CHAPTER 4

Utilities

Revised: April 30, 2012, OL-24152-02

Introduction

This module describes the following utilities:

The Setup Command

Setup Command Parameters

The setup utility is an interactive wizard that guides the user through the basic configuration process. This utility runs automatically upon initial connection to the local terminal. It may also be invoked explicitly via Telnet or via the local terminal to make changes to the system configuration.

Table 4-1 lists all the command parameters for the setup utility.

Table 4-1 Setup Command Parameters

Parameter	Definition
IP address	IP address of the SCE platform.
subnet mask	Subnet mask of the SCE platform.
default gateway	Default gateway.
hostname	Character string used to identify the SCE platform. Maximum length is 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 2007
SNTP Configuration	
broadcast client status	Sets 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

Table 4-1 Setup Command Parameters (continued)

Parameter	Definition
IP address	IP address of domain name server. (maximum of three servers)
RDR Formatter Destination Configuration	
IP address	IP address of the RDR-formatter destination
TCP port number	TCP port number of the RDR-formatter destination
Access Control Lists	
Access Control List number	How many ACLs will be necessary? What IP addresses will be permitted/denied access for each management interface? You may want ACLs for the following: • Any IP access • Telnet access • SNMP GET access • SNMP SET access
list entries (maximum 20 per list)	IP address, and whether permitted or denied access.
IP access ACL	ID number of the ACL controlling IP access.
telnet ACL	ID number of the ACL controlling telnet access.
SNMP Configuration	
SNMP agent status	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 (All Platforms)	
connection mode	Is the SCE platform installed in bump-in-the-wire topology (inline) or out of line using an optical splitter or external switch (receive-only)?
Admin status of the SCE platform after abnormal boot	After a reboot due to a failure, should the SCE platform remain in a Failure status or move to operational status provided no other problem was detected?
Topology Configuration (SCE 1000)	
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?

Table 4-1 Setup Command Parameters (continued)

Parameter	Definition
Topology Configuration (SCE 2000)	
type of deployment	Is this a cascade topology, with two SCE platforms 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 the 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 by 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?

Information regarding these parameters can be found in the appropriate sections throughout this guide.

For more information regarding SCE platform topology, and for a step-by-step description of the setup utility, see the *Cisco SCE 2000 Installation and Configuration Guide* or the *Cisco SCE 1000 2xGBE Installation and Configuration Guide*.

Entering the Setup Command

Step 1 From the SCE# prompt, type `setup` and press **Enter**.

The following dialog appears:

```
--- 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
system configuration dialog begins.
```

Defining Lists in the Setup Utility—Multiple Entry Parameters

When explicitly invoked, the setup utility offers the option of multiple entries (lists) for certain parameters.

Several parameters, such as the Access Control Lists, are actually lists containing several entries. If these lists are empty (initial configuration) or contain only one entry, they act the same as any scalar parameter, except that you are given the option of adding additional entries to the list.

If these lists already contain more than one entry, the entire list is displayed, and you are then presented with several options. Following is an excerpt from the SNMP trap manager menu, illustrating how to configure list entries.

Step 1 The entries in the list are displayed.

```
There are 2 SNMP trap managers in the current configuration as follows:
IP address: 10.10.10.10 Community: privateVersion: 1
IP address: 10.11.10.1 Community: pcubeVersion: 2c
```

Step 2 Three options are presented.

Note If only one entry exists in the table, it is displayed as the default [ ] to be either accepted or changed. The three list options are not displayed.

```
Please choose one of the following options:
1. Leave the running configuration unchanged.
2. Clear the existing lists and configure new ones.
3. Add new entries.
Enter your choice:
```

Step 3 You are prompted to continue the setup, depending on the choice you entered:

- 1. Leave the running configuration unchanged:

  The dialog proceeds to the next question. The list remains unchanged.

- 2. Clear the existing entries and configure new ones:

  The dialog prompts you for a new entry in the list.

  After completing the first entry, you are asked whether you would like to add another new entry.

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

  Since the list was empty, you may enter the maximum number of entries.

- 3. Add new entries:

  The dialog prompts you for a new entry in the list.

  After the completing one entry, you are asked whether you would like add another new entry.

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

  You may enter only enough additional entries to reach the maximum number

Working with SCE Platform Files

The CLI commands include a complete range of file management commands. These commands allow you to create, delete, copy, and display both files and directories

Note Regarding disk capacity: While performing disk operations, the user should take care that the addition of new files that are stored on the SCE disk do not cause the disk to exceed 70%.

Working with Directories

How to Create a Directory

Step 1 From the SCE# prompt, type **mkdir** *directory-name* and press **Enter**.

How to Delete a Directory

There are two different commands for deleting a directory, depending on whether the directory is empty or not.

How to Delete a Directory and All its Files

Step 1 From the SCE# prompt, type **delete** *directory-name* **/recursive** and press **Enter**.

The recursive flag deletes all files and sub-directories contained in the specified directory.

How to Delete an Empty Directory

Step 1 From the SCE# prompt, type **rmdir** *directory-name* and press **Enter**.

Use this command only for an empty directory.

How to Change Directories

Use this command to change the path of the current working directory.

Step 1 From the SCE# prompt, type **cd** *new path* and press **Enter**.

How to Display a Working Directory

Step 1 From the SCE# prompt, type **pwd** and press **Enter**.

How to List the Files in a Directory

You can display a listing of all files in the current working directory. This list may be filtered to include only application files. The listing may also be expanded to include all files in any sub-directories.

- How to List the Files in the Current Directory, page 4-7
- How to List the Applications in the Current Directory, page 4-7
- How to Include the Files in Subdirectories in the Directory Files List, page 4-7

How to List the Files in the Current Directory

Step 1 From the SCE# prompt, type **dir** and press **Enter**.

How to List the Applications in the Current Directory

Step 1 From the SCE# prompt, type **dir applications** and press **Enter**.

How to Include the Files in Subdirectories in the Directory Files List

Step 1 From the SCE# prompt, type **dir -r** and press **Enter**.

Working with Files

How to Rename a File

Step 1 From the SCE# prompt, type **rename** *current-file-name new-file-name* and press **Enter**.

How to Delete a File

Step 1 From the SCE# prompt, type **delete** *file-name* and press **Enter**.

Copying Files

You can copy a file from the current directory to a different directory. You can also copy a file (upload/download) to or from an FTP site.

To copy a file using passive FTP, use the **copy-passive** command.

How to Copy a File

Step 1 From the SCE# prompt, type **copy** *source-file-name destination-file-name* and press **Enter**.

Copying a File: Example

The following example copies the local analysis.sli file located in the root directory to the applications directory.

```
SCE#copy analysis.sli applications/analysis.sli
sce#
```

How to Download a File from an FTP Site

Use the copy command to upload and download commands from and FTP site. In this case, either the source or destination filename must begin with *ftp://*.

Step 1 From the SCE# prompt, type **copy** *ftp://source destination-file-name* and press **Enter**.

To upload a file to an FTP site, specify the FTP site as the destination (*ftp://destination*)

How to Upload a File to a Passive FTP Site

Step 1 From the SCE# prompt, type **copy-passive** *source-file-name ftp://destination* and press **Enter**.

To download a file from a passive FTP site, specify the FTP site as the source (*ftp://source*)

Uploading a File to a Passive FTP Site: Example

The following example uploads the analysis.sli file located on the local flash file system to the host 10.1.1.105, specifying Passive FTP.

```
SCE#copy-passive /appli/analysis.sli ftp://myname:mypw@10.1.1.105/p:/appli/analysis.sli
sce#
```

How to Display the Contents of a File

Step 1 From the SCE# prompt, type **more** *file-name* and press **Enter**.

How to Unzip a File

Step 1 From the SCE# prompt, type **unzip** *file-name* and press **Enter**.

User Log

The user log is an ASCII file that can be viewed in any editor. It contains a record of system events, including startup, shutdown and errors. You can use the Logger to view the user log to determine whether or not the system is functioning properly, as well as for technical support purposes.

Logging System

Events are logged to one of two log files. After a file reaches maximum capacity, the events logged in that file are then temporarily archived. New events are then automatically logged to the alternate log file. When the second log file reaches maximum capacity, the system then reverts to logging events to the first log file, thus overwriting the temporarily archived information stored in that file.

Basic operations include:

- Copying the User Log to an external source
- Viewing the User Log
- Clearing the User Log
- Viewing/clearing the User Log counters

Copying the User Log

You can view the log file by copying it to an external source or to disk. This command copies both log files to the local SCE platform disk or any external host running a FTP server.

Copying the User Log to an External Source

Step 1 From the SCE# prompt, type **logger get user-log file-name** *ftp://username:password@ipaddress/path* and press **Enter**.

Copying the User Log to an Internal Source

Step 1 From the SCE# prompt, type **logger get user-log file-name** *target-filename* and press **Enter**.

Enabling and Disabling a User Log

By default, the user log is enabled. You can disable the user log by configuring the status of the logger.

Disabling a User Log

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logger device User-File-Log disabled** and press **Enter**.

Enabling a User Log

Step 1 From the SCE# prompt, type configure and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logger device User-File-Log enabled** and press **Enter**.

Viewing the User Log Counters

- Viewing the User Log Counters for the Current Session, page 4-11
- Viewing the Nonvolatile Logger Counters for Both the User Log File and the Debug Log File, page 4-11
- Viewing the Nonvolatile Counter for the User Log File Only, page 4-11

There are two types of log counters:

- User log counters — count the number of system events logged from the SCE platform last reboot.
- Non-volatile counters — are not cleared during boot time

Viewing the User Log Counters for the Current Session

Step 1 From the SCE# prompt, type **show logger device user-file-log counters** and press **Enter**.

Viewing the Nonvolatile Logger Counters for Both the User Log File and the Debug Log File

Step 1 From the SCE# prompt, type **show logger nv-counters** and press **Enter**.

Viewing the Nonvolatile Counter for the User Log File Only

Step 1 From the SCE# prompt, type **show logger device user-file-log nv-counters** and press **Enter**.

Viewing a User Log

Note This command is not recommended when the user log is large. Copy a large log to a file to view it (see Copying the User Log, page 4-10)

Step 1 From the SCE# prompt, type **more user-log** and press **Enter**.

Clearing a User Log

Step 1 From the SCE# prompt, type **clear logger device user-file-log** and press **Enter**.

Step 2 The system asks **Are you sure?**

Step 3 Type **Y** and press **Enter**.

Generating a File for Technical Support

In order for technical support to be most effective, the user should provide them with the information contained in the system logs. Use the logger get support-file command to generate a support file via FTP for the use of Cisco technical support staff.

Step 1 From the SCE# prompt, type **logger get support-file** *filename* and press **Enter**.

The support information file is created using the specified filename. The specified file must be a file located on an FTP site, not on the local file system.

This operation may take some time.

Generating a File for Technical Support: Example

```
SCE# logger get support-file ftp://user:1234@10.10.10.10/c:/support.zip
```

Managing the Syslog

System messages are also written to the Syslog server. When enabled, all user-log messages are sent to the configured Syslog servers as well as to the SCE user logs.

You can configure the following options for syslog support:

- Up to five remote syslog hosts
- Port number
- Minimum severity level to be logged
- Logging rate limit
- Syslog facility (such as system daemon, local printer, or user process)
- Time stamp format

Transport protocol is not configurable, since the SCE platform supports Syslog over UDP, only.

Enabling and Disabling the Syslog

By default, logging to the syslog server is disabled.

Enabling the Syslog

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging on** and press **Enter**.

Disabling the Syslog

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging on** and press **Enter**.

Configuring the Remote Syslog Hosts

You can configure up to five remote syslog hosts. You can also assign a UDP port to each host.

Guidelines

- You can define the host using either the hostname or the IP address.
- To assign a port, you must use the **transport udp** option. If you are not assigning a port, this is not required, since UDP is the only transport protocol supported for Syslog on the SCE platform.
- Each host requires a separate command.

Options

The following options are available:

- **hostname**—logical name of the remote host
- **ip-address**—IP address of the remote host
- **port-number**—Number of the UDP port (1 – 65535)
  - default = 514

How to Add a Remote Syslog Host

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging host (*hostname* | *ip-address*) [transport udp [port *port-number*]]** and press **Enter**.

How to Remove a Remote Syslog Host

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging host (*hostname* | *ip-address*)** and press **Enter**.

Configuring the Minimum Severity Level to be Logged to Syslog

By default, all messages are logged to the Syslog server when it is enabled, with the exception of debug messages. However, you can configure the minimum severity level of the messages to logged to Syslog.

Table 4-2 lists the syslog severity levels and the corresponding Cisco SCOS severity levels. Not all syslog severity levels are supported on the Cisco SCE platform.

Table 4-2 Syslog and Cisco SCOS Severity Levels

Syslog Severity	Level	Cisco SCOS Severity	Cisco SCOS Definition
emergency	0	Not defined	SEVERITY_EMERGENCY_LEVEL
alert	1	Not defined	SEVERITY_ALERT_LEVEL
critical	2	Fatal	SEVERITY_FATAL_LEVEL
error	3	Error	SEVERITY_ERROR_LEVEL
warning	4	Warning	SEVERITY_WARNING_LEVEL
notice	5	Not defined	SEVERITY_NOTICE_LEVEL
informational	6	Info	SEVERITY_INFORMATIONAL_LEVEL
debug	7	Not defined	SEVERITY_DEBUG_LEVEL

Options

The following option is available:

- **severity-level**—The name of the desired severity level at which messages should be logged. Messages at or lower than the specified level are logged. Severity levels supported on the SCE platform are as follows:
  - **fatal**
  - **error**
  - **warning**
  - **info**

  Default = info

How to Configure the Minimum Severity Level for Syslog Messages

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging trap** ***severity-level*** and press **Enter**.

How to Restore the Default Minimum Severity Level for Syslog Messages

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging trap** and press **Enter**.

Configuring the Syslog Facility

You can assign Syslog messages to a specified facility.

Options

The following option is available:

- **facility-type**—Syslog facility. See Table 4-3
  - default = local7

Table 4-3 Logging Facility Types

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-local7	Reserved for locally defined messages
lpr	Line printer system

Table 4-3 Logging Facility Types

Facility Type Keyword	Description
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

How to Configure the Syslog Facility

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging facility** ***facility-type*** and press **Enter**.

How to Restore the Default Syslog Facility

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging facility** and press **Enter**.

Configuring the Syslog Logging Rate Limit

You can configure a maximum number of messages logged per second. In addition, you can specify a severity level above which the rate is unlimited. For example, you can configure a rate limit for all messages below the **fatal** severity level.

Options

The following options are available:

- **rate**—Number of messages to be logged per second (1 to 10000).
  - default = 10

- **severity-level**—Excludes messages of this severity level and higher. Severity levels supported on the SCE platform are as follows:
  - **fatal**
  - **error**
  - **warning**
  - **info**

How to Configure the Syslog Rate Limit

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging rate-limit** *rate* **[except** *severity-level***]** and press **Enter**.

How to Restore the Default Syslog Rate Limit

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging rate-limit** and press **Enter**.

Configuring the Syslog Time Stamp Format

You can configure the format of the the time stamp on the messages on the Syslog server. You can use the **no** form of this command to specify the default Syslog time stamp format (uptime).

Options

The following time stamp format options are available:

- **uptime** (default)—Time stamp shows time since the system was last rebooted. For example "4w6d" (time since last reboot is 4 weeks and 6 days).
- **datetime**—Time stamp shows date and time.

  The following additional options are available for the **datetime option:**
  - **msec—**Include milliseconds in the date-time format.
  - **localtime—**Time stamp relative to the local time zone.
  - **show-timezone—**Include the time zone name in the date-time format.
  - **year—**Include the year in the date-time format.

  If the **datetime** keyword is used without additional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.

Tip The optional **msec**, **localtime**, **show-timezone**, and **year** keywords, if present, must be in the order shown in the command syntax. All keywords up to the last specified keyword must be present
Incorrect: **service timestamps log datetime msec year**
Correct: **service timestamps log datetime msec localtime show-timezone year**

How to Configure the Syslog Time Stamp Format

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **service timestamps log (uptime | (datetime [msec] [localtime] [show-timezone] [year]))** and press **Enter**.

How to Restore the Default Syslog Time Stamp Format

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no service timestamps log** and press **Enter**.

Enabling and Disabling the Syslog Message Counter

By default, the syslog message counter is enabled. You can use this command to disable the syslog message counter. When it is disabled, no line count appears in the syslog messages.

Disabling the Syslog Message Counter

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging message-counter** and press **Enter**.

Enabling the Syslog Message Counter

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging message-counter** and press **Enter**.

Monitoring the Syslog

You can display the following Syslog information:

- Current Syslog server configuration.
- Syslog counters

How to Display the Syslog Configuration

Step 1 From the SCE# prompt, type **show logging** and press **Enter**.

How to Display the Syslog Counters

Step 1 From the SCE# prompt, type **show logging counters** and press **Enter**.

Flow Capture

The flow capture utility is a CLI-controlled utility used to capture traffic according to layer 4 attributes.

The traffic that is captured by this utility is accumulated in a CAP format file. The traffic that is identified by the capture mechanism is not available for traffic control or any service for the duration of the capture. When the flow capture is configured, the traffic that matches the rules are bypassed on Cisco SCE. At the completion of the capture, normal service to all traffic is resumed.

The recorded data is sent online to a distant location using FTP. The data is sent in a standard format and may have an unlimited size on the SCE 2000.

Limitations

Note the following known limitations of the flow capture utility:

- The actual capture starts only for newly opened flows. Therefore, already opened flows cannot be captured by this utility.
- The termination of a capture flow is verified for every new relevant packet that is being captured. As long as no packets matching the capturing attributes arrives after the time is exceeded, the capturing is not stopped and must be stopped manually.
- Capture may end prematurely due to a shortage event on the SCE platform.
- Capturing throughput is limited by the following:
  - system architectural limitations
  - line capacity to the remote FTP destination (for non-Linux platforms only, such as the SCE 2000 platform).

  The approximated throughput on a live setup is 2Mbps. When this throughput is exceeded, packets are absent from the cap file and the appropriate field in the consequent captured packet is updated to note the number of lost packets. The maximum allowed number of sequential lost packets is configurable by a const DB.

The Flow Capture Process

There are three main steps in the overall flow capture process:

1. Configure the traffic rules to define the traffic to be captured. (Configuring a Flow Capture Traffic Rule, page 4-20)
2. Configure the flow capture settings. (Optional) (Configuring the Flow Capture Settings, page 4-21)
3. Perform the actual flow capture. (Performing Flow Capture, page 4-22)

Configuring a Flow Capture Traffic Rule

The flow capture traffic rules define the traffic to be captured. You can configure a flow capture traffic rule by specifying the **flow-capture** action for the relevant flows.

For example, in order to capture all the traffic sent to or coming from subscribers whose IP addresses are in the range.2.3.0-1.2.3.255, define a traffic rule as follows:

```
SCE(config if)# traffic-rule name flowcapturerule IP-addresses subscriber-side 1.2.3.0/24
network-side all protocol all direction both traffic-counter none action flow-capture
```

Multiple rules can be configured, but note that all configured flow capture rules are in effect during the flow capture process. It is not possible to apply only a subset of the configured rules.

For more information regarding configuring traffic rules, see Configuring Traffic Rules and Counters, page 6-18.

Configuring the Flow Capture Settings

The flow capture settings control aspects of the flow capture process, as opposed to defining the flow to be captured. These settings limit the scope of the process to maximize the recorded information while minimizing the effect on traffic.

- Maximum duration of the capture: By limiting the duration of the capture, you can limit the effect of the capture on live traffic.

  You can stop the capture at any time before the maximum duration has been reached.

- Maximum length of the L4 payload of each captured packet: If you want to capture mainly the L2-L4 headers, you need only a small portion of the payload of each packet. Setting a limit on the length of the payload makes the capture more efficient, as it allows more packets to be captured within a given time frame and for a given throughput.

  Guidelines and Information:

  - If maximum L4 payload length is not configured, all bytes of each captured packet are recorded.
  - If maximum L4 payload length is configured, each captured packet will contain the entireL2/L3/L4 headers and no more than the configured maximum bytes of L4 payload.
  - Only one maximum L4 payload length value can be configured. This value applies to all recorded packets.
  - If the maximum L4 payload length value is changed while recording is performed, it will not take effect until the next recording session.
  - The cap file contains marking for packets which had TCP or UDP checksum error when received in the SCE platform, since the validity of the TCP and UDP checksum cannot be checked for the captured packets due to missing bytes.
  - The cap file contains the information to retrieve the original length of each packet that was truncated.

How to Configure the Maximum Flow Capture Duration

The following options are available:

- **duration** — the maximum duration of the flow capture in seconds.

  Default = 3600 seconds

- **unlimited** — there is no time limit to the flow capture, and it will continue until stopped by the operator.

Step 1 From the SCE(config if)# prompt, type **flow-capture controllers time (*duration* | unlimited)** and press **Enter**.

How to Configure the Maximum Length of the L4 Payload

The following options are available:

- **length** — the maximum number of L4 payload bytes to capture from each packet.
- **unlimited** — there is no limit on the number of L4 payload bytes. (Default)

Step 1 From the SCE(config if)# prompt, type **flow-capture controllers max-l4-payload-length (*length* | unlimited)** and press **Enter**.

How to Restore the Default Flow Capture Settings

Step 1 From the SCE(config if)# prompt, type **default flow-capture controllers (time | max-l4-payload-length)** and press **Enter**.

Performing Flow Capture

The flow capture begins when you execute the flow-capture command. You can stop the capture at any time. If the capture is not stopped, it continues for the configured maximum duration (Configuring the Flow Capture Settings, page 4-21).

How to Start Flow Capture

The following option is available:

- **filename** — name and FTP location to which to record the flow capture data in the format *ftp://<username>:<password>@<IP_address>/<path>/<file_name>*.

Step 1 From the SCE(config if)# prompt, type **flow-capture start format cap** *filename* and press **Enter**.

How to Stop Flow Capture

Step 1 From the SCE(config if)# prompt, type **flow-capture stop** and press **Enter**.

Monitoring Flow Capture

Use the following command to monitor the flow capture process. It displays the following information:

- status of the recording process
- current target file size
- number of packets captured
- number of packets lost
- configured values of the different controllers

How to Monitor Flow Capture

Step 1 From the SCE> prompt, type **show interface linecard 0 flow-capture** and press **Enter**.