serial cable to the console port (located on the back of the Ethernet switch), and tighten the captive retaining screws. Connect the other end to your PC's serial port. (The PC must be running VT100 terminal emulation software, such as HyperTerminal.)
6. Connect the supplied power cord to the power port, and plug the other end into an electrical outlet.

CAUTION: Make sure you use the power cord that is supplied with the Ethernet switch. Use of a different power cord could damage the Ethernet switch.

7. Power on the network devices connected to the Ethernet switch. Each active port's corresponding Act/Link LED will light up on the Ethernet switch. If a port has an active Gigabit connection, then its corresponding Gigabit LED will also light up.

If you will use the console interface to configure the Ethernet switch, proceed to "Console Configuration" section on page 33 for directions.

If you use the Web-based Utility to configure the Ethernet switch, proceed to "Web Utility Configuration" section on page 50.

Stacking Multiple Switches

The Stacking configuration provides multiple switch management through a single point as if all stack master and stack members were a single Ethernet switch. All stack masters are accessed through a single IP address through which the stack is managed. The stack can be managed from the web-based interface or the console interface.

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.

Switch software is downloaded separately for each stack member. However, all units in the stack must be running the same software version.

A stack unit can operate in one of the following modes:

- Stand-alone — 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 that is not connected to any other units may operate as a "stack–of-one."

The Stack Master unit manages the stack and is responsible for the configuration. The Master Backup Runs as a slave unit and monitors the operation of the stack master. A stack member runs a slave version of the switching algorithm, which allows the applications running on the master unit to control the resources of the member unit.

Stacking Highlights

- In stacking mode, each Ethernet switch is given a unique ID, from 1 to 8.
- Stack IDs 1 and 2 are Master-Enabled units.
- All Ethernet switches in the stack must run the same version of software.
- The Stack Master switch maintains the configuration.
- Stack cannot combine Linksys SFE2000 and SGE2000 family Ethernet switches.
- By factory default, Ethernet switches boot in stacking mode.
- Stack ID can be user assigned or automatically assigned.
- Stacking ports are available to user in standalone mode as regular network ports.
- Settings are applied only to the master unit; certain changes take place only after reset.

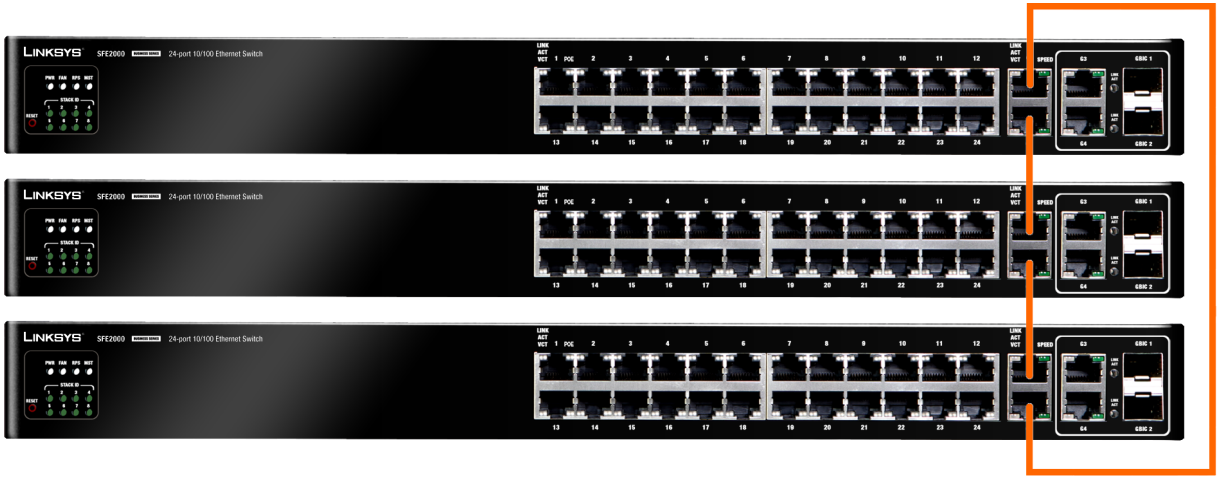
By default, the Ethernet switch is in stacking mode. Using the console interface or the web interface, you can change the mode to standalone mode.

TIP: Power the Ethernet switches in the order that you want them in the Stack ID. The first powered Ethernet switch in a stack is assigned as the Master Unit, the next powered unit is assigned as the Master-Backup. The remaining units are assigned Stack IDs in the order that they are powered.

When the device is in standalone mode, the stacking ports can be used as regular ports.

Connecting Cabling for Stacking

When the Ethernet switch is in stacking mode, ports G1 – G2 (copper Gigabit Ethernet ports) are reserved as stacking ports and cannot be used as network ports. In this case, either fiber or copper ports can be used for stacking.



Managing Stacks

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.

8. Connect the units physically through the stacking ports, using standard Ethernet cables.
9. 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 manually-assigned IDs in your network can impact system performance.

5. 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.

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.

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.

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

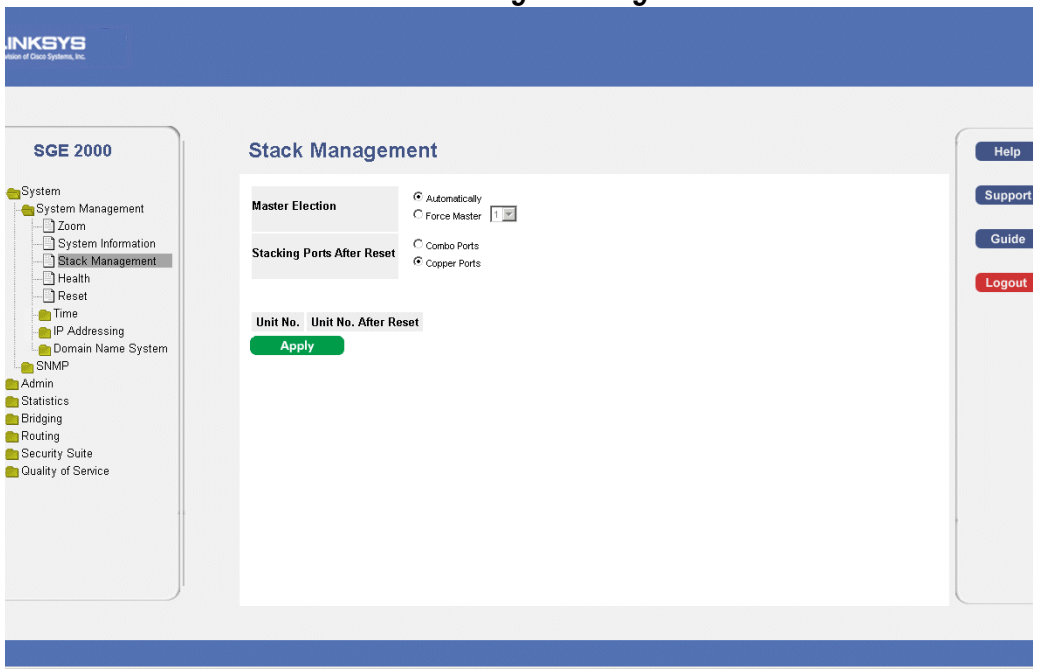
Stack Management

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:*

Stack Management Page



The *Stack Management Page* contains the following fields:

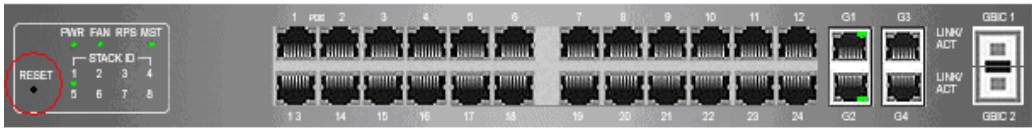
- **Master Election** — Indicates the method of electing the Stack Master device. The possible values are:
    - *Automatically* — The master is selected automatically by software.
    - *Force Master* — The unit is forced to be master of the stack. Note that only units with the Unit ID of 1 or 2 can 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.

Resetting the Unit to Factory Default Mode

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



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 *n*.
	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.

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.
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.

NOTE: 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.

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.

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.

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.

Inserting a Standalone Unit into a Running Stack

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.

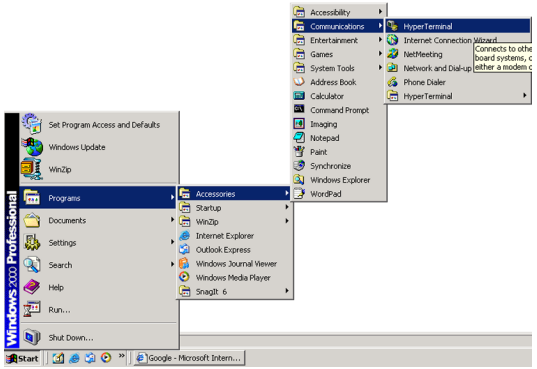
Chapter 4

Console Configuration

Overview

The Ethernet switch features a menu-based console interface for basic configuration of the Ethernet switch and management of your network. The Ethernet switch can be configured using a menu-based interface through the console port or through a telnet connection. This chapter describes console interface configuration. Configuration can also be performed through the web utility, which is covered in the next chapter.

NOTE: The Ethernet switch is setup by default to obtain its IP address via DHCP on the default VLAN 100.



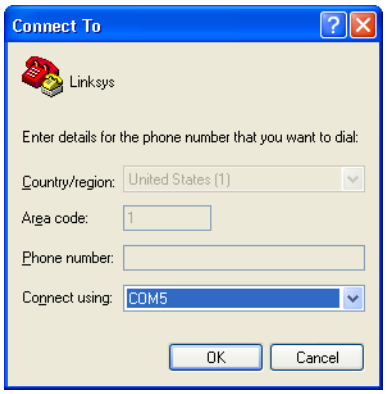
Configuring the HyperTerminal Application

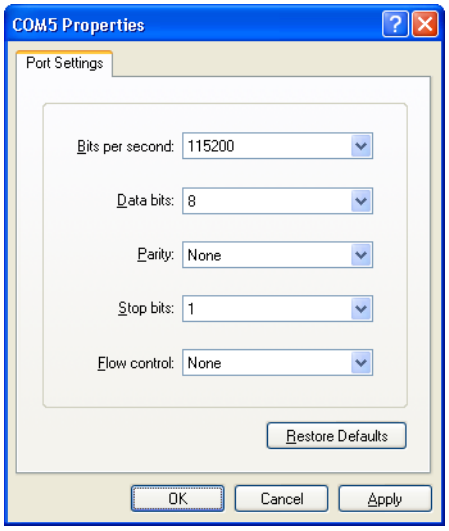
Before you use the console interface, you will need to configure the HyperTerminal application on your PC.

1. Click the Start button.
2. Select Programs and choose Accessories. Select Communications.
3. Select HyperTerminal from the options listed in this menu.
4. On the Connection Description screen, enter a name for this connection. In the example, the name of connection is Linksys One.
5. Select an icon for the application. Then, click the OK button.

6. On the Connect To screen, select a port to communicate with the Ethernet switch.
7. Set the serial port settings as follows:
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

   Then, click the OK button.





Connecting to the Switch using Telnet or SSH

If you know the IP address of your Ethernet switch (obtained from your DHCP server or the console interface), you can connect to the switch through a Telnet session.

1. Use your preferred Telnet or Secure Shell Client application, for example HyperTerminal or the Telnet application available through a Windows command window.
2. Open a telnet session using the IP address of your Ethernet switch. For example: **telnet 192.168.100.21**. The Login screen will appear.
3. Type the user name and password.
4. Press the **Enter** key.

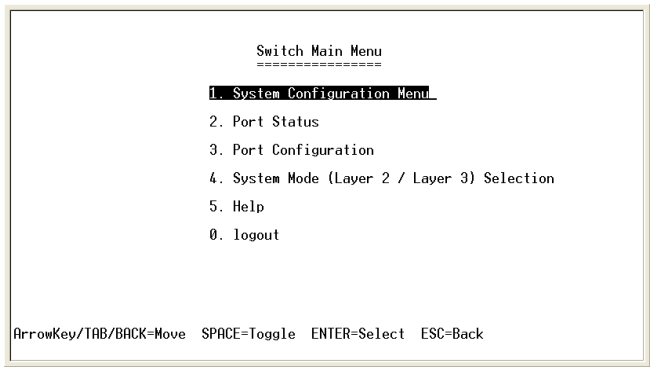
Configuring the Switch through the Console or Telnet Interface

The management screens consist of a series of menus. Each menu has several options, which are listed vertically. You select a menu option when you highlight it; pressing the **Enter** key activates the highlighted option.

To navigate through the menus and actions of the console interface, use the up or down arrow keys to move up or down, and use the left or right arrow keys to move left or right. Use the **Enter** key to select a menu option, and use the **Esc** key to go to the action menu. Menu options and any values entered or present are highlighted. The bottom of the screen lists the actions available.

Switch Main Menu

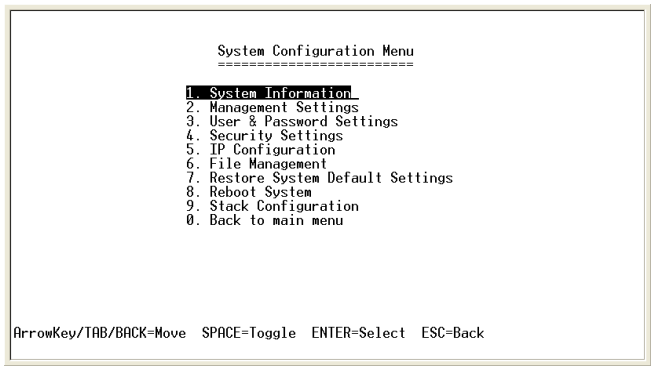
The System Main Menu screen displays these choices:



1. System Configuration Menu
2. Port Status
3. Port Configuration
4. System Mode (Layer 2 / Layer 3) Selection
5. Help

System Configuration Menu

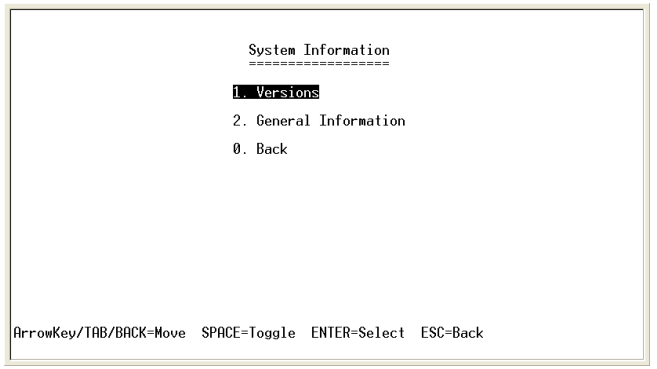
On the System Configuration Menu screen, you have these choices:



1. System Information
2. Management Settings
3. User & Password Settings
4. Security Settings
5. IP Configuration
6. File Management
7. Restore System Default Settings
8. Reboot System
9. Stack Configuration
0. Back to main menu

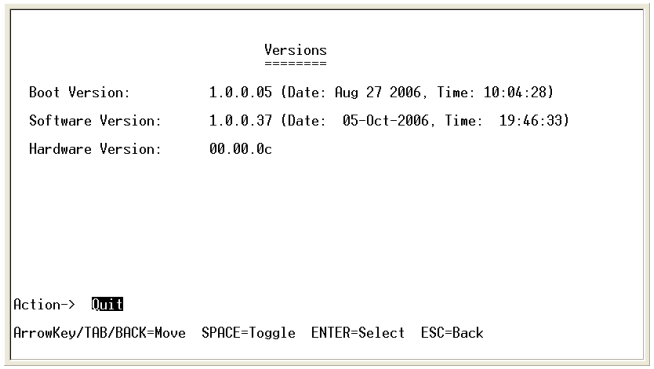
System Information

Use this screen to check firmware versions and general system information for the Ethernet switch.



Versions

Use the Versions screen to display the boot, software, and hardware firmware versions of the Ethernet switch. In stacking mode, this information is displayed for the stack master.



General System Information

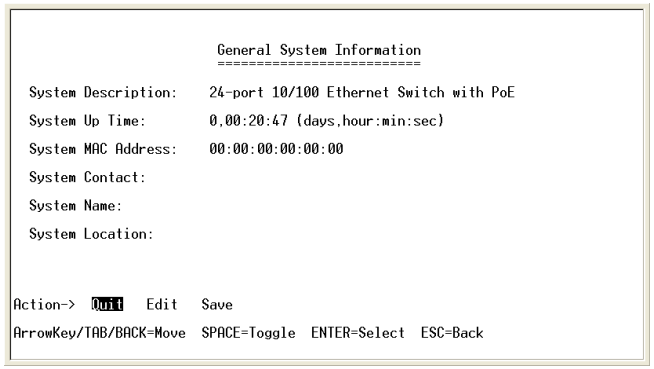
Use the General System Information screen to display the description, System Up Time, System MAC Address, System Contact, System Name, and System Location of the Ethernet switch.

To change general system information:

a. Select Edit to make changes.

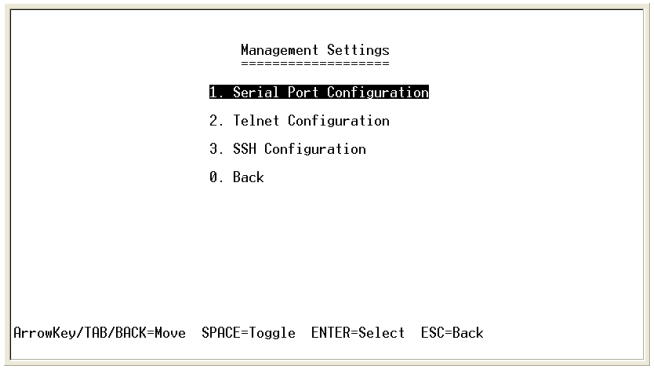
b. When your changes are complete, press the **Esc** key to return to the Action menu

c. Select Save to save your changes.



Management Settings

From the Management Settings screen, you can set Serial Port Session Configuration, Telnet Session Configuration, or Secure Telnet (SSH) Configuration.



Serial Port Configuration

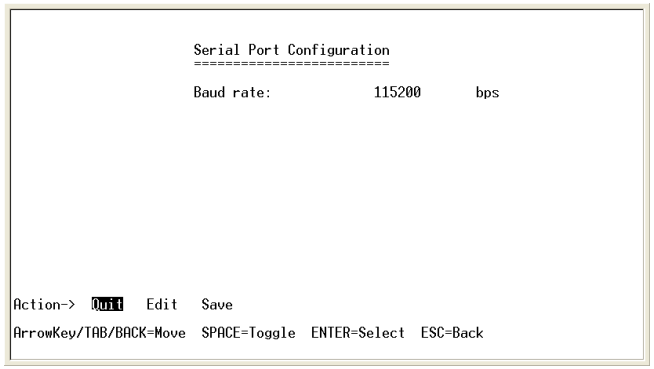
Use the Serial Port Configuration screen to display the baud rate of the Ethernet switch.

To change the baud rate of the serial port:

a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.



Telnet Configuration

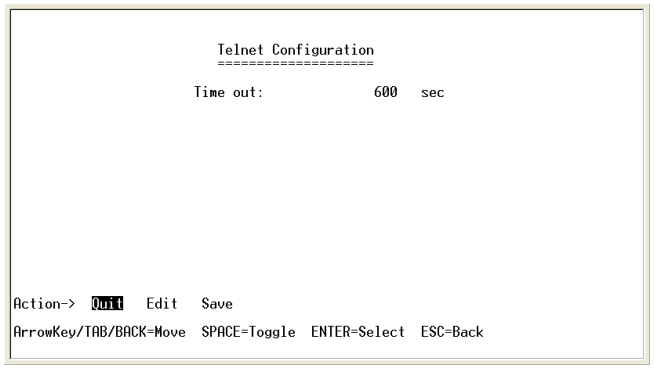
Use the Telnet Configuration screen to display the time-out settings.

To change the time-out setting:

a. Select Edit to make changes.

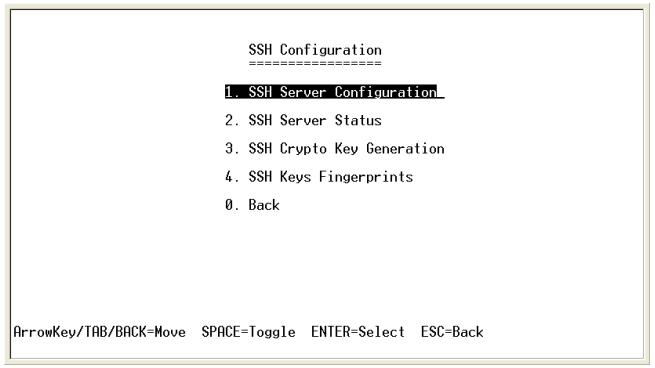
b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.



SSH Configuration

Use the SSH Configuration screen to configure and display SSH settings.



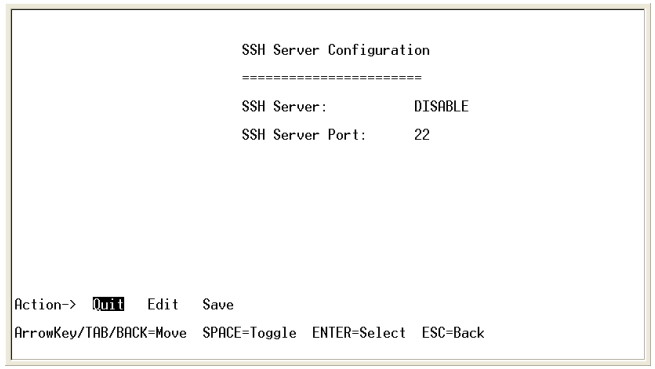
SSH Server Configuration: Use the SSH Server Configuration screen to enable or disable the SSH server, and to configure the port over which the SSH session is enabled.

To change SSH Server settings:

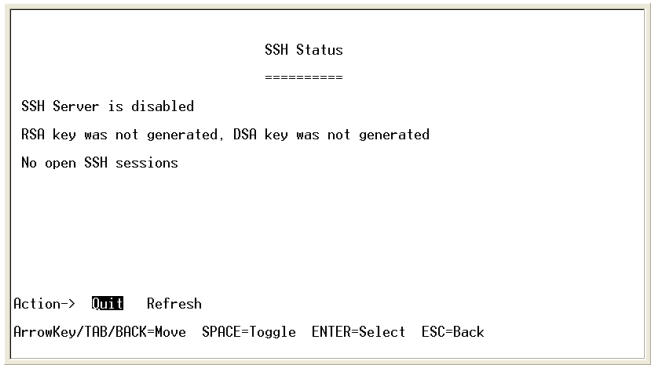
a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.



SSH Status: Use the SSH Status screen to view information about SSH sessions.



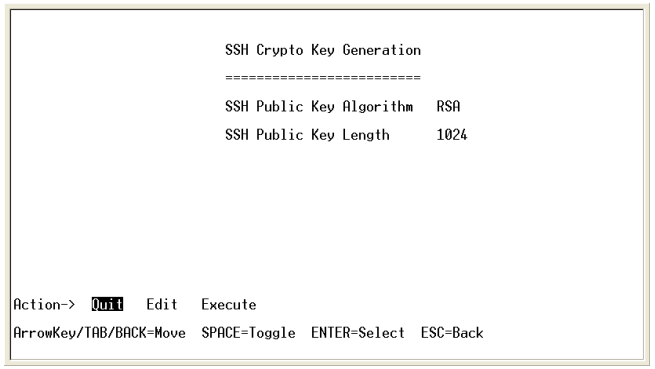
SSH Crypto Key Generation: Use the SSH Crypto Key Generation screen to generate an SSH RSA or DSA key.

To change SSH Crypto Key Generation settings:

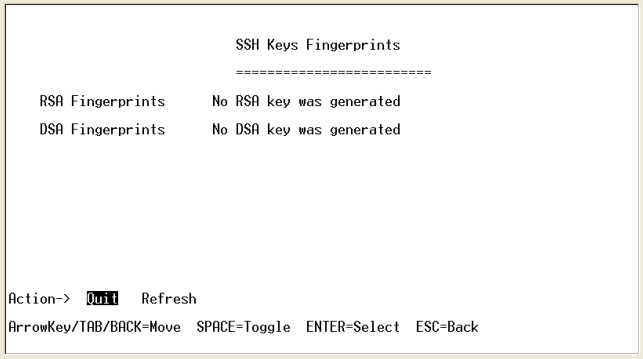
a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.

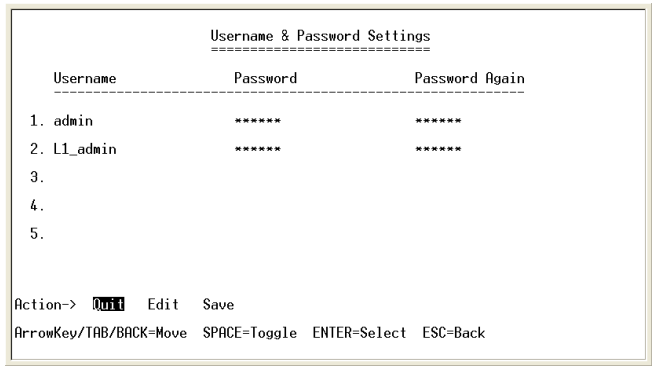


SSH Keys Fingerprints: Use the SSH Keys Fingerprints screen to view the RSA and SSA fingerprints.



User & Password Settings

The User & Password Settings screen lets you specify user names and passwords for the Ethernet switch. Up to 5 users can be assigned.



NOTE: The default user is "admin" with no password. There is also a special user defined by default for internal use by the Linksys system (l1_admin). For support reasons, it is recommended that you not delete this user.

To change User & Password settings:

a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.

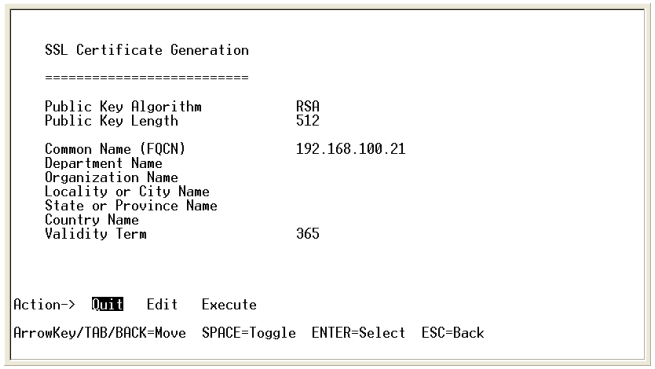
Security Settings

The Security Settings screen enables you to configure security settings on the Ethernet switch, as well as generate and display the certificate.

Use the SSL Certificate Generation screen to specify a device-generated certificate.

The following fields are specified:

Public Key Algorithm	Specifies the SSL type
Public Key Length	Specifies the SSL RSA key length. (Range: 512 to 2048)
Common Name (FQCN)	IP address of the Ethernet switch
Department Name	Specifies the department name. (Range: 1 to 32 characters)
Organization Name	Specifies the organization name. (Range: 1 to 32 characters)
Locality or City Name	Specifies the location or city name. (Range: 1 to 32 characters)
State or Province Name	Specifies the state or province name. (Range: 1 to 32 characters)



Country Name	Specifies the country name. (Range: 2 to 2)
Validity Term	Specifies number of days certification is valid. (Range: 30 to 3650)

To change SSL Certificate Generation settings:

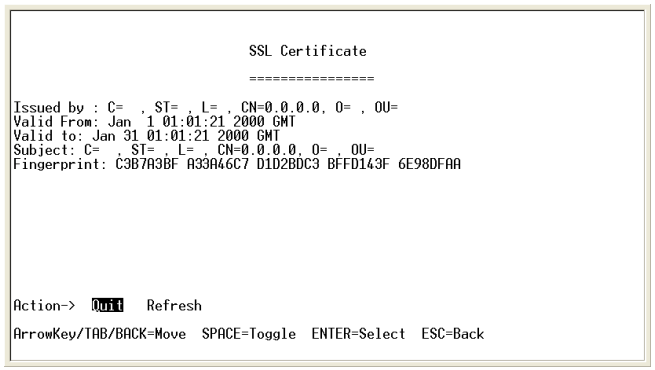
a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.

Show Certificate

Use the Show Certificate screen to display the internal certificate.



Disable Active Management Access Profile

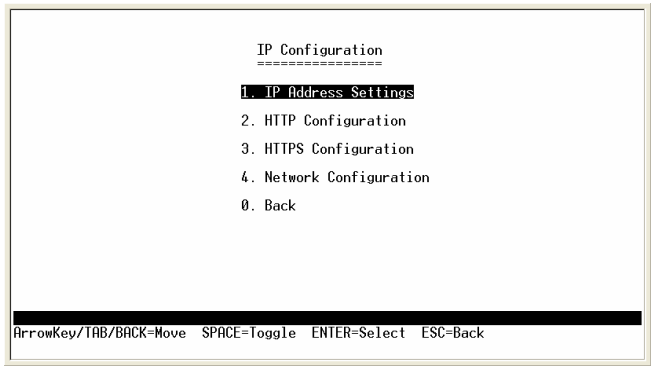
Disables the currently active management access profile.

To disable the currently active management access profile:

a. Type **Y** to verify that you want to disable the currently active management access profile.

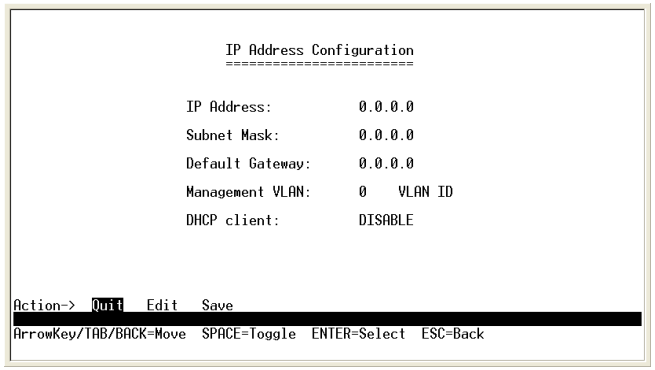
IP Configuration

The IP Configuration screen displays these choices: the IP Address Settings, HTTP, HTTPS Configuration, and Network Configuration of the Ethernet switch.



IP Address Configuration (Layer 2)

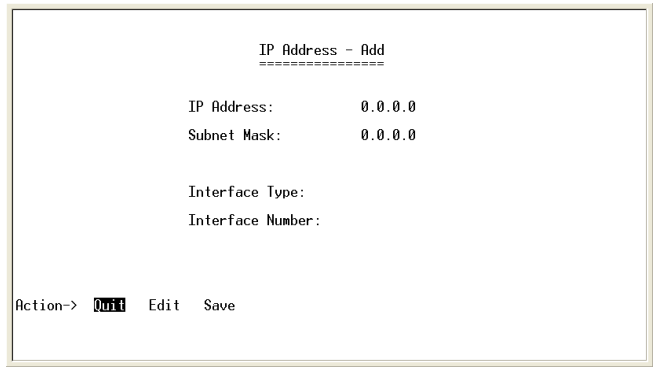
The IP information of the Ethernet switch is displayed here.



IP Address	The IP Address of the Ethernet switch is displayed. Verify that the address you enter is correct and does not conflict with another device on the network.
Subnet Mask	The subnet mask of the Ethernet switch is displayed.
Default Gateway	The IP address of your network's default gateway is displayed.
Management VLAN	The VLAN ID number is displayed.
DHCP client	The status of the DHCP client is displayed. If you want the Ethernet switch to be a DHCP client, then select ENABLE. If you want to assign an static IP address to the Ethernet switch, then enter the IP settings and select DISABLE.

IP Address Configuration (Layer 3)

The IP information of the Ethernet switch is displayed here.



IP Address	The IP Address of the Ethernet switch is displayed. Verify that the address you enter is correct and does not conflict with another device on the network.
Subnet Mask	The subnet mask of the Ethernet switch is displayed.
Interface Type	The type of interface.
Interface Number	The number of the interface.

To change IP address configuration settings:

a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.

IP Address Table (Layer 3 Only)

The IP Address Table screen lets you make changes to the IP address table.

To change the IP address table:

a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.

HTTP Configuration

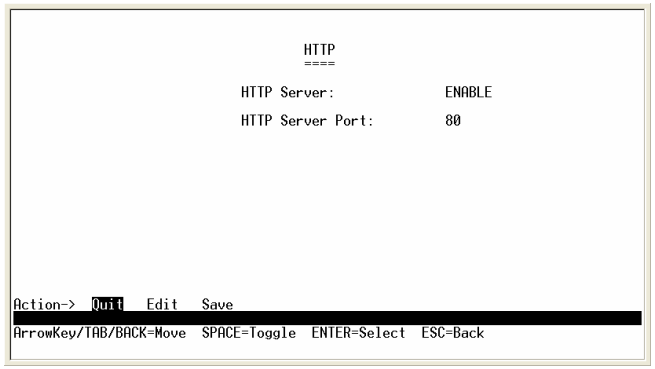
The HTTP screen displays the status and port number of the HTTP Server.

To change HTTP settings:

a. Select Edit to make changes.

b. When your changes are complete, press the **Esc** key to return to the Action menu.

c. Select Save to save your changes.



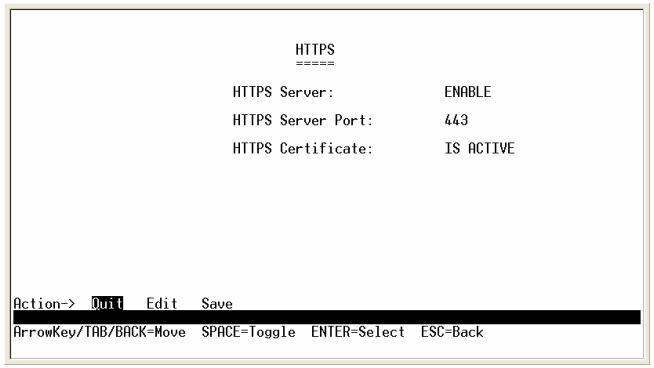
HTTPS Configuration

Use the HTTPS Configuration screen to configure HTTPS settings. You can enable or disable the HTTPS server and configure the port on which the session is enabled.

To change HTTPS settings:

a. Select Edit to make changes.

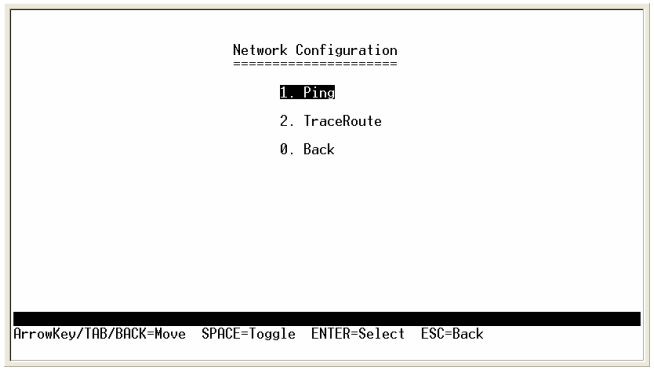
b. When your changes are complete, press the **Esc** key to return to the Action menu.



c. Select Save to save your changes.

Network Configuration

The Network Configuration screen offers a choice of two tests, Ping and TraceRoute.



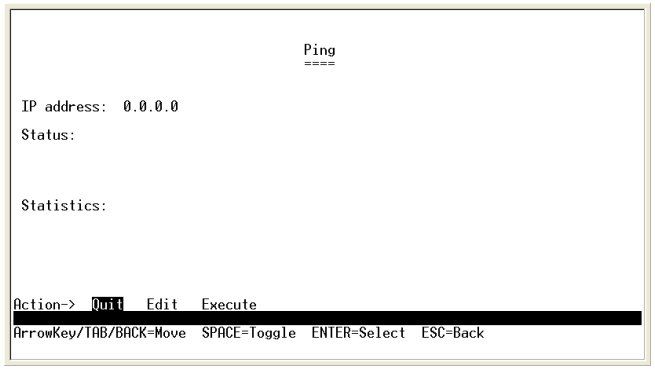
Ping

The Ping screen displays the IP address of the location you want to contact.

Select Edit to change the IP address, and select Execute to begin the ping test.

After the ping test is complete, the Ping screen displays the IP address, status, and statistics of the ping test.

Select Edit to make changes. When your changes are complete, press the **Esc** key to return to the Action menu, and select Save to save your changes.

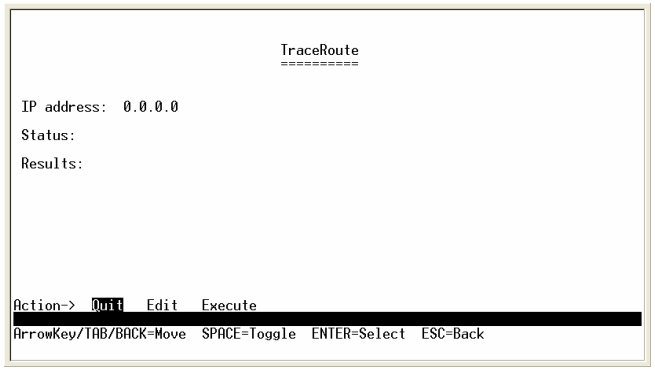


TraceRoute

The TraceRoute screen displays the IP address of the address whose route you want to trace.

Select Edit to change the IP address, and select Execute to begin the traceroute test.

After the traceroute test is complete, the TraceRoute screen displays the IP address, status, and statistics of the traceroute test.

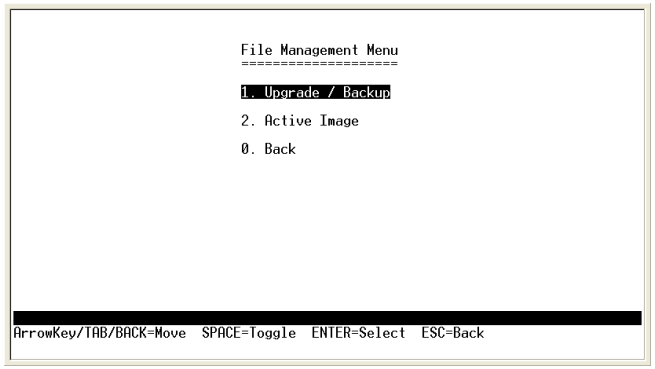


Select Edit to make changes. When your changes are complete, press the **Esc** key to return to the Action menu, and select Save to save your changes.

File Management

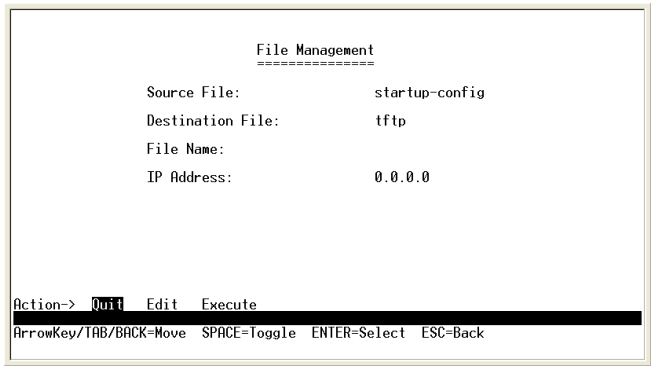
The File Management screen allows you to upload or download files, such as the startup configuration, boot, or image file, using a TFTP server.

NOTE: There are two software images on the Ethernet switch: Image 1 and Image 2. When you copy an image to the switch via TFTP, the inactive image is replaced. When you copy an image to the switch via the console port, the active image is replaced.



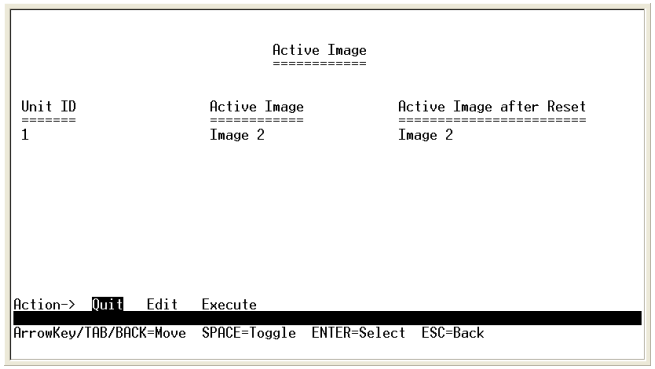
Upgrade / Backup

Select **Edit** to change the settings. Specify the source and destination of the file, the file name, and the IP address of the file server where the upgrade file is being downloaded, When your changes are complete, press the **Esc** key to return to the Action menu, and select Execute to upload or download the designated file.



Active Image

The Active Image screen shows information about the active image file and the image file that will be active after reboot.



Restore System Default Settings

To set the Ethernet switch back to the factory default settings, select Restore System Default Settings and press the **Enter** key. You will be asked if you want to continue. Press the **y** key to restore the default settings, or press the **n** key to cancel.

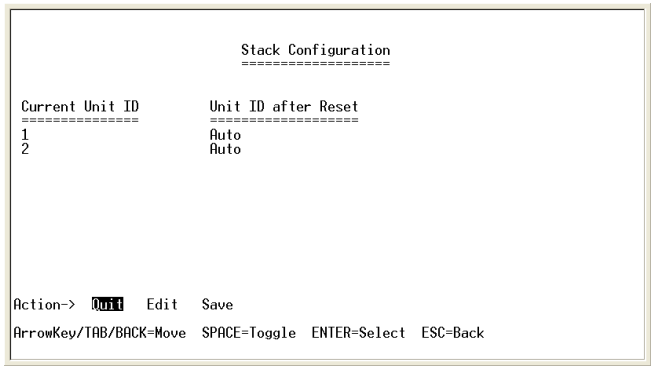
NOTE: Restoring default settings from the console, web, or Linksys One portal interfaces resets all values except stacking configuration (stacking mode, stacking ports, and auto-numbering settings are NOT reset). To reset stacking configuration, use the hardware reset button on the front of the Ethernet switch.

Reboot System

Select Reboot System and press the **Enter** key if you want to restart the Ethernet switch. You will be asked if you want to continue. Press the **y** key to reboot the Ethernet switch, or press the **n** key to cancel. After the Ethernet switch has rebooted, the Switch Main Menu screen will appear.

Stack Configuration

Select Stack Configuration to specify the Stack ID for the Ethernet switch. By default, ID numbers are automatically assigned to each device.



Back to main menu

Select Back to main menu and press the **Enter** key if you want to return to the Switch Main Menu screen.

Port Status

The Port Status screen displays the port connection status.

To view the status of the ports:

1. On the Switch Main Menu screen, select Port Status.

TIP: Use the **up** or **down** arrow keys to scroll through all the ports on the Ethernet switch.

2. Press the **Enter** key. The Port Status screen displays the port numbers, their status, Link status, speed and duplex mode, and status of flow control, which is the flow of packet transmissions.

If you want to change any settings for a port, you must use the Port Configuration screen.

Port Configuration

The Port Configuration screen lets you specify the auto negotiation status, port speed, duplex mode, and flow control settings.

To configure the ports:

1. On the Switch Main Menu screen, select Port Configuration.
2. Press the **Enter** key. The Port Configuration screen displays the port numbers, their status, auto-negotiation status, speed and duplex mode, and status of flow control, which is the flow of packet transmissions.
3. Select Edit to make changes. When your changes are complete, press the **Esc** key to return to the Action menu.
4. Select Save to save your changes.

TIP: Use the **up** or **down** arrow keys to scroll through all the ports on the Ethernet switch.

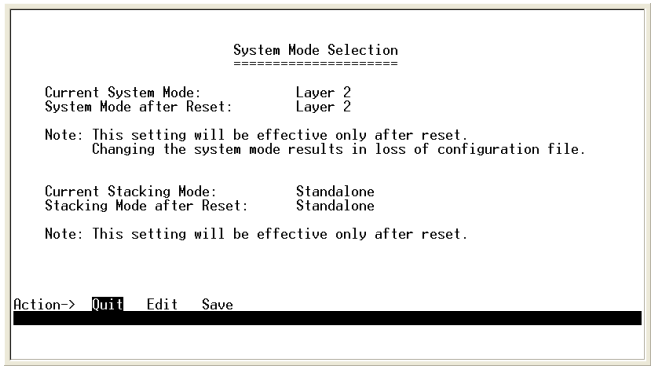
System Mode (Layer 2 / Layer 3) Selection

The System Mode Selection screen lets you specify whether the Ethernet switch is operating in Layer 2 or Layer 3 mode. You can also configure stacking mode from this screen.

IMPORTANT: If the Ethernet switch is being used as part of a Linksys One system, it must operate as a Layer 2 switch.

To view or edit the system mode:

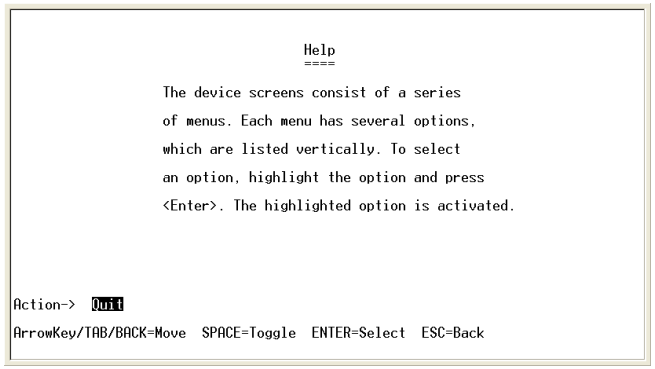
1. On the Switch Main Menu screen, select System Mode (Layer 2 / Layer 3) Selection Port Configuration.
2. Press the **Enter** key. The System Mode (Layer 2 / Layer 3) Selection screen displays the current system and stacking mode.



3. To edit these modes, select Edit to make changes. When your changes are complete, press the **Esc** key to return to the Action menu.
4. Select Save to save your changes.
5. Reboot the Ethernet switch. Your new settings will take effect after reboot.

Help

The Help screen lets you view information about how to navigate the Ethernet switch menus.



To view help information:

1. Select Help.
2. Press the **Enter** key if you want to view the help information. This screen explains how to navigate the various screens of the console interface.

Logout

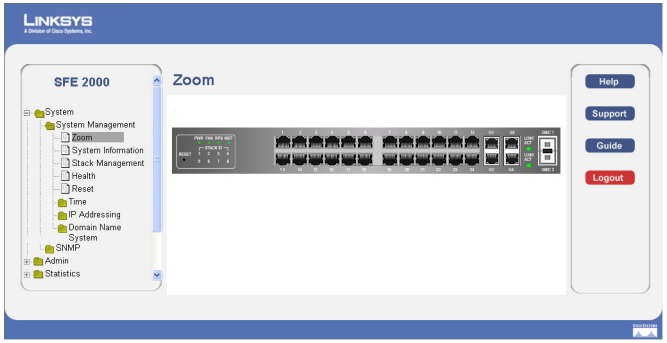
The Logout command lets you logout from the Ethernet switch.

NOTE: When you issue this command, you are immediately logged off the Ethernet switch.

To logout from the Ethernet switch:

- Select logout.

Web Utility Configuration



Overview

The Linksys Switch provides a complete web-based utility to configure the Ethernet switch. This utility is accessible through your web browser.

Use the navigation window, located on the left side of the web-based utility, to view various functions of the Ethernet switch.

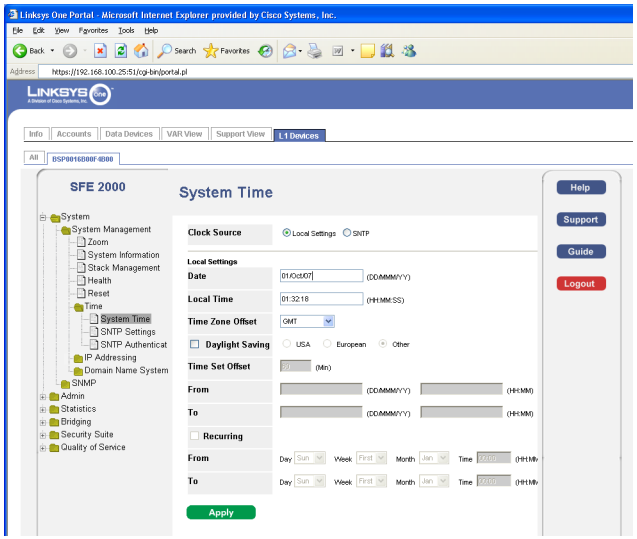
NOTE: The Ethernet switch is setup by default to obtain its IP address via DHCP on the default VLAN 100.

Accessing the Web-based Utility

To access the web-based utility, enter the IP address of the Ethernet switch to the address field of your web browser. For example: type **http://192.168.100.20** or **https://192.168.100.20** if the IP address of the Ethernet switch is 192.168.100.20. The IP address of the Ethernet switch is determined by DHCP, so you'll need to find its address using the Console configuration or the Linksys One Administrator screen.

If your Ethernet switch is part of a Linksys One system, the easiest way to manage it is with the Linksys One Portal — available only on the Linksys One Services Router. Refer to the *Customer Premises Equipment Administration Guide* for more details on the Linksys One Portal.

Linksys One Portal



Viewing Online Help

The Web Utility has complete online help functionality for each screen. To access on-line help for a particular screen, click on the Help button located on the right side of the screen.

A Linksys Contact Information

Need to contact Linksys?

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

In Europe	E-mail Address
Russia	support.ru@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom	support.uk@linksys.com

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

B

Customer Site Survey

Use this Customer Site Survey to gather customer contact information and other information about the customer site that will be needed for the implementation and installation of the Linksys Solution.

Customer Site Survey	
Site Name/Business Name	
Site Address	
Street Address	
City	
State	
Zip Code	
Shipping Address (if different from above)	
Street Address	
City	
State	
Zip Code	
Site Contact	
Name	
Title	
Phone	
Mobile	
Fax	

Customer Site Survey (Continued)	
Pager #	
E-mail	
After Hours Contact Phone Number	
Is this Site owned and maintained by the customer?	❒ Yes ❒ No If this site is not customer-owned, who is the owner and maintainer of the site?
Is this a manned site?	❒ Yes ❒ No
Hours of Operation	Specify the hours of operation (for example, Monday through Friday, 8am to 5pm, Saturday 9 am to 12 Noon).
Number of Users	How many users are at your site?
Phone number and location of the telephone nearest to the Linksys equipment	
Access Procedures	Specify room access procedures (for example, must visiting personnel be escorted by customer personnel?).

Customer Site Survey (Continued)	
Security/Safety Procedures	Specify any special security/safety procedures, such as the need for safety glasses, safety shoes, and the location(s) of hardhat areas.
Site Coordinator	Specify the name and phone number of the site coordinator responsible for ensuring that the site is adequately prepared for the installation of the Cisco equipment. Name: Phone:
Network/Bandwidth	What is the downlink and uplink speed of your broadband connection? Uplink speed (must be greater than 768 Kbps): Downlink speed (must be greater than 768 Kbps): Does your network use a firewall? ❒ Yes ❒ No

Limited Warranty

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

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

EXCLUSIONS AND LIMITATIONS

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

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

software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

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

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

OBTAINING WARRANTY SERVICE

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact the Value Added Reseller (VAR) from whom you purchased the product or Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys.

Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

TECHNICAL SUPPORT

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at www.linksys.com/support.

This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Federal Communication Commission Interference Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

WARNING: You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Industry Canada Statement

The Class [A] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation. Cet appareil numerique de la class [A] respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

EC Declaration of Conformity (Europe)

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

- EN55022 Emission
- EN55024 Immunity

Specifications

Models	• SFE2000 — 24-port 10/100 Ethernet switch • SFE2000P — 24-port 10/100 Ethernet switch with PoE
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x Flow Control, 802.3ad LACP,802.3af POE, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x Port Access Authentication
Ports	• 24 RJ-45 connectors for 10BASE-T/100BASE-TX + 4 10BASE-T/100BASE-TX/1000Base-T with 2 Gigabit combo ports shared between mini-GBIC ports • Console port • Auto MDI/MDI-X • Autonegotiate/Manual setting • RPS port for connecting to Redundant Power Supply unit
Cabling Type	UTP CAT 5 or better for 10BASE-T/100BASE-TX, UTP CAT 5e or better for 1000BASE-T
PoE	• IEEE 802.3af PoE on delivered over any of the 24 10/100 ports (SFE2000P only) • Power budget allows for max power of 15.4W on up to 12 ports simultaneously
Switching Capacity	12.8 Gbps non-blocking
LEDs	Power, Fan, Link/Act, PoE, Speed, RPS, Master, Stack ID 1 - 8
Stack Operation	• Up to 8 units in a stack (192 ports) • Hot Insertion and removal • Linksys 24-port Ethernet switch • Master and Backup master for resilient stack control • Auto-numbering or manual configuration of units in stack
Buttons	Reset Button

Layer 2 options	• MAC table size - 8K • Number of VLANs - 256 active VLANs (4096 range) • VLAN - Port-based and 802.1Q Tag-based VLANs - Protocol-based VLAN, Management VLAN - Private VLAN Edge (PVE) - GARP VLAN Registration Protocol (GVRP) • Head of line blocking prevention
Layer 3 options	• Static Routing • CIDR (Classless Interdomain Routing) • 128 Static Routes • IPv4 • Forwarding in silicon - Wirespeed forwarding of layer 3 traffic
Environment	• Operation Temperature: 0 to 40°C, 32 to 104°F • Storage Temperature: -20 to 70°C, -4 to 158°F • Operating Humidity 10% to 90% relative humidity, Non-Condensing • Storage Humidity 10% to 95% relative humidity, Non-Condensing
Web User Interface	Built-in Web UI for easy browser-based configuration (HTTP/HTTPS)
SNMP	SNMP version 1, 2c, 3 with support for traps
SNMP MIBs	• SNMP version 1, 2c, 3 with support for traps • RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 Bridge MIB, RFC2674 Extended Bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (groups 1,2,3,9 only), RFC2737 Entity MIB, RFC 2618 RADIUS Client MIB RFC 1215 Traps
Firmware Upgrade	• Web Browser upgrade (HTTP) and TFTP • Dual images for resilient firmware upgrades
Port Mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe

Other Management	• Traceroute • Single IP Management • Secure Socket Layer (SSL) security for Web UI • Secure Shell (SSH) • RADIUS • Port Mirroring • TFTP upgrade • DHCP Client • BootP • SNTP • Xmodem upgrade • Cable Diagnostics • PING • Syslog • Telnet Client (SSH secure support)
IEEE 802.1x	• 802.1x - RADIUS Authentication. MD5 Hash • Guest VLAN • Single/Multiple Host mode
Access Control	• Drop or Rate Limit based on: • Source and Destination MAC-based • Source and Destination IP address • Protocol • Port • VLAN • DSCP/IP Precedence • TCP/UDP Source and Destination ports • 802.1p priority • Ethernet Type • ICMP packets • IGMP packets • Up to 1018 rules
Link Aggregation	• Link Aggregation using IEEE 802.3ad LACP • Up to 8 ports in up to 8 groups
Storm Control	Broadcast, Multicast and Unknown Unicast

DOS prevention	DOS Attack prevention
Spanning Tree	IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, Fast Linkover
IGMP Snooping	IGMP (v1/v2) snooping limits bandwidth-intensive video traffic to only the requestors. Support 256 multicast groups.
Power Redundancy	Connection to RPSU for power redundancy
QoS	• Priority levels - 4 Hardware queues • Scheduling - Priority Queuing and Weighted Round Robin (WRR) • Class of Service - Port-based - 802.1p VLAN priority based - IPv4/v6 IP Precedence/TOS/DSCP based - Diffserv - Classification and Remarking ACLs • Rate Limiting - Ingress policer - Egress rate control
Certifications	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Regulatory Compliance	Products with the CE Marking indicate compliance with the 89/336/EEC and 73/23/EEC directives, which include the safety and EMC standards listed below.
Safety	UL 60950-1 IEC60950-1 CB / TUV/Rh CSA-C22.2 No. 60950 EN 60950 AS/NZS 60950-1 C-Tick

EMC	FCC Part 15 (CFR 47) Class A ICES-003 Class A EN 55022 Class A CISPR22 Class A EN 55024, EN 50082-1, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1
Dimensions	440 x 375 x 44 mm, 17.32 x 14.70 x 1.73 inch (W x D x H)
Unit Weight	• SFE2000 — 4.39kg, 9.68 lbs • SFE2000P — 4.94kg, 10.89 lbs
Power	• SFE2000 — 100-240VAC, 50-60 Hz, 0.54A MAX • SFE2000P — 100-240VAC, 50-60 Hz, 2.25A MAX


E

LINKSYS®
A Division of Cisco Systems, Inc.

CISCO SYSTEMS

Release 1.0