CHAPTER 5

Connecting the Management Interfaces and Performing Initial System Configuration

Revised: December 24, 2010, OL-21096-02

Introduction

This chapter explains how to connect the SCE 2000 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.

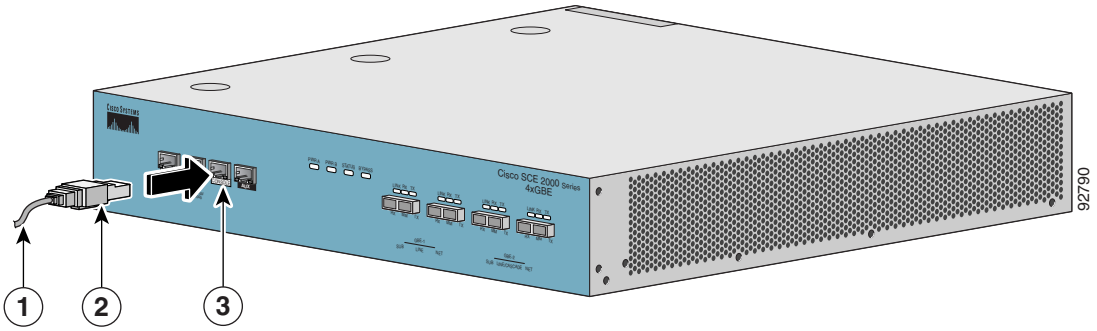
Note When installing a cascaded system, it is extremely important to follow the sequence of procedures outlined.

How to Set Up the Local Console

Even if you will be managing the SCE 2000 from a remote location, you must first connect the unit to a local console and configure the initial settings for the SCE 2000 to support remote management (Figure 5-1). When the initial connection is established, the setup utility will run automatically, prompting you to perform the initial system configuration.

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 2000 system using the setup utility.

Figure 5-1 Connecting the Local Console to the SCE 2000 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 2000 port parameters are fixed and are not configurable.

Step 1 Plug the RS-232 serial cable provided with the SCE 2000 into the CON port on the front panel of the SCE 2000.

Make sure that you push on the RJ-45 connector (attached to the RS-232 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 2000 CON port parameters.

Step 4 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 5 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 SCE 2000 and SCE 1000 Software Configuration Guide*.

Setup Command Parameters

Table 5-1 lists the setup comment parameters.

Table 5-1 Setup Command Parameters

Parameter	Definition
IP address	IP address of the SCE 2000.
subnet mask	Subnet mask of the SCE 2000.
default gateway	Default gateway.
Hostname	Character string used to identify the SCE 2000. 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)
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	

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 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 (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 2000 installed using inline topology or receive-only topology using an optical splitter?
type of deployment	Is this a cascade topology, with two SCE 2000s connected via the cascade ports? Or is this a single platform topology?
physically connected link (cascade topology only)	In a cascade deployment this parameter sets the index for the link that this SCE 2000 is deployed on. The options for SCE 2000 are link-0 or link-1. In a single- SCE 2000 platform deployment, this parameter is not relevant since one SCE 2000 is deployed on both links. In this case the link connected to port1-port2 is by default link-0 and the link connected to port3-port4 is be default link-1.
priority (cascade topology only)	If this is a cascaded topology, is this SCE 2000 the primary or secondary SCE 2000?
on-failure behavior (inline connection mode only)	If this SCE 2000 is deployed inline, should the failure behavior be bypass or cutoff of the link?
Admin status of the SCE 2000 after abnormal boot	After a reboot due to a failure, should the SCE 2000 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.

  ```
  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: How to Configure Initial Settings

Verify the following initial settings for the SCE 2000:

- 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 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: How to Configure the Hostname

The hostname is used to identify the SCE 2000. 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 2000 .

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**.

EXAMPLE:

```
Enter hostname [SCE 2000]:
```

Step 3: How to Set 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 2000. 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 The default User password is displayed.

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

Step 2 The default Admin password is displayed.

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

Step 3 The default Root password is displayed.

- To accept the displayed value, press **Enter**.
- To change the value, type any desired character 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: How to Configure 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 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 1 Type the time zone abbreviation and press **Enter**.

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

Step 2 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 3 If the time and date are correct, go to .

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 2002Time zone was successfully set.
The system clock and the calendar were successfully set.
```

Step 4 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 .

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

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

Step 5 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 6 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 7 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
```

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: How to Configure 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 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: How to Configure the RDR Formatter Destination

The SCE 2000 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 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 2000 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.

How to Configure Access Control Lists (ACLs)

The SCE 2000 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 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. Table 5-2 lists IP address and wildcard bit examples.

  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	Wildcard bits Range	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**.

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 : Configuring the Topology-Dependent Parameters (on page 5-19).

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 5-13).)

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 Steps 5 and 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.

- 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 2000 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 2000 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 platform 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: 0.0.0.0Would 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: How to Configure SNMP

Managing the SCE 2000 is possible also via a Network Management System (NMS) that supports SNMP. By default, SNMP is disabled on the SCE 2000.

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 2000).

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 Configuring the Topology-Dependent Parameters (on page 5-19). 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 residing on the SCE 2000 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.
- 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 residing on the SCE 2000 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.
- 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.

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.
- 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** and 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: How to Configure the Topology-Dependent Parameters

The topology configuration menu is a series of guided questions relating to the deployment of the SCE 2000 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, page 3-1 for a comprehensive discussion of topology and the related parameters.)

Note Values may not be requested for all topology-dependent parameters, as certain parameters do not apply to all topologies.

There are six topology-related parameters:

- **Connection mode** — Can be either of the following, depending on the physical installation of the SCE 2000.
  - Inline
  - Receive-only
- **Type of deployment** — Can be one of the following, depending on the actual deployment:
  - Single-SCE Platform — a single SCE 2000 is deployed on one or two GBE links
  - Cascade — two cascaded SCE 2000s are deployed on two GBE links, working as a fully .
- **Physically connected link (cascade topology only)** — In a cascade topology, the user must assign an index to each of the links. This index is used to identify the services per link.
  - In a single-SCE platform deployment, the indices of the links cannot be changed by the user and are:

    link-0 — the link connected to ports 1 and 2

    link-1 — the link connected to ports 3 and 4
  - In a cascade deployment, the user must define which link is connected to which SCE 2000. The index must be different for each SCE 2000. In this case the user can choose one of the following:

    Link-0 — the link connected to this SCE 2000 is identified as 0.

    Link-1 — the link connected to this SCE 2000 is identified as 1.
- **Priority (cascade topology only)** — In a cascade topology, this parameter determines which SCE 2000 is chosen as the active SCE 2000 in the "active election" procedure. This decision is taken only when both SCE 2000s are starting up together. If there is one working SCE 2000 and the other is just starting up, then the working one will automatically be chosen as active and the other one as standby. This parameter can be set to one of the following:
  - Primary
  - Secondary
- **On-Failure behavior** — Determines the behavior of the SCE 2000 upon failure, or reboot. One of the following link modes may be chosen for the SCE 2000 in the cases of failure or reboot.
  - Bypass — traffic is bypassed using the internal bypass card.
  - Cutoff — the link is forced down.
- **Admin status after abnormal reboot** — This parameter determines whether the **S**CE 2000 returns to full operational mode after abnormal (not user-requested) boot, or stays in non-operational mode, in which the SCE 2000 behaves as in failure mode. This parameter can be set to one of the following:
  - Operational
  - Non-operational

The procedure described below is a presentation of all the questions in the topology configuration. In actual practice, all questions may not be presented for a particular configuration, depending on the topology deployed.

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
```

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 deployment type.

- To specify a **Single-SCE Platform** deployment, press **Enter**.
- To specify a **Cascade** deployment, type **y and** press **Enter**.

```
Is this a cascade deployment? [no]:
```

Step 4 Specify the physically-connected-link index.

- To specify **link-0**, press **Enter**.
- To specify **link-1**, type **1**and press **Enter**.

```
Enter Physically connected link:
0- link-0
1- link-1
Enter your choice [0]:
```

Step 5 Specify the SCE 2000 priority.

- To specify **Primary**, press **Enter**.
- To specify **Secondary**, type **2** and press **Enter**.

```
Enter SCE 2000 priority:
1- primary
2- secondary
Enter your choice [1]:
```

Step 6 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 7 Specify the status of the SCE 2000 after abnormal boot.

- To specify **Operational** status after abnormal boot, press **Enter**.
- To specify **Not-Operational** status after abnormal boot, type **2** 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.

EXAMPLE 1

Following is a sample topology configuration for a non-redundant topology using an optical splitter, that is, a single SCE 2000 connected in receive-only connection mode, to one or two GBE links

```
Would you like to enter the Topology configuration menu? [no]: y
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
Is this a cascade deployment? [no]: no
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]: 1
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 inline topology. In this topology, a single SCE 2000 is connected to one or two GBE links.

When the inline connection mode is specified, the user must specify the on-failure link behavior.

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 1
Is this a cascade deployment? [no]: no
Enter On-failure behavior:
1- bypass
2- cutoff
Enter your choice [1]: 1
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]: 1
Data collection for the system configuration is completed.
```

All other parameter values are automatically assigned by the system.

EXAMPLE 3

Following is a sample topology configuration for a secondary SCE 2000 in a redundant inline topology. In this topology there are two SCE 2000 s that are cascaded via the cascade GBE ports (ports 3 and 4). Each SCE 2000 is connected inline to both sides (subscribers/network) of one GBE link.

In this case, the user must specify the physically-connected-link index (link-0 in our example), the priority of the SCE 2000, and the on-failure link behavior.

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 1Is this a cascade deployment ? [no]: yes
Enter Physically connected link:
0- link-0
1- link-1
Enter your choice [0]: 0
Enter SCE 2000 priority:
1- primary
2- secondary
Enter your choice [1]: 2
Enter On-failure behavior:
1- bypass
2- cutoff
Enter your choice [1]: 1
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]: 1
Data collection for the system configuration is completed.
```

Step 10: How to Complete and Save 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.

Step 1 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 .

```
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!
```

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://user1:vk@10.10.10.10/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 2000 and the remote management host are explained in the following sections:

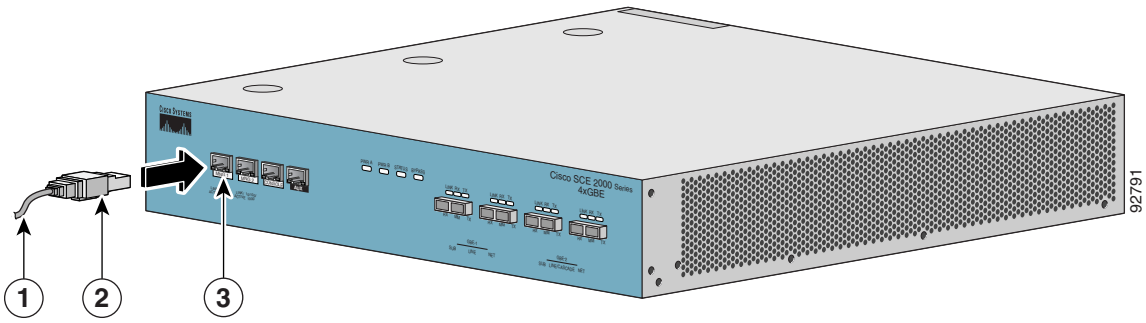
- Cabling the Management Port, page 5-25
- Verifying Management Interface Connectivity, page 5-26

Cabling the Management Port

The SCE 2000 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 2000, 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 2000 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 2000 still does not light, verify that the cable is connected correctly to the appropriate network element on its second end.

Verifying Management Interface Connectivity

If the SCE 2000 platform has been powered up, test now to verify that connectivity has been established between the SCE 2000 and the remote management host. If the SCE 2000 platform is not powered up, perform this step after starting the SCE 2000 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 Table 2-3).

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 2000 by typing **ping** and the SCE 2000 IP address, and pressing Enter (see the example, below).

Note Please note that only Step 2 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
```