CHAPTER 5

Connecting the Management Interfaces and Performing Initial System Configuration

Revised: April 19, 2010, OL-21094-02

Introduction

This chapter 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.

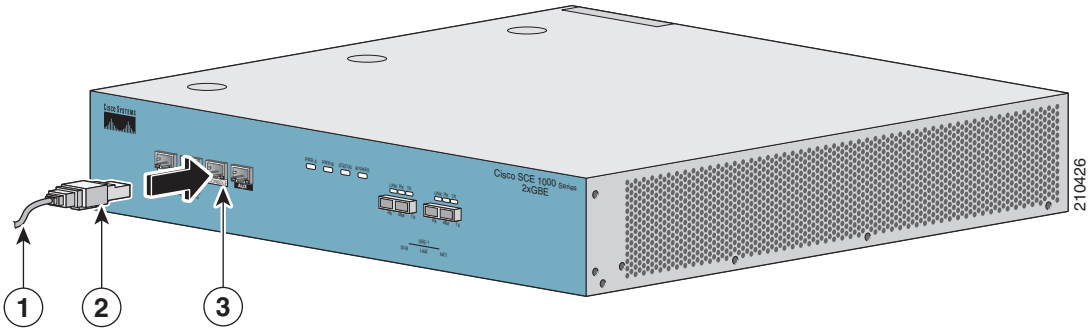
Additionally, this chapter contains instructions for cabling the Fast Ethernet Management interfaces.

How to Set Up the Local Console

Even if you will be managing the SCE 1000 from a remote location, 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 (Figure 5-1).

This section provides instructions for setting up your local terminal at your workstation, to enable you to perform the initial system configuration of the SCE 1000 system using the setup utility.

Figure 5-1 Connecting the Local Console to the SCE 1000 CON Port



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 <SKIP> serial cable provided with the SCE 1000 into the CON port on the front panel of the SCE 1000.

Make sure that you push on the RJ-45 connector (attached to the <SKIP> serial cable) until you hear a "click", which indicates that the connector is fully inserted and secured in the receptacle. Gently pull on the plug to confirm whether the plug is locked into the socket.

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 Make sure the local terminal is configured as a VT-100 terminal, according to the fixed SCE 1000 CON port parameters.

Step 4 Press Enter several times until the Cisco logo appears on the local terminal and the setup configuration

Step 5 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 6 Type **y** and press Enter. The system configuration dialog begins.

Perform the Initial System Configuration

Initial System Configuration

Setup Command

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.

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 SCE 2000 and SCE 1000 Software Configuration Guide*.

Setup Command Parameters

Table 5-1 lists the 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. Maximum 20 characters.
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.
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)
TCP port number	TCP port number of the RDR-formatter destination
Parameter	Definition
Access Control Lists	

Table 5-1 Setup Command Parameters (continued)

Parameter	Definition
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 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 (maximum 20)	Trap manager IP address, community string, and SNMP version.
Authentication Failure trap status	Sets the status of the Authentication Failure traps.
enterprise traps status	Sets the status of the enterprise traps.
system administrator	Name of the system administrator.
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.

Step 1 Configure the IP address.

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 Configure the subnet mask.

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 Configure the default gateway.

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 maximum length is 20 characters.

The default hostname is SCE 1000.

Step 1 Specify the hostname for the SCE platform.

The default 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”.

Step 1 Configure the User password

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 Configure the Admin password.

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 Configure the Root password.

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 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.

Step 1 Enter the time settings menu.

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

Type y and press Enter.

Step 2 Configure the time zone name.

Type the time zone abbreviation and press Enter.

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

Step 3 Specify the offset from UTC.

Type the minutes offset from UTC and press Enter.

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

Step 4 Confirm the local time and date.

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]:
```

- If the time and date are correct, press Enter and go to Step 5: Configuring the DNS Settings.
- 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 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 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, page 5-11.

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.

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

Step 8 Specify 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.

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. 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 Configure the primary domain name server.

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 Configure any additional domain name servers.

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 Step 6 Exit the dialog.

When IP addresses for all servers have been entered, exit the dialog by pressing press 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.

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 Specify the IP address of the RDR-formatter destination.

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 Specify the TCP port number of the RDR-formatter destination.

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)

Information About Access Control Lists

Configuring 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:

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.

2. Assign the ACLs to the appropriate management interface.

   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 Table 5-2 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 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.

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

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, page 5-14.)

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
```

Examples

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 platform on the management port (for example ping, SNMP polling, and so forth).
- 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).

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. The rest of the dialog is not presented, as it is irrelevant when SNMP management is disabled.

Step 3 Configure the SNMP GET community.

a. 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.

b. 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 4 Configure additional GET communities.

The maximum number of GET communities is 20.

a. To add more entries, do not accept the default:

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

Type y and press Enter.

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

c. When all entries have been added, accept the default:

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

Press Enter to accept.

Step 5 Configure the SNMP SET community.

a. 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.

b. 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 6 Configure additional SET communities.

a. To add more entries, do not accept the default:

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

Type y and press Enter.

b. Enter up to 20 SNMP SET communities as described in step 5.

c. When all entries have been added, accept the default:

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

Press Enter to accept.

Step 7 Configure the SNMP trap managers.

a. 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 9.)

b. Configure the trap manager IP address

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

Type the trap manager community string and press Enter.

Note that there is no default for this parameter.

c. Configure the trap manager community string

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

Type the trap manager community string and press Enter.

Note that there is no default for this parameter.

d. Configure the trap manager SNMP version.

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

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

Note that there is no default for this parameter.

Step 8 Configure additional trap managers.

The maximum number of trap managers is 20.

a. To add more entries do not accept the default:

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

Type y and press Enter.

b. Enter up to 20 trap managers as described in step 7.

c. When all entries have been added, accept the default:

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

Press Enter to accept.

Step 9 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 10 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 11 Specify the system administrator.

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

- About the Topology-Dependent Parameters
- Examples

About 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 Information About 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.

Step 1 Enter the topology configuration menu.

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

- Enter your password if prompted.

  Type y and press Enter.

  Enters the topology configuration dialog.

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]:
```

Examples

The following examples present the procedure for configuring the topology-related parameters for various topologies. Refer to Information About Topology for a summary of appropriate values for the parameters for each topology.

- Example 1:, page 5-22
- Example 2:, page 5-22
- Example 3:, page 5-23

Example 1:

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

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

All other parameter values are automatically assigned by the system.

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 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 Review the new configuration.

The system informs you that data collection is complete.

We recommend 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 View errors (if any).

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 Apply and save the configuration.

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.

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

If the setup is aborted, the dialog is ended.

Step 4 Confirm saving and applying the configuration.

If there are no errors, the system requests confirmation of either a yes or no answer, 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.
```

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 Save the configuration to a remote location.

If the configuration was applied and saved, you may also save a backup copy 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 This completes the procedures for initial configuration of the SCE 1000 platform.

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!
```

Examples

- Example 1:, page 5-25
- Example 2:, page 5-25
- Example 3:, page 5-25

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.
```

Connecting the Management Interface

The SCE platform is equipped with two RJ-45 management (MNG) ports. These ports provide access from a remote management console to the SCE platform via a LAN. The two management ports provide the possibility for a redundant management interface, thus ensuring management access to the SCE platform even if there is a failure in one of the management links.

If only one management port is used, the desired port is simply connected directly to the LAN. If both management ports are used, they must both be connected to the management console via a switch. In this way, the IP address of the MNG port is always the same, regardless of which physical port is currently active.

The procedures for cabling the management port and testing connectivity between the SCE 1000 and the remote management host are explained in the following sections:

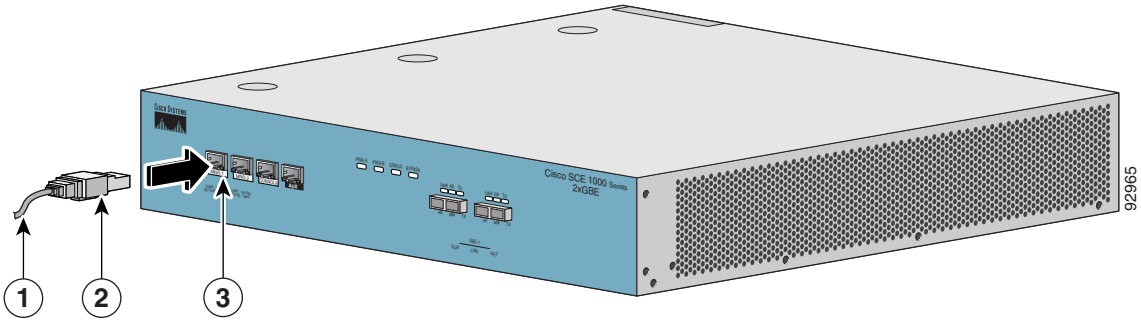
- How to Cable the Management Port
- How to Verify Management Interface Connectivity

How to Cable the Management Port

The SCE 1000 has two management ports, labeled Mng1 and Mng 2.

Step 1 Take the Ethernet cable provided (with attached RJ-45 connector) and plug it into the desired MNG port on the front panel of the SCE 1000, as shown in Figure 5-2.

Figure 5-2 Cabling the Management Port



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

- If only one management port is used — connect the port directly to the LAN.
- If both management ports are used — connect both ports to the LAN via a switch.

Make sure that you push on the RJ-45 connector attached to the cable until you hear a click, which indicates that the connector is fully inserted and secured in the receptacle. Gently pull on the plug to confirm whether the plug is locked into the socket.

If the Link LED on the SCE 1000 management port does not light, try removing the cable and reinserting it firmly into the module socket. To disconnect the plug from the socket, press down on the raised portion on top of the plug, releasing the latch. You should hear an audible click indicating the latch has released. Carefully pull the plug out of the socket.

If the management port Link LED on the SCE 1000 still does not light, verify that the cable is connected correctly to the appropriate network element on its second end.

How to Verify Management Interface Connectivity

If the SCE 1000 platform has been powered up, test now to verify that connectivity has been established between the SCE 1000 and the remote management host. If the SCE 1000 platform is not powered up, perform this step after starting the SCE 1000 platform.

Step 1 After you connect the cable to the appropriate Mng port and to your network, check the relevant Mng port LEDS.

There are two Mng LEDs—Link/Active, and 10/100/1000 (refer to Front Panel).

At this point, check that the Link/Active LED is green.

The state of the 10/100/1000 LED will depend on the Ethernet network settings.

Green indicates 100 Mbps and ‘Off’ indicates 10 Mbps.

Step 2 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).

Note Please note that only above, is performed from the remote management host (Mng port connection).

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

The ping program sends an echo request packet to an IP address and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

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
```