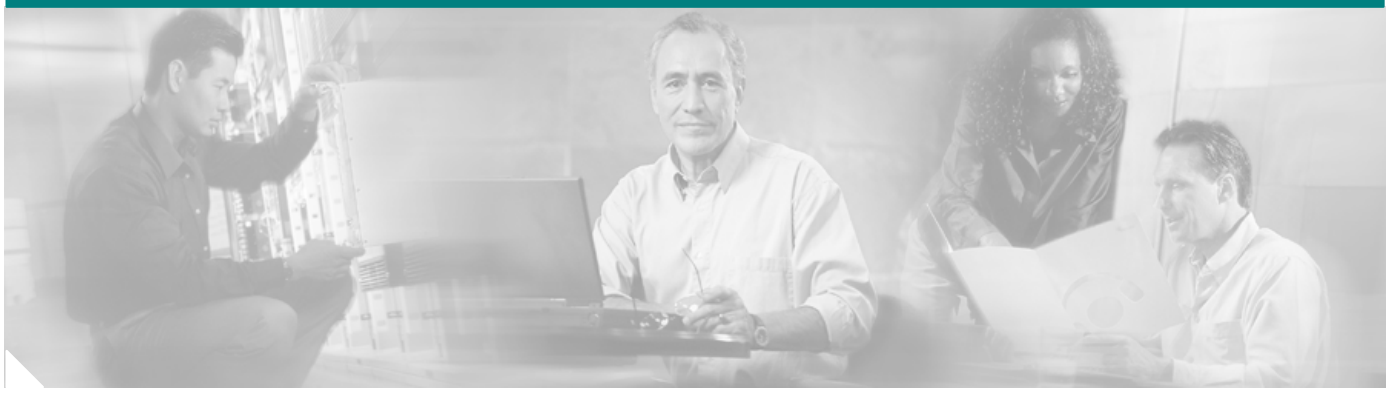
Quick Start Guide



Cisco Cisco Service Control Engine (SCE) Quick Start Guide

OL-7822-05

1 Documentation and Resources

Documentation for the ***SCE 1000*** platform is online and orderable. For detailed hardware installation instructions, refer to the online ***SCE 1000*** *Installation and Configuration Guide*.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- *http://www.cisco.com*
- *http://www-china.cisco.com*
- *http://www-europe.cisco.com*

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/pcgi-bin/marketplace/welcome.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can email your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

2 Prepare for Installation

This section contains warnings, information about tools and parts, site preparation information, and information for workbench or tabletop installation and rack-mount installation.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Warning Only trained and qualified personnel should install, replace, or service this equipment.

Warning Read the installation instructions before you connect the system to its power source.

Warning This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Warning Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.

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

Before beginning the installation of the ***SCE 1000***, read the *Regulatory Compliance and Safety Information for the Cisco Service Control Engine* document.

Site Preparation and Unpacking

- Lift the ***SCE 1000*** platform safely out of the packing container.
- Ensure the power service at the site is suitable for the ***SCE 1000*** platform.
- Check the packing slip to ensure that all the proper components are present.
- Locate and have accessible the Site Log for recording information about this installation.

Tools and Parts

Use the following list of tools and parts as a checklist for preparing for installing the ***SCE 1000*** platform:

- Appropriate cables to connect the ***SCE 1000*** to the network and console terminal
- Tape measure (optional)
- Level (optional)
- Number 1 Phillips screwdriver
- Number 2 Phillips screwdriver
- 1/4-inch flat-blade screwdriver
- 1/4-inch hex wrench
- Grounding kit (shipped with ***SCE 1000***)
- 12 AWG or 2.5 mm copper installation wire with hex or loop connectors for DC power leads (DC power only)

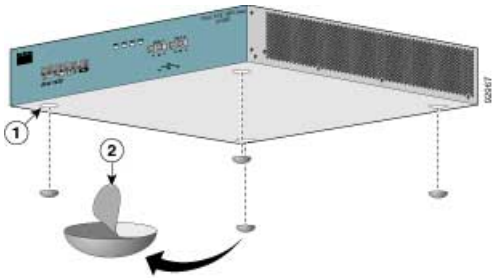
  Ring terminals must be UL approved and suitable for 12 AWG wire.
- AC power cords (AC power only, shipped with ***SCE 1000***)
- Rack-mounting kit (shipped with ***SCE 1000***)
  - Spare screws for changing bracket position

Prepare for Rack-Mount Installation

Before you begin the rack-mounting tasks, determine the type of rack—four-post or two-post—that you will be using.

Workbench or Tabletop Installation

Figure 1: Installing the System on a Flat Surface



For a workbench or tabletop installation, verify the following before installing the ***SCE 1000*** platform:

- The ***SCE 1000*** platform is off the floor and has adequate ventilation.
- An adequate chassis ground (earth) connection exists for the ***SCE 1000*** platform.
- The ***SCE 1000*** platform has at least 2 inches (5 cm) of clearance at each side and at least 5 inches (12.7 cm) of clearance at the rear to allow proper air flow.

Step 1 Remove the adhesive strips from the four rubber feet and affix the feet onto the four marked locations on the bottom panel of the unit.

Step 2 Place the ***SCE 1000*** platform on the tabletop or workbench.

3 Rack-Mount the SCE 1000

This section provides information for rack-mounting the ***SCE 1000*** platform.

There are two standard types of equipment racks, and the appropriate brackets for each are provided in the enclosed kit.

- 19” rack with front rack posts — the mounting kit includes two mounting brackets as illustrated below:

- 19” rack with front and back rack posts — in addition to the mounting brackets illustrated below, the mounting kit includes two crossrail supports that the unit slides onto.

The ***SCE 1000*** mounts to the two front rack posts with brackets that attach to the front of the ***SCE 1000*** The inside width between the two posts or mounting strips (left and right) must be at least 17.3 inches (44 cm).

Note Remember to leave a two-inch (5 cm) clearance on both sides of the ***SCE 1000*** and at the rear for adequate airflow for the inlet and exhaust vents.

Attach the Brackets to the SCE 1000

Before installing the ***SCE 1000*** in the rack, you must first install an appropriate rack-mount bracket on each side of the front of the ***SCE 1000***, as illustrated in the following figures.

Figure 2: Attaching the Mounting Brackets (4-post)

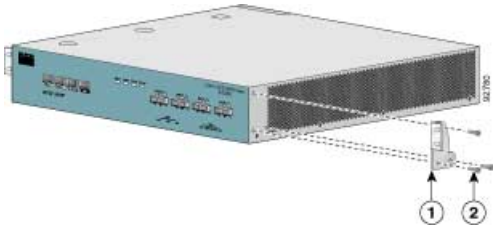
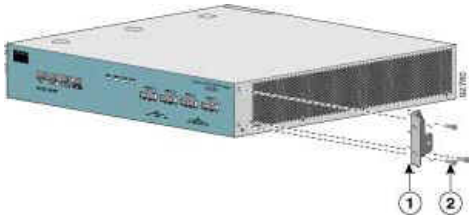


Figure 3: Attaching the Mounting Brackets (2-post)



To install the rack-mount brackets on the ***SCE 1000*** chassis, complete the following steps:

Before installing the ***SCE 1000*** in the rack, you must first install a rack-mount bracket on each side of the front of the ***SCE 1000***.

Step 1 Align the rack-mount bracket to the side of the ***SCE 1000***. Choose the proper bracket for your installation (2-post rack or 4-post rack) as illustrated in *Rack-Mount the* ***SCE 1000*** (on page 7).

Step 2 Insert and tighten three screws.

Step 3 Repeat steps 1 and 2 on the other side of the ***SCE 1000***.

If mounting the ***SCE 1000*** in a rack with only two posts, skip to Mounting the System to a Rack.

If mounting the ***SCE 1000*** in a rack with four posts, proceed to the next step to attach the crossrail supports to the rack.

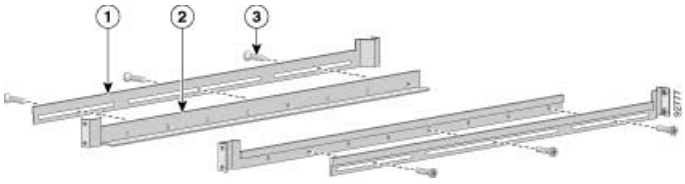
Installing the Crossrail Supports (Four-post rack only)

This section provides information for assembling the crossrail supports and attaching them to the rack.

When mounting in a rack with four posts (front and back) the two crossrail supports are mounted one on each side of the rack. The ***SCE 1000*** then slides into these crossrails, which support the weight of the unit.

Assemble the Crossrail Supports

Figure 4: Assembling the Slider Brackets

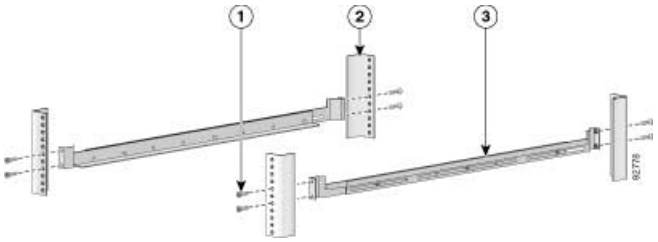


Step 1 Assemble the two crossrail supports. Use three screws for each crossrail assembly.

Make sure that they are oriented so that both crossrails will support the ***SCE 1000*** when they are attached to the rack.

Attach the Crossrail Supports to the Rack

Figure 5: Attaching the Crossrails to the Rack



Step 1 Align the crossrail supports with the side of the rack, parallel to the floor.

Step 2 Insert and tighten two screws to the front posts or mounting strips of the rack

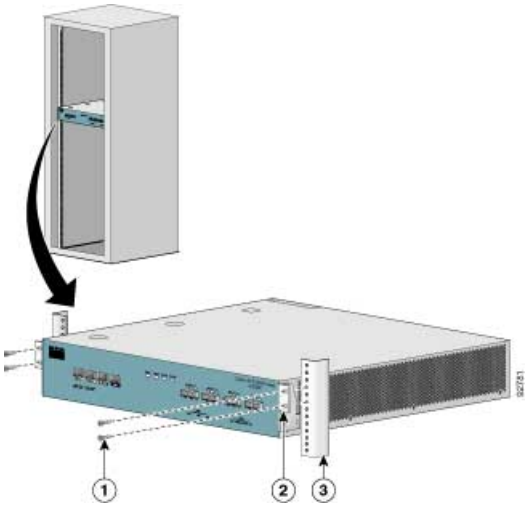
Step 3 Insert and tighten two screws to the Back posts of the rack.

Step 4 Repeat steps 2 and 3 on the other side of the rack, keeping the brackets flush against the posts and parallel to the supporting bracket on first side of the rack.

Mount the System to the Rack

When the appropriate mounting brackets are securely installed, the ***SCE 1000*** can be installed into the rack.

Figure 6: Sliding the SCE 1000 into the Rack



Step 1 Make sure that the rack brakes are locked or that the rack is otherwise stabilized.

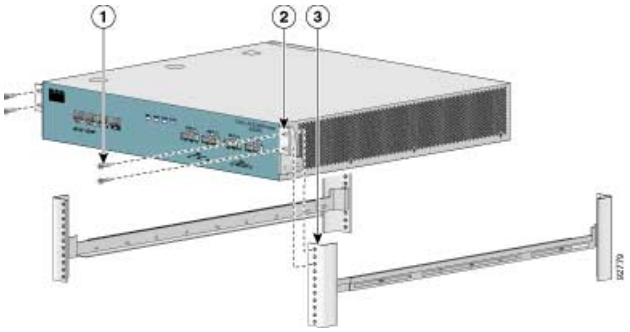
Step 2 Position the ***SCE 1000*** so that the front end is closest to you, and lift it carefully to place it into the rack. To prevent injury, avoid sudden twists or moves.

Step 3 Slide the ***SCE 1000*** into the rack, pushing it back until the brackets (installed at the front of the ***SCE 1000***) meet the mounting strips or posts on both sides of the rack.

A rack with both front and back posts will have the crossrail supports installed. Slide the ***SCE 1000*** onto these crossrails and push it all the way back.

Step 4 While keeping the brackets flush against the posts or mounting strips, align the holes in the brackets with the holes on the rack or mounting strip.

Figure 7: Securing the SCE 1000 to the Rack



Step 5 For each bracket, insert and tighten two appropriate screws to the rack.

Note Since the brackets support the weight of the entire ***SCE 1000*** chassis, be sure to use all four screws to fasten the two rack-mount brackets to the rack posts.

4 Connect the Power Supply Units

This section provides information for grounding the ***SCE 1000*** platform and connecting the AC or DC power supply units.

Connect the Chassis Ground

Figure 8: Grounding the Unit (AC)

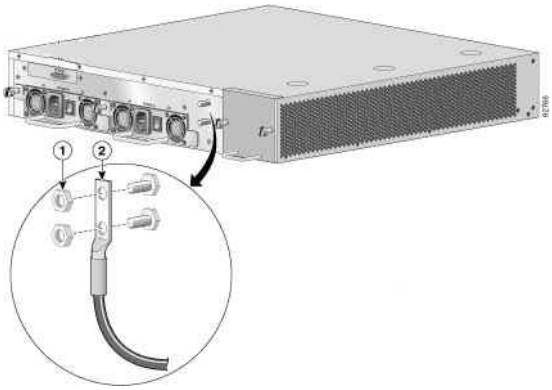
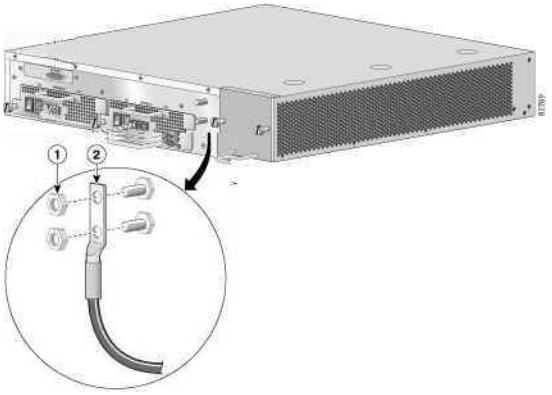


Figure 9: Grounding the Unit (DC)



A Grounding kit is provided with each ***SCE 1000***. Use this Grounding kit to properly ground the ***SCE 1000*** chassis.

Warning When installing the unit, the chassis ground connection must always be made first and disconnected last.

Step 1 On the rear panel of the ***SCE 1000***, locate the chassis grounding connector (refer to the appropriate figure for an AC- or DC-powered ***SCE 1000*** above).

Step 2 Attach the grounding cable (green and yellow colored cable), firmly fastening the (enclosed) hex nuts and spring washers with a #¼" hex wrench (refer to the appropriate figure for an AC- or DC-powered ***SCE 1000*** above).

The other side of the grounding cable must be connected to the site equivalent of the AC earth.

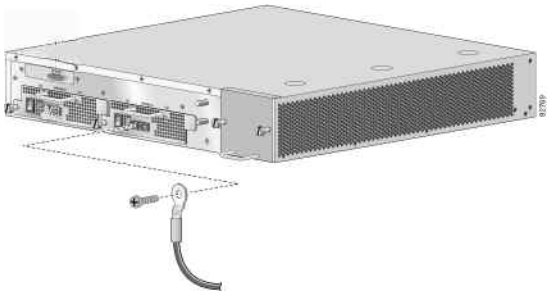
Connect the Power

The following sections describe how to reconnect the AC or DC power:

- *Connect the DC-Input Power Supply Unit* (on page 12)
- *Connect the AC-Input Power Supply Unit* (on page 13)

Connect the DC-Input Power Supply Unit

Figure 10: Connecting the DC Power



Warning Before completing any of the following steps, and to prevent short-circuit or shock hazards, ensure that power is removed from the DC circuit. To ensure that all power to the power supply unit is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.
Note that the power to the relevant power supply unit should be off, not necessarily all power to the ***SCE 1000*** platform. One DC-input power supply can be running when the other power supply is being removed or replaced.

Warning Wiring should be done by a professional in accordance with state and local electrical codes.

Step 1 Ensure that the DC power line input leads are disconnected from the power source.

Step 2 Using the number 2 Phillips screwdriver, remove the protective plate from the terminal block.

Step 3 Insert one receptacle screw into the hex or loop connector on one power line input, insert the screw with the connector into the corresponding lead receptacle and tighten the receptacle screw using the number 2 Phillips . Repeat for the remaining power line input lead.

Note The color coding of the DC-input power supply leads depends on the color coding of the DC power source at your site. Make certain the lead color coding you choose for the DC-input power supply matches lead color coding used at the DC power source.

Note Use 12 AWG (2.5 mm) copper wire only with hex or loop connectors. Ring terminals must be UL approved and suitable for 12 AWG wire.

Step 4 Using the number 2 Phillips screwdriver, securely fasten the protective plate to the terminal block.

Step 5 Connect the DC power line input leads to the DC power source through a fast 10A circuit breaker.

Step 6 Turn the on/off switch to the on (|) position.

Step 7 Look at the IN and OK LEDs on the power supply unit and the corresponding Power LED on the front panel. If the DC-input power supply unit is operating properly, these LEDs will be glowing green.

Step 8 Ensure that the power supply is properly aligned and the installation screw is tightened.

This completes the steps for reconnecting the DC-input power supply to the ***SCE 1000*** platform.

Connect the AC-Input Power Supply Unit

Figure 11: Connecting the AC Power

Step 1 Plug the AC-input power cable into the AC-input power receptacle on the AC-input power supply

Note For AC-input power, we recommend powering the ***SCE 1000*** platform from a 120 VAC, 15A receptacle U.S. (240 VAC, 10A international) at the power source.
15 A branch circuit protection is recommended.

Step 2 Plug the AC power supply cable into the AC power source.

Step 3 Turn the on/off switch to the on (|) position.

Step 4 Look at the IN and OK LEDs on the power supply unit and the corresponding Power LED on the front panel. If the AC-input power supply unit is operating properly, these LEDs will be glowing green.

Step 5 Ensure that the power supply is properly aligned and the installation screw is tightened.

5 Connect the Management Interfaces and Perform Initial System Configuration

This section explains how to connect the ***SCE 1000*** platform to a local console and perform the initial system configuration via the setup wizard that runs automatically.

Additionally, this section contains instructions for cabling the Fast Ethernet Management interface.

Connect the Local Console

Figure 12: Connecting to the Local Console

You must first connect the unit to a local console and configure the initial settings for the ***SCE 1000*** to support remote management. When the initial connection is established, the setup utility will run automatically, prompting you to perform the initial system configuration.

Make sure that the terminal configuration is as follows:

- 9600 baud
- 8 data bits
- No Parity
- 1 stop bits
- No flow control

The above ***SCE 1000*** port parameters are fixed and are not configurable.

Step 1 Plug the RS-232 serial cable provided with the ***SCE 1000*** into the CON port on the front panel of the ***SCE 1000***.

Step 2 Connect the other end of the serial cable (with an attached DB-9 connector) to the VT100 compatible local (serial) terminal.

Step 3 At the console. press **Enter** several times until the Cisco logo appears on the local terminal and the setup configuration dialog is entered.

```
                --- System Configuration Dialog ---

At any point you may enter a question mark '?' followed by 'Enter' for help.
Use ctrl-C to abort configuration dialog at any prompt.
Use ctrl-Z to jump to the end of the configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Would you like to continue with the System Configuration Dialog? [yes/no]: y
```

Step 4 Type y and press **Enter**.

The system configuration dialog begins.

Initial System Configuration

Upon initial connection to the local terminal, as described above, the system configuration wizard automatically runs to guide the user through the entire setup process. The wizard prompts for all necessary parameters, displaying default values, where applicable. You may accept the default values or define other values.

With the exception of the time settings, which take effect immediately when entered, the new configuration is applied and saved only at the end of the dialog when approved by the user. Therefore, if the setup dialog is aborted, no change takes place in the configuration, other than time settings (if entered).

When the dialog is complete, you may review the new configuration before applying it. The system displays the configuration, including parameters that were not changed. The system also displays any errors that are detected in the configuration. When the configuration is satisfactory, you may apply and save the new configuration.

The following table lists all the parameters included in the initial configuration. It is recommended that you obtain values for any parameters that you will configure at this time before beginning the setup.

Note For further information regarding any configuration step or specific parameter, refer to the relevant section in the `Cisco Service Control Engine (SCE) Software Configuration Guide`.

Setup Command Parameters

Table 5-1 Setup Command Parameters

Parameter	Definition
IP address	IP address of the ***SCE 1000***.
subnet mask	Subnet mask of the ***SCE 1000***.
default gateway	Default gateway.
hostname	Character string used to identify the ***SCE 1000***
admin password	Admin level password. Character string from 4-100 characters beginning with an alpha character.
root password	Root level password. Character string from 4-100 characters beginning with an alpha character.
password encryption status	Enable or disable password encryption?
Time Settings	
time zone name and offset	Standard time zone abbreviation and minutes offset from UTC.

Parameter	Definition
local time and date	Current local time and date. Use the format: 00:00:00 1 January 2002
SNTP Configuration	
broadcast client status	Set the status of the SNTP broadcast client. If enabled, the SCE will synchronize its local time with updates received from SNTP broadcast servers.
unicast query interval	Interval in seconds between unicast requests for update (64 – 1024)
unicast server IP address	IP address of the SNTP unicast server.
DNS Configuration	
DNS lookup status	Enable or disable IP DNS-based hostname translation.
default domain name	Default domain name to be used for completing unqualified host names
IP address	IP address of domain name server. (maximum of 3 servers)
RDR Formatter Destination Configuration	
IP address	IP address of the RDR-formatter destination
TCP port number	TCP port number of the RDR-formatter destination
Access Control Lists	
Access Control List number	How many ACLs will be necessary? What IP addresses will be permitted/denied access for each management interface? You may want ACLs for the following : • Any IP access • Telnet access • SNMP GET access • SNMP SET access
list entries (maximum 20 per list)	IP address, and whether permitted or denied access.
IP access ACL	ID number of the ACL controlling IP access.
telnet ACL	ID number of the ACL controlling telnet access.
SNMP Configuration	
SNMP agent status	Enable or disable SNMP management.
GET community names	Community strings to allow GET access and associated ACLs (maximum 20).
SET community names	Community strings to allow SET access and associated ACLs (maximum 20).
trap managers	Trap manager IP address, community string, and SNMP version. (maximum 20)
Authentication Failure trap status	Set the status of the Authentication Failure trap. (See Traps.)
enterprise traps status	Set the status of the enterprise traps. (See Traps.)
system administrator	Name of the system administrator.

Parameter	Definition
Topology Configuration	
connection mode	Is the ***SCE 1000*** installed in inline topology or receive-only using an optical splitter?
link bypass mode on operational status	When the ***SCE 1000*** is operational, should it bypass traffic or not?
redundant ***SCE 1000*** platform?	Is there a redundant ***SCE 1000*** installed as a backup?
link bypass mode on non-operational status	When the ***SCE 1000*** is not operational, should it bypass traffic or cut it off?
operational status of the SCE after abnormal boot	After a reboot due to a failure, should the ***SCE 1000*** remain in a Failure status or move to operational status provided no other problem was detected?

Following are some general instructions regarding the setup dialog:

- All default values appear in square brackets [**default**].

  If no value appears in the brackets [], or more than one option appears [**yes/no**], then this parameter does not have a default value.

- To accept the default value, press **Enter.**
- If you need more information about any parameter, type **?** and press **Enter**.

  A help message will appear describing the expected format of the parameter and any other requirements.

- To jump to the end of the setup dialog at any point, accepting all remaining default values, press **^z.**
- In certain cases, there will be two or more logically related parameters within a menu. In these situations, it is not permitted to jump to the end of the setup dialog until all related parameters are configured. If you try to jump to the end of the setup dialog, the following message will appear: "`Sorry, Skipping is not allowed at this stage`."
- Certain groups of related parameters, such as time, date, and SNTP settings, form sub-dialogs or menus within the setup dialog. You may skip an entire menu, thereby accepting all default values for the parameters within the menu.

  Each group of related parameters is prefaced by a question, asking whether you want to enter the menu. To skip the menu, answer no ("n") to the question.

EXAMPLE:

```
Would you like to enter the SNMP configuration menu? n
```

- To abort the setup dialog at any point without making any configuration changes, press **^c.** All changes already entered will be lost, with the exception of time settings.

Step 1: Configuring Initial Settings

Verify the following initial settings for the ***SCE 1000***:

- IP address
- Subnet mask
- Default gateway

All values are Internet addresses of the form *'X.X.X.X'*, where each letter corresponds to a decimal number between 0 and 255.

To configure the initial settings, complete the following steps:

Step 1 The current IP address is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired value in the format "*x.x.x.x*" and press **Enter**.

Step 2 The current subnet mask is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired value in the format "*x.x.x.x*" and press **Enter**.

Step 3 The current IP address of the default gateway is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired value in the format "*x.x.x.x*" and press **Enter**.

EXAMPLE:

The following example displays a typical configuration of the IP address (10.1.5.109), subnet mask (255.255.0.0), and default gateway (10.1.1.3).

Since the IP address and the subnet mask are related, when the IP address is changed, there is no longer a default value of the subnet mask, and it must be entered explicitly.

```
Enter IP address [10.1.1.201]:10.1.5.109
Enter IP subnet mask:255.255.0.0
Enter IP address of default gateway [10.1.1.3]:
```

Step 2: Configuring the Hostname

The hostname is used to identify the ***SCE 1000***. It appears as part of the CLI prompt and is also returned as the value of the MIB-II object sysName.

The default hostname is ***SCE 1000***.

To configure the hostname, complete the following steps:

Step 1 The current hostname is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type any desired character string and press **Enter**.

```
Enter hostname [SCE 1000]:
```

Step 3: Setting the Passwords

Configure the passwords as follows:

- Set the password for each authorization level (User, Admin, Root).
- Enable/disable password encryption. When password encryption is enabled, it encrypts the previously entered passwords.

Note Passwords are needed for all authorization levels in order to prevent unauthorized users from accessing the ***SCE 1000***. Admin level should be used by the network administrator. Root level is for use by Cisco technician.

Passwords must meet the following criteria:

- Minimum length — 4 characters
- Maximum length — 100 characters
- Begin with an alpha character
- May contain only printable characters

Note Passwords are case sensitive.

Note The default password for all levels is "**cisco**".

To change the passwords, complete the following steps:

Step 1 The default User password is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired string and press **Enter**.

Step 2 The default Admin password is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired string and press **Enter**.

Step 3 The default Root password is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type the desired string and press **Enter**.

Step 4 Configure password encryption. By default, password encryption is not enabled.

- To disable password encryption, press **Enter**.
- To enable password encryption, type **y** and press **Enter**.

EXAMPLE:

Following is an example of changing all passwords. Password encryption is not enabled (default).

```
Enter a User password [cisco]: userin
Enter an Admin password [cisco]: mng123
Enter a Root password [cisco]: cistech
Enable passwords encryption? [no]:
```

Step 4: Configuring Time Settings

The time settings menu configures all time and date related parameters in the system. The time settings menu includes the following:

- Time zone
- Local time
- Date
- SNTP menu

You must enter the time setting menu in order to configure SNTP settings. You may choose to skip the time settings menu if you wish to accept all default values.

Note Unlike all other settings defined in the system configuration, setting the time is done immediately and not at the end of the setup process.

To configure the time settings, complete the following steps:

Step 1 Enter the time settings menu.

```
Would you like to enter the Time settings menu? [no]: y
```

Type **y** and press **Enter**.

The time settings dialog begins.

Step 2 Type the time zone abbreviation and press **Enter**.

```
Enter time zone name [UTC]: CET
```

Step 3 Type the minutes offset from UTC and press **Enter**.

```
Enter time zone minutes offset from UTC: 60
```

The local time and date are displayed, and you are asked whether you want to change them.

```
The local time and date is 15:00:01 CET FRI 01 July 2002
Would you like to set a new time and date? [no]:
```

Step 4 If the time and date are correct, go to step 5.

If the time and date are not correct, answer yes to the above question, and press **Enter**.

```
Would you like to set a new time and date? [no]: y
```

Confirm your response and type the new time and date.

```
This change will take effect immediately both on the system clock and the calendar; it
will also set the time zone you entered. Are you sure? [yes/no]: y
Enter new local time and date: 14:00:01 1 July 2002
Time zone was successfully set.
The system clock and the calendar were successfully set.
```

Step 5 You are asked whether you wish to enter the SNTP configuration menu.

If you do not wish to configure the SNTP, skip the rest of this section and go to *Step 5: Configuring the DNS Settings* (on page 23).

To enter the SNTP configuration dialog, type **y**, and press **Enter**

```
Would you like to enter the SNTP configuration menu? [no]: y
```

Step 6 Configure the SNTP broadcast client. By default the SNTP broadcast client is not enabled.

- To disable the SNTP broadcast client, press **Enter**.
- To enable the SNTP broadcast client, type **y** and press **Enter**.

```
Enable SNTP broadcast client? [no]:
```

Step 7 Define the time interval between unicast updates.

- To accept the displayed default value, press **Enter**.
- To change the value, type the desired number of seconds (64 through 1024**)** and press **Enter**.

```
Enter time interval in seconds between unicast updates [1024]:
```

Step 8 You may enter an IP address for the SNTP unicast server. Type in the hostname or the IP address in the form *x.x.x.x*, and press **Enter**

```
Would you like to configure SNTP unicast servers? [no]: y
Enter IP address or hostname of SNTP unicast server: 10.1.1.1
```

EXAMPLE:

Following is a sample time setting dialog. In addition to setting the time zone, time and date are changed, and SNTP unicast updates are configured.

```
Would you like to enter the Time settings menu? [no]: y
Enter time zone name [UTC]: ISR
Enter time zone minutes offset from UTC: 120

The local time and date is 15:35:23 ISR FRI July 19 2002
Would you like to set a new time and date? [no]: y
This change will take effect immediately both on the system clock and the calendar; it
will also set the time zone you entered. Are you sure? [yes/no]: y
Enter new local time and date: 14:35:23 19 July 2002
Time zone was successfully set.
The system clock and the calendar were successfully set.
Would you like to enter the SNTP configuration menu? [no]: y
Enable SNTP broadcast client? [no]: y
Enter time interval in seconds between unicast updates [900]:
Would you like to configure SNTP unicast servers? [no]: y
Enter IP address or hostname of SNTP unicast server: 10.1.1.1
```

Step 5: Configuring the DNS Settings

The DNS configuration menu defines the IP address of the domain name server, which is used for DNS lookup, as well as the default domain name, which is used to complete unqualified host names.

You may choose to skip the DNS configuration menu if you wish to accept all default values.

To configure DNS settings, complete the following steps:

Step 1 Enter the DNS settings menu.

```
Would you like to enter the DNS configuration menu? [no]: y
```

Type **y** and press **Enter**.

The DNS settings dialog begins.

Step 2 Enable or disable DNS lookup.

- To enable DNS lookup, press **Enter**.
- To disable DNS lookup, type **n** and press **Enter**.

```
Enable IP DNS-based hostname translation? [yes]:
```

If you choose to disable DNS lookup, skip the rest of this section and go to *Step 6: Configuring the RDR Formatter Destination* (on page 24). The rest of the dialog is not presented, as it is irrelevant when DNS lookup is disabled.

Step 3 Type the default domain name to be used, and press **Enter.**

Note that there is no default domain name.

You may accept the default domain name or enter a new one.

```
Enter default domain name []:
```

Step 4 Type the IP address of the primary domain name server and press **Enter**.

```
Enter Primary DNS IP address:
```

Note that there is no default for this parameter.

Step 5 You may configure up to three domain servers.

```
Would you like to add another Name Server? [no]:
```

- To exit the DNS settings dialog, press **Enter**.
- To add another domain server, type **y** and press **Enter**.

You are asked to enter the IP address of the next domain name server.

```
Enter Secondary DNS IP address:
```

Step 6 When IP addresses for all servers have been entered, exit the dialog by pressing **Enter**.

```
Would you like to add another Name Server? [no]:
```

EXAMPLE:

Following is a sample DNS configuration dialog. The default domain name is pcube.com, and the IP address of the Domain Name Server is 10.1.1.230.

```
Would you like to enter the DNS configuration menu? [no]: y
Enable IP DNS-based hostname translation? [yes]:
Enter default domain name []: pcube.com
Enter Primary DNS IP address: 10.1.1.230
Would you like to add another Name Server? [no]:
```

Step 6: Configuring the RDR Formatter Destination

The ***SCE 1000*** passes Raw Data Records (RDRs) to an external collection system via the RDR-Formatter. In order for the data to reach the correct location, the IP address of the external collection system and its port number must be configured.

To configure the RDR-formatter destination, complete the following steps:

Step 1 Enter the RDR formatter configuration menu.

```
Would you like to enter the RDR-formatter configuration menu? [no]: y
```

Type **y** and press **Enter**.

The RDR-formatter destination dialog begins.

Step 2 Type the IP address of the RDR-formatter destination and press **Enter.**

```
Enter RDR-formatter destination's IP address:
```

Note that there is no default for this parameter.

Step 3 Type the TCP port number of the RDR-formatter destination and press **Enter.**

Note that there is no default for this parameter.

```
Enter RDR-formatter destination's TCP port number:
```

EXAMPLE:

Following is a sample RDR-formatter configuration dialog, assigning the IP address and TCP port number.

```
Would you like to enter the RDR-formatter configuration menu? [no]: y
Enter RDR-formatter destination's IP address: 10.1.1.230
Enter RDR-formatter destination's TCP port number: 33000
```

Step 7: Configuring Access Control Lists (ACLs)

The ***SCE 1000*** can be configured with Access Control Lists (ACLs), which are used to permit or deny incoming connections on any of the management interfaces.

Note ACL #0 is a pre-defined list that permits access to all IP addresses.

Configuration of access control lists is done in two stages:

Step 1 Create the access control lists.

You may create 99 ACLs with a maximum of 20 entries per list. Each entry consists of an IP address, and an indication of whether access is permitted or denied to this IP address.

Step 2 Assign the ACLs to the appropriate management interface. (See *Step 9: Configuring the Topology-Dependent Parameters* (on page 31).)

The dialog permits you to skip the creation/editing of the ACLs and go directly to assigning ACLs to the management interfaces.

Entry Formats

Each ACL may permit/deny access to any IP address, one or more ranges of IP addresses, or one or more individual IP address. Three entry formats are available to support these options:

- **Any IP address** — Type the word "**any**". Any IP address will be permitted or denied access.
- **Range of IP addresses** — Type the beginning IP address in the desired range, then enter the wildcard bits that define the range.

  This wildcard functions like a reverse mask, in that all "1" bits in the wildcard indicate the corresponding bit in the IP address should be ignored. All other bits must match the corresponding bit in the specified IP address. Refer to the table below for examples.

  Each range of IP addresses can be configured to be permitted or denied access.
- **Individual IP address** — Type the desired IP address, then enter the wildcard bits **0.0.0.0**.

  Each individual IP address can be configured to be permitted or denied access.

Table 5-2 IP address/Wildcard bit examples

Initial IP address	Wildcard bits	Range
10.1.1.0	0.0.0.255	10.1.1.0–10.1.1.255
10.1.1.0	0.0.0.63	10.1.1.0–10.1.1.63
10.1.1.0	0.0.0.0	10.1.1.0 (individual entry)

Order of Entries

The order of the entries in the list is important. The entries in the list are tested sequentially, and the action is determined by the first entry that matches the connecting IP address. Therefore, when the entry “any” appears in an Access Control List, all succeeding entries are irrelevant.

Consider two hypothetical ACLs containing the same entries in a different order.

The following list would permit access to all IP addresses, including 10.1.1.0:

permit any

deny 10.1.1.0

Note that the above list could not actually be created using the setup utility, since after the “any” entry, no other entries could be added to the list.

The following list will deny access to IP address 10.1.1.0, but permit access to all others:

deny 10.1.1.0

permit any

If no entry in the assigned Access Control List matches the connection, or if the Access Control List is empty, the default action is **deny**.

To create the access control lists, complete the following steps:

Step 1 Enter the Access Control Lists configuration menu.

```
Would you like to enter the Access lists configuration menu? [no]: y
```

Type **y** and press **Enter**.

The Access Control Lists configuration dialog begins.

Step 2 You have the option of creating or modifying Access Control Lists, or skipping this section and proceeding directly to assign the existing ACLs to the desired management interfaces.

```
Would you like to create new Access lists or modify existing lists? [no]: y
```

If you choose not to create or edit Access Control Lists, skip to *Step 9: Configuring the Topology-Dependent Parameters* (on page 31).

Step 3 Type the number of the Access Control List to be configured (1 through 99) and press **Enter.**

Note that there is no default for this parameter.

Step 4 Begin adding entries to the selected list.

Indicate whether this entry is permitted access or denied access.

- To permit access press **Enter**.
- To deny access type **n** and press **Enter**.

```
Does this entry permit access? [yes]:
```

Step 5 Type the IP address to be added to this list, and press **Enter.**

Type “**any**” and press **Enter** to include any IP address in the ACL.

Note that there is no default for this parameter.

```
Enter IP address or the word 'any' to denote any IP address:
```

Step 6 If you entered a specific IP address, enter the wildcard bits to define a range of IP addresses and press **Enter**. (See *Entry Formats* (on page 25).)

To define an individual IP address, type **0.0.0.0** and press **Enter**.

There is no default for this parameter.

```
Enter wildcard bits:
```

Step 7 The maximum number of entries in an ACL is 20.

If the "any" option was used, no other IP addresses may be added to the list.

- To add more entries, type **y** and press **Enter**

```
Would you like to add another entry to this list? [no]:y
```

Enter up to 20 entries as described in step 5 and step 6.

- When all entries have been added, press **Enter**

```
Would you like to add another entry to this list? [no]:
```

Step 8 When all entries are added to one list, you are asked whether you would like to create another ACL. You may define up to 99 ACLs.

- To create another ACL, type **y** and press **Enter**

```
Would you like to configure another list? [no]: y
```

Enter up to 20 IP addresses in this new ACL, as described in step 5 and step 6.

- When all ACLs have been created, press **Enter.**

```
Would you like to configure another list? [no]:
```

You are now prompted to assign the desired ACLs to restrict IP and Telnet access.

Step 9 Restrict IP access to the ***SCE 1000*** by assigning the appropriate ACL.

Type the number of the ACL to be assigned to IP access and press **Enter.**

To accept the default ACL, press **Enter.**

```
Enter IP access-class [0]:
```

Step 10 Restrict Telnet access to the ***SCE 1000*** by assigning the appropriate ACL.

Type the number of the ACL to be assigned to the Telnet interface and press **Enter.**

To accept the default ACL, press **Enter.**

```
Enter Telnet access-class [0]: 2
```

EXAMPLE 1:

This example illustrates a common access control scenario. Let us assume the following:

- We want to permit every station to access the SCE on the management port (e.g. ping, SNMP polling etc.).
- We want to restrict Telnet access to only a few permitted stations.

We therefore need to create two access control lists:

- For general IP access — permit access to all IP addresses.
- For Telnet — permit access to the specified IP address, and deny to all others.

ACL #1 = permit any IP address. Assign to IP access.

ACL #2 = permit access to 10.1.1.0, 10.10.10.1, deny to all others. Assign to Telnet access.

```
Would you like to enter the Access lists configuration menu? [no]: y
Would you like to create new Access lists or modify existing lists? [no]: y
Enter ACL number: 1
Does this entry permit access? [yes]:
Enter IP address or the word ‘any’ to denote any IP address: any
This entry matches every IP address, no use in adding more entries to this list.
Would you like to configure another list? [no]: y
Enter ACL number: 2
Does this entry permit access? [yes]:
Enter IP address or the word ‘any’ to denote any IP address: 10.1.1.0
Enter wildcard bits: 0.0.0.0
Would you like to add another entry to this list? [no]:y
Does this entry permit access? [yes]:
Enter IP address or the word ‘any’ to denote any IP address: 10.10.10.1
Enter wildcard bits: 0.0.0.0
Would you like to add another entry to this list? [no]:y
Does this entry permit access? [yes]:n
Enter IP address or the word ‘any’ to denote any IP address: any
This entry matches every IP address, no use in adding more entries to this list.
Would you like to configure another list? [no]:
Enter IP access-class [0]: 1
Enter Telnet access-class [0]: 2
```

EXAMPLE 2:

This example skips the first section of the dialog (creating/modifying), and proceeds directly to assign existing ACLs.

```
Would you like to enter the Access lists configuration menu? [no]: y
Would you like to create new Access lists or modify existing lists? [no]:
Enter IP access-class [0]: 10
Enter Telnet access-class [0]: 22
```

Step 8: Configuring SNMP

Managing the ***SCE 1000*** is possible also via a Network Management System (NMS) that supports SNMP. By default, SNMP is disabled on the ***SCE 1000***.

To enable SNMP management you must configure the following basic SNMP parameters:

- SNMP traps status and managers.
- Community strings (where an SNMP community string is a text string that acts like a password to permit access to the SNMP agent on the ***SCE 1000***).

To configure SNMP parameters, complete the following steps:

Step 1 Enter the SNMP configuration menu.

```
Would you like to enter the SNMP configuration menu? [no]: y
```

Type **y** and press **Enter**.

The SNMP configuration dialog begins.

Step 2 Enable SNMP management.

Type **y** and press **Enter**.

```
Enable SNMP management? [no]: y
```

If you choose to disable SNMP management, skip the rest of this section and go to *Step 9: Configuring the Topology-Dependent Parameters* (on page 31). The rest of the dialog is not presented, as it is irrelevant when SNMP management is disabled.

Step 3 Type the SNMP GET community name and press **Enter**.

The SNMP agent that resides inside the ***SCE 1000*** will respond only to GET requests that use this community string.

```
Enter SNMP GET community name:
```

Note that there is no default for this parameter.

Step 4 Assign an access list to restrict the SNMP management stations that may use this GET community.

Type a number (1 through 99) or type "0" to permit access to all IP addresses, and press **Enter**.

```
Enter Access list number allowing access with this community string, use '0' to allow
all:
```

Step 5 The maximum number of GET communities is 20.

- To add more entries, type **y** and press **Enter**
- Would you like to add another SNMP GET community? [no]:**y**

  Enter up to 20 SNMP GET communities as described in step 3 and step 4.

- When all entries have been added, press **Enter**

```
Would you like to add another SNMP GET community? [no]:
```

Step 6 Type the SNMP SET community name and press **Enter**.

The SNMP agent that resides inside the ***SCE 1000*** will respond only to SET requests that use this community string.

```
Enter SNMP SET community name:
```

Note that there is no default for this parameter.

Step 7 Assign an access list to restrict the SNMP management stations that may use this SET community.

Type a number (1 through 99) or type "0" to permit access to all IP addresses, and press **Enter**.

```
Enter Access list number allowing access with this community string, use '0' to allow
all:
```

Step 8 The maximum number of SET communities is 20.

- To add more entries, type **y** and press **Enter**

```
Would you like to add another SNMP SET community? [no]:y
```

  Enter up to 20 SNMP SET communities as described in step 6 and step 7.

- When all entries have been added, press **Enter**

```
Would you like to add another SNMP SET community? [no]:
```

Step 9 Enter the SNMP trap managers menu.

```
Would you like to configure SNMP trap managers? [no]: y
```

Type **y** and press **Enter**.

The SNMP trap managers dialog begins.

If you choose not to configure SNMP trap managers, the dialog skips to the authentication failure trap status. (See step 14.)

Step 10 Type the trap manager IP address and press **Enter**.

```
Enter SNMP trap manager IP address:
```

Note that there is no default for this parameter.

Step 11 Type the trap manager community string and press **Enter**.

Note that there is no default for this parameter.

```
Enter SNMP trap manager community string:
```

Step 12 Type the number of the trap manager SNMP version (1 or 2c) and press **Enter**

Note that there is no default for this parameter.

```
Enter trap manager SNMP version:
```

Step 13 The maximum number of trap managers is 20.

- To add more entries, type **y** and press **Enter**

```
Would you like to add another SNMP trap manager? [no]:y
```

Enter up to 20 trap managers as described in step 10 through step 12.

- When all entries have been added, press **Enter**

```
Would you like to add another SNMP trap manager? [no]:
```

Step 14 Configure the Authentication Failure trap status.

- To disable the Authentication Failure trap, press **Enter**.
- To enable the Authentication Failure trap, type **y** and press **Enter**.

```
Enable the ‘Authentication Failure’ trap [no]:
```

Step 15 Configure the SCE enterprise trap status.

- To disable the SCE enterprise traps, type **n** press **Enter**.
- To enable the SCE enterprise traps, type **y** and press **Enter**.

```
Enable the SCE enterprise traps []:
```

Step 16 Type the name of the system administrator and press **Enter.**

Note that there is no default for this parameter.

```
Enter system administrator contact name []:
```

EXAMPLE:

Following is a sample SNMP configuration, configuring one trap manager, one GET community, and one SET community, and enabling the authentication failure trap, as well as all enterprise traps.

```
Would you like to enter the SNMP configuration menu? [no]: y
Enable SNMP management? [no]: y
Enter SNMP GET community name[]: public
Enter Access list number allowing access with this community string, use '0' to allow
all: 0
Would you like to add another SNMP GET community? [no]:
Enter SNMP SET community name[]: private
Enter Access list number allowing access with this community string, use '0' to allow
all: 2
Would you like to add another SNMP SET community? [no]:
Would you like to configure SNMP trap managers? [no]: y
Enter SNMP trap manager IP address: 10.1.1.253
Enter SNMP trap manager community string: public
Enter trap manager SNMP version: 2c
Would you like to add another SNMP trap manager? [no]:
Enable the 'Authentication Failure' trap [no]: y
Enable SCE enterprise traps []: y
Enter system administrator contact name []: John Smith
```

Step 9: Configuring the Topology-Dependent Parameters

The topology configuration menu is a series of guided questions relating to the deployment of the ***SCE 1000*** in the network and its mode of operation. Values for the parameters are configured based on the user answers.

The correct value for each parameter must be ascertained before configuring the system to make sure that the system will function in the desired manner. (See Topology for a comprehensive discussion of topology and the related parameters.)

There are three topology-related parameters:

- **Connection mode** — Can be either Inline or Receive-only, depending on the physical installation of the ***SCE 1000***.
- **Bypass state when the *SCE 1000* is not operational (on-failure)** — This parameter determines whether the system cuts the traffic or bypasses it when the ***SCE 1000*** has failed.
- **Status after reboot caused by fatal error or abnormal shutdown** — This parameter determines whether the ***SCE 1000*** returns to normal operational state after a failure.

The procedure described below is a hypothetical presentation of all the questions in the topology configuration. In actual practice, it is impossible for all questions to be presented in any one configuration, as this part of the dialog is not linear like the other sections, but branches depending on the parameter values entered.

Study the examples that follow to understand the procedure for various topologies.

To configure topology dependent parameters, complete the following steps:

Step 1 Enter the topology configuration menu.

```
Would you like to enter the Topology configuration menu? [no]: y
```

Type **y** and press **Enter**.

The topology configuration dialog begins.

Step 2 Specify the connection mode.

- To define **inline** connection mode, press **Enter**.

- To define **receive-only** connection mode, type **2** and press **Enter**.

```
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]:
```

Step 3 Specify the On-failure link behavior.

- To specify **Bypass**, press **Enter**.
- To specify **Cutoff**, type **2** and press **Enter**.

```
Enter On-failure behavior:
1- bypass
2- cutoff
Enter your choice [1]:
```

Step 4 Specify the admin status of the ***SCE 1000*** after abnormal boot.

- To specify **Not-Operational** status after abnormal boot, press **Enter**.
- To specify **Operational** status after abnormal boot, type **1** and press **Enter**.

```
Enter admin status of the SCe after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:
```

The following examples present the procedure for configuring the topology-related parameters for various topologies. Refer the Topology Configuration Summary Table for a summary of appropriate values for the parameters for each topology.

EXAMPLE 1:

Following is a sample topology configuration for a topology using an external switch.

All other parameter values are automatically assigned by the system as follows:

- Link bypass mode on-failure — Bypass
- Admin status of the SCE after abnormal boot — Operational

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
```

EXAMPLE 2:

Following is a sample topology configuration for a non-redundant bump-in-the-wire (inline) topology. All values are the system default values, so it is not necessary to type in the response. Simply press enter at each line.

- Connection mode — Inline
- For a non-redundant topology, link bypass on-failure should be Bypass, so that traffic continues to flow through the link.
- After operation of the system resumes, and the ***SCE 1000*** reboots, the ***SCE 1000*** will resume operation. (Admin status after abnormal reboot is Operational.)

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]:
Enter On-failure behavior:
1- Bypass
2- Cutoff
Enter your choice [1]:
Enter admin status of the SCe after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:

Data collection for the system configuration is completed.
```

EXAMPLE 3:

Following is a sample topology configuration for a redundant inline topology.

- Connection mode — Inline
- For a redundant topology, link bypass on-failure should be Cutoff, so that operation switches to the backup link.
- After operation of the system resumes, and the ***SCE 1000*** reboots, the ***SCE 1000*** will resume operation. (Admin status after abnormal reboot is Operational.)

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
Enter On-failure behavior:
1- Bypass
2- Cutoff
Enter your choice [1]:2
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:

Data collection for the system configuration is completed.
```

Step 10: Completing and Saving the Configuration

When you have completed the entire configuration, the system checks for errors. If errors are found, a warning message appears. When the configuration is error-free, you may apply and save it.

To complete and save the configuration, complete the following steps:

Step 1 The system informs you that data collection is complete.

It is recommended that you view the entire new configuration before it is applied.

Type **y** and press **Enter**.

Note that there is no default.

If there are no errors, go to step 3.

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]: y
```

Step 2 If any errors are detected, you may choose to view them.

Press **Enter**.

```
Found errors in the new configuration, would you like to view them? [yes]:
The following errors were found:
Warning - RDR formatter destination 10.1.1.1 is not allowed in the IP access-class.
```

Step 3 You are asked whether to apply and save the configuration.

```
Apply and Save this configuration? [yes/no]:
```

- To apply and save the configuration, type **y** and press **Enter**.
- To abort the setup procedure without applying or saving the configuration (recommended if there are errors), type **n** and press **Enter**.

  ```
  Setup procedure aborted, no configuration changes made.
  ```

  If the setup is aborted, the dialog is ended.

Step 4 If there are no errors, the system requests confirmation of either a yes or no answer, in order to prevent mistakes.

Type the appropriate answer (y or n) and press **Enter**.

```
The running configuration would be overwritten by the changes you have just entered, are
you sure? [yes/no]:
```

The selected action is carried out by the system.

- If the apply and save action is not confirmed (**no**), the setup is aborted.

  ```
  Setup procedure aborted, no configuration changes made.
  ```

- If the apply and save action is confirmed (**yes**), the configuration is applied and saved.

  ```
  The new running configuration will be saved to the startup configuration.
  ```

Step 5 If the configuration was applied and saved, you may also save it to a file at a remote station.

```
Do you want to save a copy of the startup configuration file in a remote station? [no]:
```

To save the configuration to a remote station, type **y** and press **Enter**.

The system will ask for FTP path:

```
Enter a full FTP path of the remote destination:
```

Step 6 The system informs you that the configuration is complete.

```
Committing configuration...

Configuration completed successfully.

Saving configuration...
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...

Done!
```

This completes the procedures for initial configuration of the ***SCE 1000*** platform.

EXAMPLE 1:

Following is an example of a configuration that the user aborted due to errors detected in the configuration.

Note that no confirmation is requested for the decision to abort the setup. Had there been no errors, confirmation would have been requested before aborting.

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]: n
Found errors in the new configuration, would you like to view them? [yes]: y
The following errors were found:
Warning - RDR formatter destination 10.1.1.1 is not allowed in the IP access-class.
Warning - default Gateway 10.1.1.1 is not allowed in the IP access-class.
Warning - IP Access list (1) conflicts with Telnet Access list (2) as follows:
Access list 2 permits all addresses while Access list 1 denies it.
Apply and Save this configuration? [yes/no]: n

Setup procedure aborted, no configuration changes made.
```

EXAMPLE 2:

Following is an example of a configuration that was applied and saved to the startup configuration as well as to an FTP site.

Although not demonstrated in this example, it is recommended that you always view the configuration before applying it.

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]:
Apply and Save this configuration? [yes/no]: y

(New configuration would be displayed here)

The running configuration would be overwritten by the changes you have just entered, are
you sure? [yes/no]:y

The new running configuration will be saved to the startup configuration.
Do you want to save a copy of the startup configuration file in a remote station? [no]:y
Enter a full FTP path of the remote destination:
ftp://vk:vk@10.1.1.253/h:/copyofstartup.txt
Committing configuration...

Configuration completed successfully.

Saving configuration...
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...

Done!
```

EXAMPLE 3:

Following is an example of a configuration that was aborted, although no errors were detected.

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]:
Apply and Save this configuration? [yes/no]: n
The changes you have just entered would be discarded, are you sure? [yes/no]:y


Setup procedure aborted, no configuration changes made.
```

Connect the Management Interface

Figure 13: Cabling the Management Port

Note By default, the management port is configured to auto-negotiation enabled.

The ***SCE 1000*** has two management ports, labeled Mng1 and Mng 2. Use the Mng 1 port.

Step 1 Plug the Ethernet cable provided (with attached RJ-45 connector) into the Mng 1 port on the front panel of the ***SCE 1000***.

Step 2 Connect the other end of the Ethernet cable into your management network.

The Link LED on the ***SCE 1000*** management port should light up.

Step 3 Test connectivity. From the host that you intend to use for remote management, ping to the ***SCE 1000*** by typing **ping** and the ***SCE 1000*** IP address, and pressing **Enter** (see the example, below).

This verifies that an active connection exists between the specified station and the management port.

EXAMPLE:

The following example displays a typical ping response where the target IP address is 10.1.1.201.

```
C:\>ping 10.1.1.201
pinging 10.1.1.201 ...
PING 10.1.1.201: 56 data bytes
64 bytes from host (10.1.1.201): icmp_seq=0. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=1. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=2. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=3. time=0. ms
----10.1.1.201 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

6 Cable the Line Ports

This chapter provides instructions for cabling the Gigabit Ethernet ports and for configuring Gigabit Ethernet (GBE) interface parameters.

Note When installing an External Optical Bypass module, the ***SCE 1000*** line ports are connected to the module. See Appendix A in the *SCE 1000 2xGBE Installation and Configuration Guide* for complete instructions.

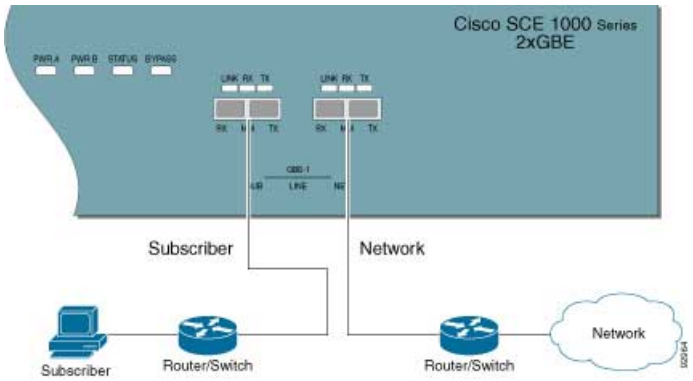
Cabling Diagrams

Before beginning, find the appropriate cabling diagram for the topology in your installation:

- Single ***SCE 1000*** topologies
  - *Single Link: Inline Topology* (on page 37)
  - *Single Link: Receive-only Topology* (on page 38)

Single Link: Inline Topology

Figure 14: Bump-in-the-Wire Installation



In the inline or bump-in-the-wire topology, illustrated in the diagram above, the ***SCE 1000*** resides physically on the data link between the subscriber side, usually either a BRAS (in DSL access), a PDSN (in wireless access), a CMTS (in the Cable access), or a switch or router aggregator (in other topologies), and the network side, usually a router or layer 3 switch network element. This is the inline topology, providing both traffic monitoring and control capabilities.

In this topology, all the traffic of the ***SCE 1000*** is deployed as a transparent layer2 overlay on the customer's existing network.

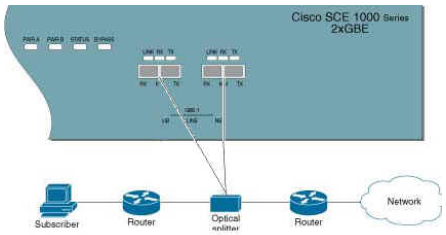
Single Link: Receive-only Topology

In this topology, an external optical splitter resides physically on the GBE link between the subscriber side and the network side. The external splitter is connected to the ***SCE 1000*** via Rx links only.

In this topology, the traffic passes through the external splitter, which splits traffic to the ***SCE 1000***. The ***SCE 1000***, therefore, is in receive-only topology, having only traffic monitoring capabilities.

Note Receive-only topologies can also be implemented using a switch. Such a switch must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN-ports destinations.

Figure 15: External Splitting Topology



Configure GigabitEthernet Auto-Negotiation

By default, the ***SCE 1000*** GBE line interface ports are configured with auto-negotiation disabled.

Note Auto-negotiation must be disabled when the ***SCE 1000*** is deployed via an external optical splitter (receive-only topology)

.

Note If you change any parameters, you must save the new configuration settings.
Type **`copy running-config startup-config`**, and press **Enter**

Step 1 To enter the Global Configuration Mode, at the ***SCE 1000***# prompt, type **configure** and press **Enter**.

The ***SCE 1000***(config)# prompt appears.

Step 2 To enter the desired GBE port interface, type **interface GigabitEthernet 0/***`portnumber`*, and press **Enter**, where *`portnumber`* is the number of the selected port (1 or 2).

The ***SCE 1000***(config if)# prompt appears.

Step 3 Type **auto-negotiate** and press **Enter**.

The ***SCE 1000***(config if)# prompt appears.

Step 4 To return to Global Configuration Mode, type **exit** and press **Enter**.

The ***SCE 1000***(config)# prompt appears.

Repeat this procedure to configure auto-negotiation for the other GBE port interfaces as needed.

Connect the GBE Line Interface Ports

Figure 16: Cabling the GBE Interface

Refer to *Cabling Diagrams* (on page 37) to find the appropriate cabling diagram for the topology of your system for the specific connections required.

The following table presents the fiber specifications. The ***SCE 1000*** may be ordered with either Multimode or Single Mode transceivers The transceiver type is indicated on the front panel under the ports. Note that both transceivers on any individual ***SCE 1000*** are the same, either 850nm Multimode OR 1310 Single Mode.

Table 6-1 Fiber Specifications

SCE Model	Transceiver	Transmit Power	Receive Power	Typical (Max.) Distance
SCE 1000 2xGBE MM	850nm Multimode	–9.5 to –4 dBm	–17 to 0 dBm	• 750m for 50µm Core Diameter MMF • 400m for 62.5µm Core Diameter MMF
SCE 1000 2xGBE SM	1310nm FRP laser Single Mode	–9.5 to –3 dBm	–20 to 3 dBm	10 km for 9.0µm Core Diameter SMF

Step 1 Plug the specified fiber optic cable (see table above) into the appropriate GBE port on the front panel of the ***SCE 1000***.

Step 2 Verify that the link LED is green.

If the link LED does not light, try removing the network cable plug and reinserting it firmly into the module socket.

7 Completing the Installation

This section discusses how to verify link connectivity and how to install a Service Control application.

Examining the LEDs

The GBE Link LED must be green in order to verify that an active connection exists.

The GBE Rx and Tx LEDs (if flashing green) indicate that traffic is being received or transmitted by the ***SCE 1000*** platform, respectively.

Note that in an inline topology, the Rx and Tx LEDs indicate that packets are being received/transmitted by the ***SCE 1000*** platform.

In optical splitter topologies, the Rx LEDs are the sole indicators. The Tx LEDs do not “blink”, since the Tx is not connected to the port in this topology.

Final Tests

The procedures for performing the final tests to verify that the ***SCE 1000*** is functioning properly are explained in the following sections:

- *Verifying Operational Status* (on page 40)
- *Viewing the User Log Counters* (on page 41)

Verifying Operational Status

After all the ports are connected, verify that the ***SCE 1000*** is not in a Warning state.

To verify that the ***SCE 1000*** is not in a warning state, complete the following steps:

Step 1 On the ***SCE 1000*** Front panel, examine that the Status LED is flashing green.

Step 2 To display the operation status of the system, at the ***SCE 1000***# prompt, type **`show system operation-status`** and press **Enter**.

A message displaying the operation status of the system appears. If the system is operating in order, the following message appears:

```
System Operation status is Operational.
```

EXAMPLE:

The following example displays a sample output where the LEDs appear red/orange:

```
SCE 1000#show system operation-status
System Operation status is Operational
```

Viewing the User Log Counters

View the user log for errors that occurred during the installation process.

To display the user log device counters, complete the following steps:

At the ***SCE 1000***# prompt, type **`show logger device User-File-Log counters`** and press **Enter**.

EXAMPLE:

The following example shows the current User-File-Log device counters.

```
SCE 1000#show logger device user-file-log counters
Logger device User-File-Log counters:
Total info messages: 1
Total warning messages: 0
Total error messages: 0
Total fatal messages: 0
```

If there are “Total error messages” or “Total fatal messages”, use the **`show logger device User-File-Log`** command to display details about the errors.

Viewing Configuration

When you enter configuration commands, it immediately effects the SCE platform operation and configuration. This configuration, referred to as the *`running-config`*, is saved in the SCE platform volatile memory and is effective while the SCE platform is up. After reboot, the SCE platform loads the *`startup-config`*, which includes the non-default configuration as saved by the user, into the *`running-config`*.

The SCE platform provides commands for:

- Viewing the running configuration
- Viewing the startup configuration

After configuring the SCE platform, you may query for the running configuration using the command **`show running-config`**. This command displays the non-default running configuration. To view all SCE platform running configuration, whether it is the default or not, you may use the option **`all-data`** in the **`show running-config`** command.

To view the running configuration, complete the following steps:

At the ***SCE 1000***# prompt, type **`show running-config`**.

The system shows the running configuration.

```
SCE 1000#show running-config
#This is a general configuration file (running-config).
#Created on 15:50:56  CET  MON  December  11  2005
#cli-type 1
#version 1

clock timezone CET 1
snmp-server community “public” ro
snmp-server host 10.1.1.253 traps version 1 “public”
interface LineCard 0
connection-mode active
no silent
no shutdown
flow-aging default-timeout UDP 60
interface FastEthernet 0/0
ip address 10.1.5.109 255.255.0.0
interface FastEthernet 0/1
interface FastEthernet 0/2
exit
line vty 0 4
no timeout
exit
SCE 1000#
```

One of the useful show commands is the **`show version`** command. This command displays global static information on the ***SCE 1000*** as software and hardware version, image build time, system uptime, last open packages names and information on the SLI application assigned.

To show the version information for the ***SCE 1000*** software and hardware, complete the following steps:

At the ***SCE 1000***# prompt, type **`show version`**.

The system shows the version information.

```
SCE 1000#show version
System version: Version 3.0.0 Build 240
Build time: Jan 11 2006, 07:34:47
Software version is: Version 2.5.2 Build 240
Hardware information is:
rx            : 0x0075
dp            : 0x1808
tx            : 0x1708
ff            : 0x0077
cls           : 0x1721
cpld          : 0x0025
Lic           : 0x0176
rev           : G001
Bootrom       : 2.1.0
L2 cache      : Samsung 0.5
lic type      : MFE
optic mode    :
Part number: 53AA-BXC1-AAAA
Revision: A02A
Software revision: G001
Serial number: 043P6982
Power Supply type: AC

SML Application information is:
Application file: /tffs0/temp.sli
Application name:
Application help:
Original source file: H:\work\Emb\jrt\V2.5\sml\actions\drop\drop_basic_anyflow.san
Compilation date: Wed, December 21 2005 at 21:25:21
Compiler version: SANc v2.50 Build 32 gcc_codelets=true built on: Tue December 23 2005
09:51:57 AM.;SME plugin v1.1
Default capacity option used.


Logger status: Enabled


Platform: SCE 2000 - 4xFE
Management agent interface version: SCE Agent 3.0.0 Build 18
Software package file: ftp://vk:vk@10.1.8.22/P:/EMB/LatestVersion/3.0.0/se1000.pkg

SCE 2000 uptime is 21 minutes, 37 seconds
SCE 1000#
```

Another useful show command is the **show system-uptime** command. This command displays information similar to the last line above, which indicates how long the system has been running since the last reboot.

To show the system uptime for the SCE platform software and hardware, complete the following steps:

At the ***SCE 1000***# prompt, type **show system-uptime.**

The system shows how long the system has been running since the last reboot.

```
SCE 1000#show system-uptime
SCE 1000 uptime is 21 minutes, 37 seconds
SCE 1000#
```

Saving the Configuration Settings

When you make changes to the current running configuration and you want those changes to continue to be valid when the system restarts, you must save the changes before leaving the management session, that is, you must save the running configuration to the startup configuration file.

The SCE platform provides multiple interfaces for the purpose of configuration and management. All interfaces supply an API to the same database of the SCE platform and any configuration made through one interface is reflected through all interfaces. Furthermore, when saving the running configuration to the startup configuration from any management interface, all configuration settings are saved regardless of the management interface used to set the configuration.

To save configuration changes, complete the following steps:

Step 1 At the ***SCE 1000***# prompt, type **show running-config** to view the running configuration.

The running configuration is displayed.

Step 2 Check the displayed configuration to make sure that it is set the way you want. If not, make the changes you want before saving.

Step 3 Type **copy running-config startup-config**.

The system saves all running configuration information to the configuration file, which is used when the system reboots.

The configuration file holds all information that is different from the system default in a file called config.txt located in the directory: tffs0:system.

EXAMPLE:

The following example shows the running configuration file.

```
SCE 1000#show running-config
#This is a general configuration file (running-config).
#Created on 15:50:56  CET  MON  February  11  2002
#cli-type 1
#version 1

clock timezone CET 1
snmp-server community “public” ro
snmp-server host 10.1.1.253 traps version 1 “public”
interface LineCard 0
connection-mode active
no silent
no shutdown
flow-aging default-timeout UDP 60
interface FastEthernet 0/0
ip address 10.1.5.109 255.255.0.0
interface FastEthernet 0/1

interface FastEthernet 0/2

exit
line vty 0 4
no timeout
exit
SCE 1000#
SCE 1000#copy running-config startup-config
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
SCE 1000#
```

For backup purposes, the old startup-config file is saved under the directory: `tffs0:system/prevconf`. Refer to Recovering a Previous Configuration for an explanation on how to recover previous configuration.

To remove a configuration command from the running-config, use the no form of the command.

EXAMPLE:

The following example illustrates how to remove all DNS settings from the running configuration.

```
SCE 1000(config)#no ip name-server
SCE 1000(config)#
```

Performing Complex Configurations

After you have installed your ***SCE 1000*** platform hardware, checked all external connections, turned on the system power, allowed the system to boot up, and performed the initial system configuration, you might need to perform more complex configurations, which are beyond the scope of this publication.

For further information on system and interface configuration, refer to the following documents:

- *Cisco Service Control Engine (SCE) Software Configuration Guide*
- *Cisco Service Control Engine (SCE) CLI Command Reference*

Loading and Activating a Service Control Application

The ***SCE 1000*** platform provides the basic functionalities of Service Control analysis and enforcement. A Service Control solution requires that a Service Control application be loaded into the platform, to take advantage of the unique SCE platform capabilities.

Loading and activating an application includes the following stages:

- Downloading the application provided as an SLI file to the ***SCE 1000*** disk.
- Activating the application.
- Configuring the application.

The detailed procedure of how to perform these operations is not specified and described in this manual. For further details, refer to the following documentation:

- *Service Control Application Suite for Broadband User Guide*
- *Service Control Application Suite for Broadband Reference Guide*

8 Troubleshoot Startup Problems

SCE 1000 Operational Status

The following table lists the operational states of the ***SCE 1000***. The Status LED on the ***SCE 1000*** Front Panel reflects the current ***SCE 1000*** operational status. The operational status can be displayed using CLI command **`show system operation-status`**.

Table 8-1 SCE 1000 **Operational States**

SCE 1000 **Operational Status**	**Description**	**Status LED State**
Booting	Initial state after reset	Orange
Operational	***SCE 1000*** becomes operational after completing the following process: • Boot is completed • Power self-tests are completed without failure • Platform configuration is applied	Flashing green
Warning	***SCE 1000*** is fully operational (as above) but one of the following occurred: • Line ports (GBE ports) to the link are down • Management port link is down • Temperature raised above threshold • Voltage not in required range • Fans problem • Power supply problem • Insufficient space on the disk Note: If the condition that caused the ***SCE 1000*** to be in Warning state is resolved (for example, link is up) the ***SCE 1000*** reverts to Operational state.	Flashing orange
Failure	System is in Failure state after Boot due to one of the following conditions: • Power on test failure • Three abnormal reboots in less than 20 minutes • Platform configured to enter Failure mode consequent to failure-induced reboot (this is configurable using CLI command) Note: Depending on the cause of failure, the management interface and the platform configuration may or may not be active/available.	Red

Identifying Startup Problems

Startup problems are commonly due to the source power or to a poor cable connection.

When you start up the ***SCE 1000*** platform for the first time, you should observe the startup sequence described in the Starting the ***SCE 1000*** Platform. This section contains a more detailed description of the normal startup sequence and describes the steps to take if the system does not perform that sequence as expected. LEDs indicate all system states in the startup sequence. By checking the state of the LEDs, you can determine when and where the system failed in the startup sequence. Use the following descriptions to isolate the problem to a subsystem, and then proceed to the appropriate sections to try to resolve the problem.

When you start up the system by turning on the power supply switch, the following should occur:

- You should immediately hear the fans operating.
- When all LEDs come on to indicate that the system has booted successfully, the initial system banner should be displayed on the console screen. If it is not displayed, see *Connecting the Local Console* (on page 15) to verify that the terminal is set correctly and that it is properly connected to the console port.
- If the banner is displayed, but the Status LED is flashing orange, indicating a warning state, check the user log:

  At the prompt, type: **`more user log`**

  If any of the following warning messages appear, turn the ***SCE 1000*** platform off and call technical support.

  - "voltage problem:"
  - "fans problem"
  - "abnormal raise in interior temperature:"

  If the following warning message appears, delete unneeded files from the disk.

  - “insufficient disk space:”

CLI Commands for Troubleshooting

Use the following commands to provide information to help you troubleshoot installation of your ***SCE 1000*** platform. Refer to *Cisco Service Control Engine (SCE) Software Configuration Guide* or the *Cisco Service Control Engine (SCE) CLI Command Reference* for more information.

Note Remember that if the management interface is not operational, you should connect the ***SCE 1000*** platform to a local console so that you can enter CLI commands for troubleshooting.

- **Troubleshooting firmware package installation:**
  - **`Boot system <filename>`** — Specifies and verifies the package file to be installed. Error messages or other output identify problems with the package file.

    Following is a sample output from the **`Boot system`** command.

```
SCE 1000(config)#boot system ftp://vk:vk@10.1.1.230/downloads/SENum.pkg.pkg
Verifying package file SENum.pkg.pkg…
Package file verified OK.
```

- **Troubleshooting the management subsystem:**
  - show interface **`Mng`** — Displays IP address and auto-negotiation information for the management interfaces.

Following is a sample output from the show interface **Mng** command.

```
ip address: 10.1.6.145
subnet mask: 255.255.0.0
Configured speed: auto, configured duplex: auto
AutoNegotiation is On, link is Up, actual speed: 100, actual duplex: half
```

- show ip default-gateway — Displays the IP address of the configured default gateway.

  Following is a sample output from the show ip default-gateway command.

```
Default gateway: 10.1.1.1
```

- show ip route — Displays the entire routing table and the destination of last resort (default-gateway).

  Following is a sample output from the show ip route command.

```
gateway of last resort is        10.1.1.1
```

- show access-lists — Shows all access-lists or a specific access list.

  Following is a sample output from the show access-lists command.

```
Standard IP access list 1
    Permit 10.1.1.0, wildcard bits 0.0.0.255
    deny   any
```

- show telnet — Displays the status of the telnet server daemon (**status**) or any active Telnet sessions (**sessions**).

  Following is a sample output from the show telnet command.

```
show telnet sessions
There is 1 active telnet session:

Index | Source
===============
 0    | 10.1.1.201
show telnet status
Telnet deamon is enabled.
```

- show line vty timeout — Shows the timeout configured for Telnet sessions.

  Following is a sample output from the show line vty timeout command.

```
Timeout is 30 minutes
```

- **Troubleshooting the link interface subsystem:**
  - show interface GigabitEthernet **0/# —** Displays information for a specific GBE Interface.

    Following is a sample output from the show interface command.

```
ip address: 10.1.6.145
subnet mask: 255.255.0.0
Configured duplex: auto
AutoNegotiation is On, link is Up, actual duplex: half
```

- show interface **GigabitEthernet 0/#** counters — Displays the values of counters of a GBE interface.

  Following is a sample output from the show interface **counters** command.

```
In total octets: 191520
In good unicast packets: 560
In good multicast packets: 0
In good broadcast packets: 0
In packets discarded: 0
In packets with CRC/Alignment error: 0
In undersized packets: 0
In oversized packets: 0
Out total octets: 0
Out unicast packets: 0
Out non unicast packets: 0
Out packets discarded: 0
```

Refer to The User Log for an explanation of commands related to the user log.

9 Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page 51) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page 51), go to the following website:

http://tools.cisco.com/RPF/register/register.do

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.