



## About this Guide

---

**Revised: February 18, 2015**

## Introduction

This preface describes who should read *Cisco SCE 8000 10 GBE Installation and Configuration Guide*, how it is organized, and its document conventions.

This guide is for the networking or computer technician responsible for installing and configuring the Cisco SCE 8000 platform on-site. To use this publication, you should be familiar with telecommunications equipment and installation procedures, as well as electronic circuitry and wiring practices. You should also have experience as an electronic or electromechanical technician.

This installation guide explains the initial hardware installation and basic configuration procedures for the Cisco SCE 8000. It contains procedures for unpacking and installing the device and performing basic configuration via the setup wizard. After completing the installation and basic configuration procedures covered in this guide, use the appropriate companion publications to configure your system.

This guide contains instructions on how to install and run the Cisco SCE 8000 platform. This guide assumes a basic familiarity with telecommunications equipment and installation procedures.

# Document Revision History

**Table 1**      **Document Revision History**

| Revision | Release and Date                 | Change Summary                                                    |
|----------|----------------------------------|-------------------------------------------------------------------|
|          | Release 4.2.x<br>August 30, 2014 | First version of this document (new for the Release 4.2.x train). |

# Organization

The major sections of this guide are as follows:

**Table 2**            **Organization**

| Chapter    | Title                                                                   | Description                                                                                                                                                                                                                                                                                                  |
|------------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chapter 1  | <a href="#">Cisco Service Control Overview</a>                          | This chapter provides a brief introduction to Cisco Service Control.                                                                                                                                                                                                                                         |
| Chapter 2  | <a href="#">Introduction to the Cisco SCE 8000 10 GBE Platform</a>      | This chapter provides a hardware overview of the Cisco SCE 8000 platform.                                                                                                                                                                                                                                    |
| Chapter 3  | <a href="#">Cisco SCE 8000 Topology and Topology-Related Parameters</a> | This chapter describes the possible deployment topologies of the Cisco SCE 8000 and explains how various aspects of the topology determine the configuration of the system.                                                                                                                                  |
| Chapter 4  | <a href="#">Installing the Cisco SCE 8000 Chassis</a>                   | This chapter explains how to install a Cisco SCE 8000 platform in the rack and properly ground it.                                                                                                                                                                                                           |
| Chapter 5  | <a href="#">Connecting the Management Interfaces</a>                    | This chapter explains how to connect the Cisco SCE 8000 platform to a local console and perform the initial system configuration via the setup wizard that runs automatically.                                                                                                                               |
| Chapter 6  | <a href="#">Cabling the Line Ports and Completing the Installation</a>  | This chapter provides instructions for cabling the Gigabit Ethernet ports for both one and two Cisco SCE 8000 topologies, and for configuring Gigabit Ethernet (GBE) interface parameters. In a topology utilizing two Cisco SCE 8000s (cascade), this includes the cascade ports as well as the line ports. |
| Chapter 7  | <a href="#">Basic Cisco SCE 8000 Platform Operations</a>                | This chapter describes how to start up the Cisco SCE 8000 platform, reboot, and shutdown. It also describes how to manage configurations.                                                                                                                                                                    |
| Chapter 8  | <a href="#">Troubleshooting</a>                                         | This chapter provides basic system startup troubleshooting information.                                                                                                                                                                                                                                      |
| Chapter 9  | <a href="#">Removal and Replacement Procedures</a>                      | This chapter explains the procedures for removing and replacing the power supplies, fan trays, and other modules.                                                                                                                                                                                            |
| Appendix A | <a href="#">Using Optical Splitters with 10 GBE Links</a>               | This appendix supplies important information about supported and not supported optical splitter configurations in the 10 GBE environment.                                                                                                                                                                    |

**Table 2**      **Organization**

| Chapter    | Title                                                            | Description                                                                                                |
|------------|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Appendix B | <a href="#">CLI Commands to Verify a Successful Installation</a> | This appendix provides a basic post-installation checklist to verify that the installation was successful. |
| Appendix C | <a href="#">Cisco Service Control Engine System Log Messages</a> | This appendix describes the system log messages generated by the Cisco SCE 10 8000 GBE platform.           |

## Related Publications

The Cisco SCE 8000 platform and the software running on it contain extensive features and functionality, which are documented in the following resources:

- Cisco CLI software:
  - [Cisco SCE8000 10GBE Software Configuration Guide](#)
  - [Cisco SCE8000 CLI Command Reference](#)
- For initial installation and startup information, see the [Cisco SCE8000 Quick Start Guide](#).
- For international agency compliance, safety, and statutory information for wide-area network (WAN) interfaces for the Cisco SCE 8000 platform, see the [Regulatory Compliance and Safety Information for Cisco SCE8000](#).
- For installation and configuration of the other components of the Service Control Management Suite see:
  - [Cisco SCMS Subscriber Management User Guide](#)
  - [Cisco SCMS Collection Manager User Guide](#)
  - [Cisco Service Control Application for Broadband User Guide](#)
  - [Cisco Insight User Guide](#)
- To view Cisco documentation or obtain general information about the documentation, see the Cisco Information Packet that is shipped with your Cisco SCE 8000 platform.

# Conventions

This document uses the following conventions:

**Table 3**      **Conventions**

| Convention         | Indication                                                                                                                  |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>bold</b> font   | Commands and keywords and user-entered text appear in <b>bold</b> font.                                                     |
| <i>italic</i> font | Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.              |
| [ ]                | Elements in square brackets are optional.                                                                                   |
| { x   y   z }      | Required alternative keywords are grouped in braces and separated by vertical bars.                                         |
| [ x   y   z ]      | Optional alternative keywords are grouped in brackets and separated by vertical bars.                                       |
| string             | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| courier font       | Terminal sessions and information the system displays appear in <code>courier</code> font.                                  |
| < >                | Nonprinting characters such as passwords are in angle brackets.                                                             |
| [ ]                | Default responses to system prompts are in square brackets.                                                                 |
| !, #               | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.                   |



## Note

Means *reader take note*.



## Tip

Means *the following information will help you solve a problem*.



## Caution

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



## Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



## Warning

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

---

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# Cisco Service Control Overview

---

Revised: February 18, 2015

## Introduction

This chapter provides a general overview of the Cisco Service Control solution. It introduces the Cisco service control concept and capabilities.

It also briefly describes the hardware capabilities of the service control engine (SCE) platform and the Cisco specific applications that together compose the complete Cisco service control solution.

- [Cisco Service Control Solution, page 1-2](#)
- [Cisco Service Control Capabilities, page 1-3](#)
- [SCE Platform Description, page 1-4](#)
- [Management and Collection, page 1-6](#)

# Cisco Service Control Solution

The Cisco service control solution is delivered through a combination of specific hardware and software solutions that address various operational and business-related challenges. Service providers can use the SCE platform to support classification, analysis, and control of Internet and IP traffic.

Service control enables service providers to:

- Capitalize on existing infrastructure.
- Analyze, charge for, and control IP network traffic at multigigabit wire line speeds.
- Identify and target high-margin content-based services and enable their delivery.

As access and bandwidth have become commodities where prices continually fall and profits disappear, service providers have realized that they must offer value-added services to derive more revenue from the traffic and services running on their networks.

Cisco service control solutions allow the service provider to capture profits from IP services through detailed monitoring, precise, real-time control, and awareness of applications as they are delivered.

## Service Control for Broadband Service Providers

Service providers of any access technology (DSL, cable, mobile, and so on) targeting residential and business consumers must find new ways to get maximum leverage from their existing infrastructure, while differentiating their offerings with enhanced IP services.

The Cisco service control application for broadband adds a layer of service intelligence and control to existing networks that can:

- Report and analyze network traffic at subscriber and aggregate level for capacity planning.
- Provide customer-intuitive tiered application services and guarantee application service level agreements (SLAs).
- Implement different service levels for different types of customers, content, or applications.
- Identify network abusers who are violating the acceptable use policy (AUP).
- Identify and manage peer-to-peer traffic, Network News Transfer Protocol (NNTP) traffic, and spam abusers.
- Enforce the AUP.
- Integrate Service Control solutions easily with existing network elements and business support systems (BSS) and operational support systems (OSS).

# Cisco Service Control Capabilities

The core of the Cisco service control solution is the network hardware device: the Service control engine (SCE). The core capabilities of the SCE platform, which support a wide range of applications for delivering service control solutions, include:

- Subscriber and application awareness—Application-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific subscriber.
  - Subscriber awareness—Ability to map between IP flows and a specific subscriber to maintain the state of each subscriber transmitting traffic through the SCE platform and to enforce the appropriate policy on this subscriber's traffic.

Subscriber awareness is achieved either through dedicated integrations with subscriber management repositories, such as a DHCP or a RADIUS server, or through sniffing of RADIUS or DHCP traffic.

- Application awareness—Ability to understand and analyze traffic up to the application protocol layer (Layer 7).

For application protocols implemented using bundled flows (such as FTP, which is implemented using Control and Data flows), the SCE platform understands the bundling connection between the flows and treats them accordingly.

- Application-layer, stateful, real-time traffic control—Ability to perform advanced control functions, including granular bandwidth (BW) metering and shaping, quota management, and redirection, using application-layer, stateful, real-time traffic transaction processing. This requires highly adaptive protocol and application-level intelligence.
- Programmability—Ability to quickly add new protocols and adapt to new services and applications in the service provider environment. Programmability is achieved using the Cisco Service Modeling Language (SML).

Programmability allows new services to be deployed quickly and provides an easy upgrade path for network, application, or service growth.

- Robust and flexible back-office integration—Ability to integrate with existing third-party systems at the service provider, including provisioning systems, subscriber repositories, billing systems, and OSS systems. The SCE provides a set of open and well-documented APIs that allows a quick integration process.
- Scalable high-performance service engines—Ability to perform all these operations at wire speed.

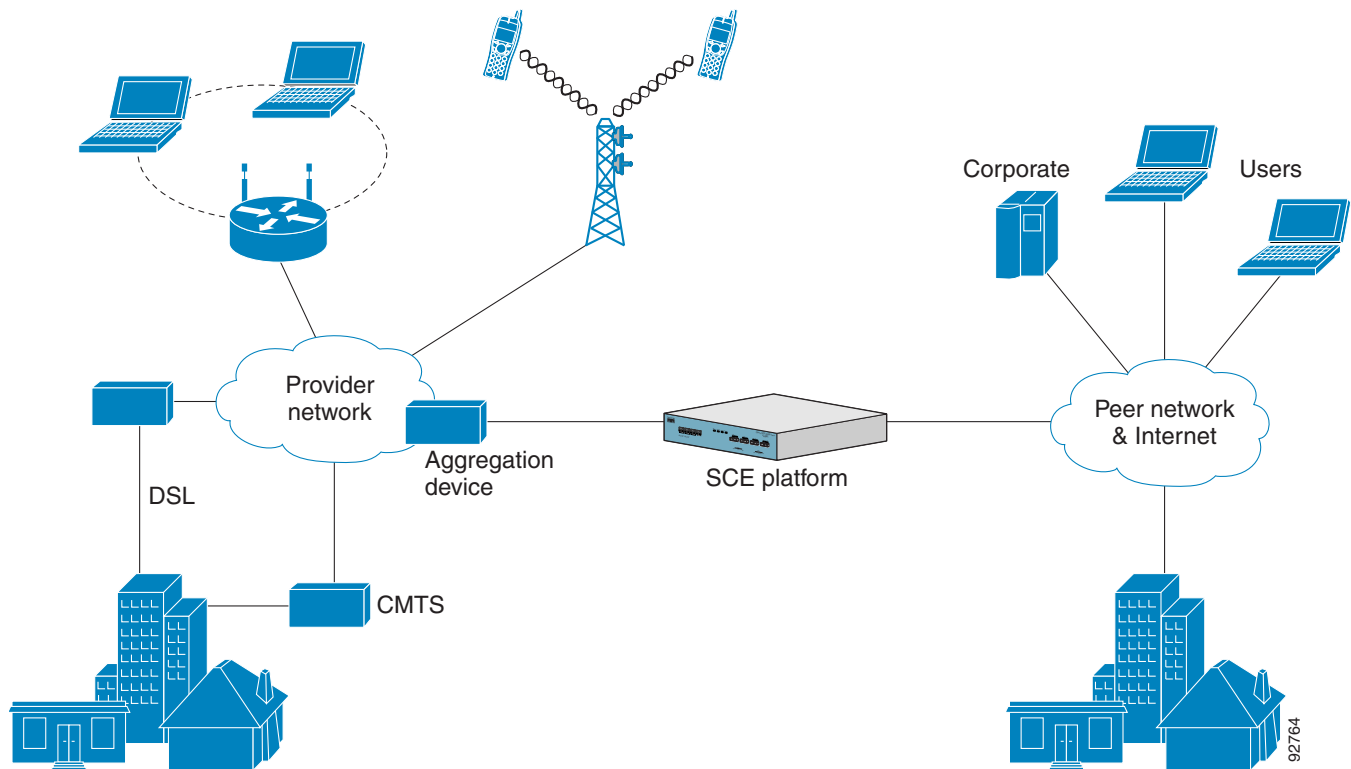
# SCE Platform Description

The SCE family of programmable network devices performs application-layer stateful-flow inspection of IP traffic, and controls the traffic based on configurable rules. The *SCE platform* is a network device that uses ASIC components and reduced instruction set computer (RISC) processors to exceed beyond packet counting and expand into the contents of network traffic. Providing programmable, stateful inspection of bidirectional traffic flows, and mapping these flows with user ownership, SCE platforms provide real-time classification of network use. The classification provides the basis of the SCE platform advanced traffic-control and bandwidth-policing functionality. Where most bandwidth control functionality ends, the SCE platform provides further control and shaping options, including:

- Layer 7 stateful wire-speed packet inspection and classification.
- Robust support for more than 600 protocols and applications, including:
  - General—HTTP, HTTPS, FTP, Telnet, NNTP, Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Wireless Application Protocol (WAP), and others
  - Peer-to-Peer (P2P) file sharing—FastTrack-KaZaA, Gnutella, BitTorrent, Winny, Hotline, eDonkey, DirectConnect, Piolet, and others
  - P2P VoIP—Skype, Skinny, DingoTel, and others
  - Streaming and Multimedia—Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), HTTP streaming, Real Time Protocol (RTP) and Real Time Control Protocol (RTCP), and others
- Programmable system core for flexible reporting and bandwidth control.
- Transparent network and BSS and OSS integration into existing networks.
- Subscriber awareness that relates traffic and usage to specific customers.

Figure 1-1 illustrates a common deployment of an SCE platform in a network.

**Figure 1-1**      **SCE Platform in the Network**



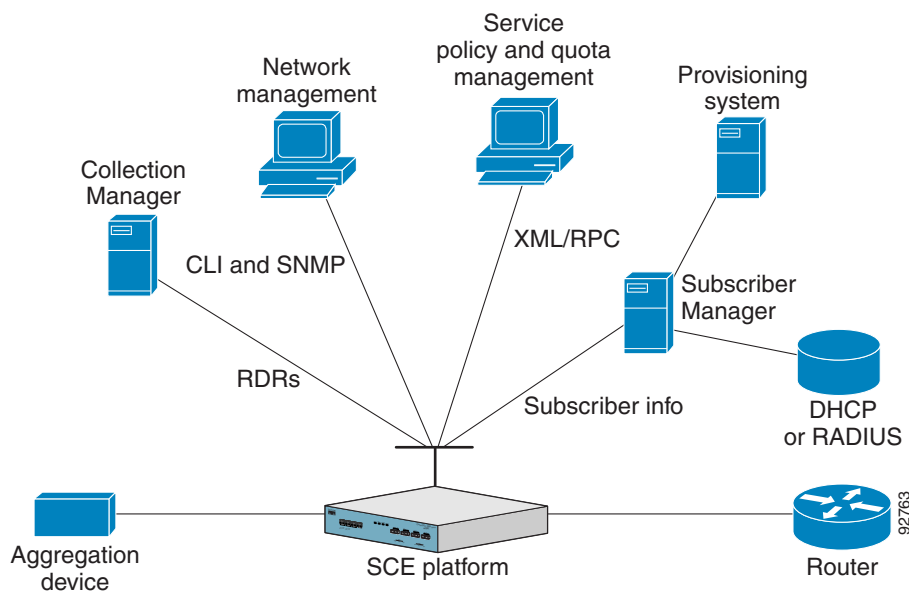
# Management and Collection

The Cisco service control solution includes a complete management infrastructure that provides the following management components to manage all aspects of the solution:

- Network management
- Subscriber management
- Service Configuration management

These management interfaces are designed to comply with common management standards and to integrate easily with existing OSS infrastructure (See [Figure 1-2](#)).

**Figure 1-2 Service Control Management Infrastructure**



## Network Management

The Cisco service control solution provides complete network Fault, Configuration, Accounting, Performance, Security (FCAPS) Management.

Two interfaces provide network management:

- **Command-line interface (CLI)**—Accessible through the Console port or through a Telnet connection, the CLI is used for configuration and security functions.
- **Simple Network Management Protocol (SNMP)**—Provides fault management (through SNMP traps) and performance-monitoring functionality.

## Subscriber Management

Where the Cisco service control application for broadband (SCA BB) enforces policies on different subscribers and tracks usage on an individual subscriber basis, the Cisco service control management suite (SCMS) subscriber manager (SM) may be used as middleware software for bridging between OSS and SCE platforms. Subscriber information is stored in the SM database and can be distributed between multiple platforms according to actual subscriber placement.

The SM provides subscriber awareness by mapping network IDs to subscriber IDs. It can obtain subscriber information using dedicated integration modules that integrate with AAA devices, such as RADIUS or DHCP servers.

Subscriber information may be obtained in one of these ways:

- Push Mode—SM pushes subscriber information to the SCE platform automatically upon logon of a subscriber.
- Pull Mode—SM sends subscriber information to the SCE platform in response to a query from the SCE platform.

## Service Configuration Management

*Service configuration management* is the ability to configure the general service definitions of a service control application. A service configuration file containing settings for traffic classification, accounting and reporting, and control is created and applied to an SCE platform. The SCA BB application provides tools to automate the distribution of these configuration files to SCE platforms. This standards-based approach makes it easy to manage multiple devices in a large network.

Service Control provides a GUI to edit and create these files and a complete set of APIs to automate their creation.

## Data Collection

Data collection occurs as follows:

1. All analysis and data processing functions of the SCE platform result in the generation of Raw Data Records (RDRs), which the SCE platform forwards using a simple TCP-based protocol (RDR-Protocol).
2. RDRs are processed by the Cisco service control management suite collection manager.
3. The collection manager software is an implementation of a collection system that receives RDRs from one or more SCE platforms. It collects these records and processes them in one of its adapters. Each adapter performs a specific action on the RDR.

RDRs contain a variety of information and statistics, depending on the configuration of the system. Three main categories of RDRs include:

- Transaction RDRs—Records generated for each *transaction*, where a transaction is a single event detected in network traffic. The identification of a transaction depends on the particular application and protocol.
- Subscriber Usage RDRs—Records generated per subscriber, describing the traffic generated by that subscriber for a defined interval.
- Link RDRs—Records generated per link, describing the traffic carried on the link for a defined interval.





# Introduction to the Cisco SCE 8000 10 GBE Platform

---

Revised: February 18, 2015

## Introduction

This chapter provides an introduction to the Cisco SCE 8000 10 GBE platform, the Service Control hardware component.

- [Information About the Cisco SCE 8000 10 GBE Platform, page 2-2](#)
- [Service Control Module \(Cisco SCE 8000-SCM-E\), page 2-4](#)
- [Introduction to SIPs and SPAs, page 2-6](#)
- [The Cisco SCE 8000-SIP LED, page 2-9](#)
- [The 1-Port 10 GBE SPA Interface Module, page 2-10](#)
- [The Cisco SCE 8000 Optical Bypass, page 2-12](#)
- [Checking the Shipping Container Contents, page 2-18](#)
- [Cisco SCE 8000 Installation Checklist, page 2-20](#)

# Information About the Cisco SCE 8000 10 GBE Platform

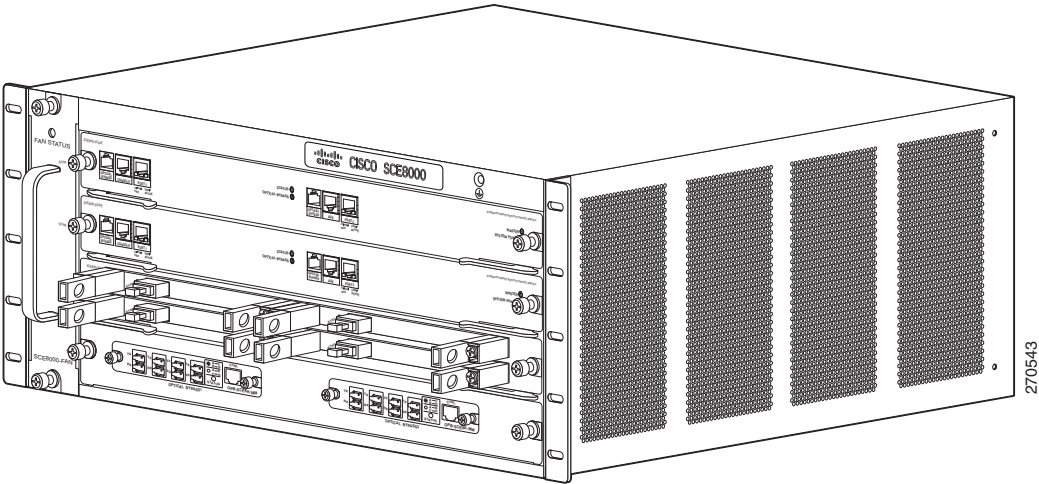
The Service Control Engine (SCE) platform, which is the hardware component of the Cisco Service Control solution, is designed to support observation, analysis, and control of Internet/IP traffic. [Table 2-1](#) summarizes model information for the Cisco SCE 8000 platform.

**Table 2-1** SCE Platform Model Information

| Model number    | Cisco SCE 8000 10 GBE |
|-----------------|-----------------------|
| Link type       | 10 Gigabit Ethernet   |
| Number of ports | 2 or 4                |
| Number of links | 1 or 2                |

The *Cisco SCE 8000 10 GBE* is a transparent element with 10 GBE links service throughput (See [Figure 2-1](#)). It can be installed inline in the network where the entire traffic passes through it or in receive-only mode where it receives replication of the traffic through SPAN ports or optical splitters.

**Figure 2-1** Cisco SCE 8000 Platform



The Cisco SCE 8000 supports the following network insertion models:

- Single appliance (inline)
- Single appliance (receive-only)
- Cascade configuration
- MGSCP configuration

The Cisco SCE 8000 platform is a 4-slot chassis hosting the following modules:

- One or two Service Control Modules (Cisco SCE 8000-SCM-E) that each contain special purpose fast path chipset, traffic processors and control processor.
- One SPA Interface Processor card (Cisco SCE 8000-SIP) that holds up to four SPA 10 GBE interface modules.
- One optional optical bypass module hosting panel that holds up to two optical bypass modules.

In addition, the Cisco SCE 8000 chassis contains two power supply modules in a 1+1 configuration, as well as a fan tray module.

# Service Control Module (Cisco SCE 8000-SCM-E)

The Cisco SCE 8000 GBE contains one or two Cisco SCE 8000-SCMs located in slots 1 and 2 (the top two slots). If only one Cisco SCE 8000-SCM module is installed, it must be installed in slot 1.

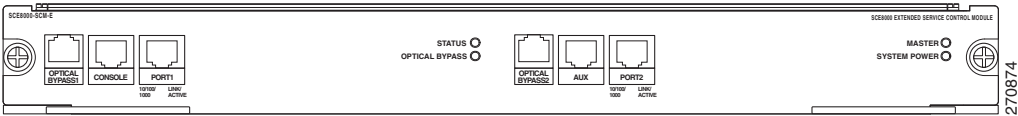
The Cisco SCE 8000-SCM in slot 1 performs the following functions:

- Service engine (Deep Packet Inspection (DPI)) and traffic processing
- Management interfaces and functionality
- Chassis control and management

The Cisco SCE 8000-SCM in slot 2 serves only DPI and traffic processing purposes, doubling the performance and capacity of the Cisco SCE 8000. Although the two modules are identical (with the same ports and LEDs), this second SCM module does not run chassis management or control software.

The Service Control module contains ports and LEDs as shown in [Figure 2-2](#), and described in [Table 2-2](#) and [Table 2-3](#).

Figure 2-2 Cisco SCE 8000-SCM-E



Note

Although the Cisco SCE 8000-SCM module in slot 2 contains all the ports listed in [Table 2-2](#), these ports are not used. All connections should be made to the Cisco SCE 8000-SCM module in slot 1.

Table 2-2 Cisco SCE 8000-SCM-E Ports

| Port        | Quantity            | Description                                                                                                                                                               | Connect This Port To...                                                                                                                                                      |
|-------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10/100/1000 | 2 (Port1 and Port2) | 10/100/1000 Ethernet RJ-45 ports for management of the Cisco SCE 8000.<br><br>CLI designation: interface GigabitEthernet 1/1, 1/2<br><br>OR<br><br>interface MNG 0/1, 0/2 | A LAN using a GBE cable with an RJ-45 connector.<br><br>If both interfaces are used to provide a redundant management interface, connect both ports to the LAN via a switch. |
| Console     | 1                   | RS-232 RJ-45 port used by technicians.                                                                                                                                    | A local terminal (console) using an RS-232 cable with an RJ-45 connector, as provided in the Cisco SCE 8000 kit.                                                             |
| AUX         | 1                   | RS-232 RJ-45 port used by technicians.                                                                                                                                    | —                                                                                                                                                                            |
| Bypass      | 2                   | RJ-11 port.                                                                                                                                                               | The control connector on the optical bypass module.                                                                                                                          |

**Table 2-3 Cisco SCE 8000-SCM-E LEDs**

| LEDs                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power                                   | <ul style="list-style-type: none"> <li>Green—Installed power supplies are functioning normally.</li> <li>Amber—Only one power supply is functioning normally.</li> <li>Unlit—No power from either power supply.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Status                                  | <p>The Status LED indicates the operational status of the Cisco SCE 8000 10 GBE system, as follows:</p> <ul style="list-style-type: none"> <li>Unlit—No power from either power unit.</li> <li>Amber—The system is booting up.</li> <li>Flashing amber—The system is operational, but is in a warning state.</li> <li>Green—The system is fully operational.</li> <li>Red—There is a problem or failure</li> </ul> <p><b>Note</b> Alarms are hierarchical: Failure takes precedence over Warning, which takes precedence over Operational.</p>                                                                                                                    |
| Optical bypass                          | <ul style="list-style-type: none"> <li>Green—Optic bypass modules are present, but not operating.</li> <li>Amber—Optic bypass modules are present and operating.</li> <li>Unlit—Optic bypass modules are not present or there is no power.</li> </ul> <p>On a slave Cisco SCE 8000-SMC-E module (in slot 2), this LED is always off.</p> <p><b>Note</b> This functionality is consistent even when the Cisco SCE 8000 10 GBE is turned off.</p>                                                                                                                                                                                                                   |
| Master                                  | <p>Master Service Control module indicator.</p> <ul style="list-style-type: none"> <li>Steady green—Master Service Control module (in slot 1)</li> <li>Unlit—Slave Service Control module (in slot 2)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Port1 and Port2 (Management interfaces) | <p>The Port1 and Port2 LEDs indicate the operational status of the Cisco SCE 8000 out-of-band LAN-based management port, as follows:</p> <ul style="list-style-type: none"> <li>Link/Active <ul style="list-style-type: none"> <li>Steady green—Port link is up</li> <li>Flashing green—Activity on the port link</li> <li>Unlit—Port link is down</li> </ul> </li> <li>Speed <ul style="list-style-type: none"> <li>Unlit—Port is set to 10 Mbps</li> <li>Steady green—Port is set to 100 Mbps</li> <li>Steady amber—Port is set to 1000 Mbps</li> </ul> </li> </ul> <p>On a slave Cisco SCE 8000-SMC-E module (in the second slot), this LED is always off.</p> |

# Introduction to SIPs and SPAs

SIPs and SPAs are a new carrier card and port adapter architecture used to increase modularity, flexibility, and density for network connectivity. This section describes the SIPs and SPAs and provides some guidelines for their use.

- [SPA Interface Processors, page 2-6](#)
- [Specifying the SIP Subslot Location for a SPA, page 2-6](#)
- [Shared Port Adapters, page 2-7](#)
- [Modular Optics, page 2-8](#)
- [XFP Connections, page 2-9](#)

## SPA Interface Processors

The SIP module supported by the Cisco SCE 8000 chassis is the Cisco SCE 8000-SIP.

The following list describes some of the general characteristics of a SIP:

- SIP is a carrier card that inserts into a slot in the chassis like a line card. It provides no network connectivity on its own.
- SIP contains one or more subslots (bays), which are used to house one or more SPAs. The SPA provides interface ports for network connectivity.
- During normal operation the SIP should reside in the Cisco SCE 8000 chassis fully populated either with functional SPAs in all subslots, or with a blank filler plate (SPA-BLANK=) inserted in all empty subslots.

## Specifying the SIP Subslot Location for a SPA

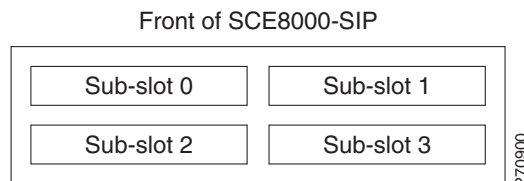
Cisco SCE 8000-SIP subslots begin their numbering with “0” and have a horizontal orientation.

[Figure 2-3](#) shows the subslot numbering for the Cisco SCE 8000-SIP.

The Cisco SCE 8000-SIP supports four subslots for the installation of SPAs, as follows:

- SIP subslot 0—Top-left subslot
- SIP subslot 1—Top-right subslot
- SIP subslot 2—Bottom-left subslot
- SIP subslot 3—Bottom-right subslot

**Figure 2-3**      **SPA Module Subslot Location**



## Shared Port Adapters

The SPA supported by the Cisco SCE 8000-SIP is the 1-Port 10-Gigabit Ethernet SPA, SPA-1X10GE-L-V2

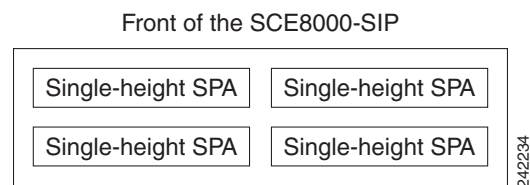
The following list describes some of the general characteristics of a SPA:

- A SPA is a modular type of port adapter that inserts into a subslot of a compatible SIP carrier card to provide network connectivity and increased interface port density. The Cisco SCE 8000-SIP can hold up to four SPAs.

If the interfaces are connected in subscriber/network pairs, either two or four SPAs must be installed.

- The supported SPA is a single-height SPAs, which inserts into one SIP subslot. (See [Figure 2-4](#).)

**Figure 2-4**      **Single-Height SPA Size**



- Each SPA provides a one 10 GBE port, which is the interface to either subscriber or network traffic. These interfaces can be individually configured using the Cisco command-line interface (CLI).
- Either a blank filler plate or a functional SPA should reside in every subslot of an SIP during normal operation to maintain cooling integrity. Blank filler plates are available in single-height form only.

If the interfaces are connected in subscriber/network pairs, the Cisco SCE 8000-SIP must be either fully populated or have both the bottom bays covered with blank filler plates.

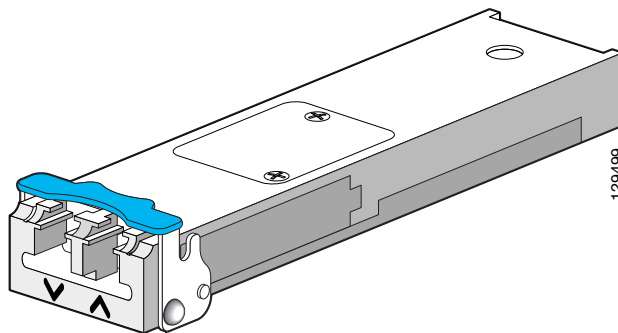
## Modular Optics

The SPAs implement 10 GBE small form-factor pluggable (XFP) optical transceivers to provide network connectivity (See [Figure 2-5](#)). An XFP module is a transceiver device that mounts into the front panel to provide network connectivity.

**Note**

It is highly recommended to use only the XFP modules listed as supported in this document. Use of unsupported or unqualified XFP modules may affect reliability or operation.

**Figure 2-5**      **10 GBE Small Form-factor Pluggable (XFP0)**



The interface connector on the 1-Port 10-Gigabit Ethernet SPA is a fiber optic receiver that supports one XFP.

The types of optics modules that have been qualified for use with the 1-Port 10-Gigabit Ethernet SPA on the Cisco SCE 8000 platform are as follows:

- XFP-10GLR-OC192SR
- XFP-10GER-OC192IR
- XFP-10GZR-OC192LR
- XFP-10G-MM-SR

## XFP Connections

The qualified XFPs include an optical transmitter and receiver pair integrated with Clock and Data Recovery (CDR) integrated circuits. The XFPs provide high-speed serial links at 10.3125 Gbps on single mode fibers. [Table 2-4](#) lists the XFP port cabling specifications.

The transmit side recovers and retimes the 10 Gbps serial data and passes it to a laser driver. The laser driver biases and modulates a laser, enabling data transmission over fiber through an LC connector. The receive side recovers and retimes the 10 Gbps optical data stream from a photo detector trans impedance amplifier and passes it to an output driver.

See the label on the XFP for technology type and model.

XFP dimensions are:

- Height 12.5 mm
- Width 18.35 mm
- Length 71.1mm

The XFP operating temperature range is from 0°C to 70°C (32°F to 158°F).

**Table 2-4 XFP Port Cabling Specifications**

| XFP               | Wavelength | Fiber Type |
|-------------------|------------|------------|
| XFP-10GLR-OC192SR | 1310 nm    | SMF        |
| XFP-10GER-OC192IR | 1550 nm    | SMF        |
| XFP-10GZR-OC192LR | 1550 nm    | SMF        |
| XFP-10G-MM-SR     | 850 nm     | MMF        |

## The Cisco SCE 8000-SIP LED

[Table 2-5](#) list the status and description of the Cisco SCE 8000-SIP LED.

**Table 2-5 Cisco SCE 8000-SIP LED**

| LEDs   | Description                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | <ul style="list-style-type: none"> <li>• Green—Operational</li> <li>• Flashing Amber—Electrical bypass in operation</li> <li>• Red—Not initialized or failed</li> <li>• Unlit—No power</li> </ul> |

# The 1-Port 10 GBE SPA Interface Module

The Cisco SCE 8000-SIP is installed in slot 3 of the Cisco SCE 8000 chassis. It hosts up to four single-width, single-height 1-Port 10 GBE SPA interface modules, but in the Cisco SCE 8000, it must be configured with either two 1-Port 10 GBE SPAs (in the top two subslots) or four 1-Port 10 GBE SPAs, to provide interfaces for either one or two complete traffic links. [Figure 2-6](#) provides an illustration of the SPA module, [Table 2-6](#) lists the SPA module ports, and [Table 2-7](#) lists the SPA module LEDs.

Figure 2-6 1-Port 10 GBE SPA Interface Module

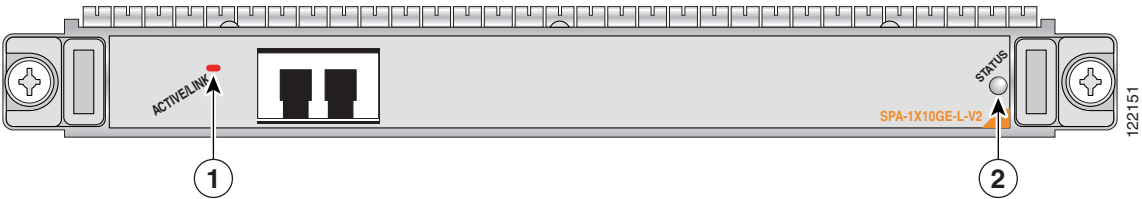


Table 2-6 SPA Ports

| Port             | Quantity      | Description                                                                                                                                                                                                                                                                                        | Connect This Port To...                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 GBE Line port | 1 on each SPA | <p>Any one of the following:</p> <ul style="list-style-type: none"><li>• XFP-10GLR-OC192SR (10km)</li><li>• XFP-10GER-OC192IR (40km)</li><li>• XFP-10GZR-OC192LR (80km)</li><li>• XFP-10G-MM-SR (300m)</li></ul> <p>CLI designation: interface TenGigabitEthernet 3/0/0, 3/1/0/, 3/2/0, 3/3/0.</p> | <p>Any one of the following:</p> <ul style="list-style-type: none"><li>• Subscriber side network component</li><li>• Network side network component</li><li>• Optical bypass 10 GBE line port</li><li>• 10 GBE line port of a cascaded Cisco SCE 8000 platform</li><li>• EtherChannel port of a Cisco 7600 Series router (MGSCP topology)</li></ul> <p>See <a href="#">Connecting the Line Ports to the Network, page 6-2</a> for further information.</p> |

**Table 2-7**      **SPA LEDs**

| LEDs            | Description                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active/Link (1) | <ul style="list-style-type: none"><li>• Green—Port is enabled by software and the link is up.</li><li>• Amber—Port is enabled by software and the link is down.</li><li>• Unlit—Port is not enabled by software.</li></ul>                                                         |
| Status (2)      | <p>The Status LED indicates the operational status of the SPA module, as follows:</p> <ul style="list-style-type: none"><li>• Green—SPA is ready and operational.</li><li>• Amber—SPA power is on and good, and SPA is being configured.</li><li>• Off—SPA power is off.</li></ul> |

# The Cisco SCE 8000 Optical Bypass

This section describes the following:

- [Optical Bypass Functionality, page 2-12](#)
- [Optical Bypass Module \(OPB-SCE8K\), page 2-13](#)

The Cisco SCE 8000 platform optical bypass module preserves the service provider 10 GBE links under all circumstances. At power failure, the bypass is automatically activated. It can also be activated by the Cisco SCE 8000 software.

The Cisco SCE 8000-SIP module already includes an internal electrical bypass, but it is strongly recommended to use the optical bypass module for addressing the following scenarios:

- During platform reboot (Software reload)—If the external bypass module is not used, there is a 11-second period during which the link is forced down (cutoff functionality). If any routing or spanning tree protocols are used in the network, this delay may be extended.
- During a power failure—The Cisco SCE 8000 has two power supplies. A power failure occurs only when both of them fail.

In case the Cisco SCE 8000 platform must be replaced, it is possible to remove the bypass modules from the Cisco SCE 8000 chassis without disconnecting them from the network and then reinstall them in the new SCE platform, so that traffic links are preserved even in a case of complete failure and replacement of the Cisco SCE 8000 platform. (See the [“Replacing the Optical Bypass Module Without Disrupting Traffic on the Link”](#) section on page 9-33.)

## Optical Bypass Functionality

The optical bypass module is connected bump-in-the-wire in the 10-GBE link. It is then connected to the Cisco SCE 8000 platform with two types of connections:

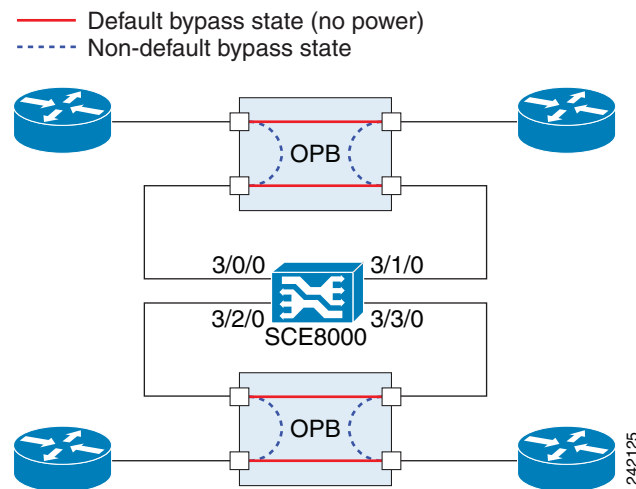
- 10 GBE optical connections for data link traffic—10 GBE connections from the optical bypass module to one pair of the 10 GBE SPA ports.
- Control connection—Connection to the RJ-11 External Bypass connector on the Cisco SCE 8000-SCM, so the optical bypass is activated if the Cisco SCE 8000 platform fails.

## Optical Bypass Module Connectivity

The optical bypass module functions as follows:

- Under normal conditions, the bypass module directs traffic to flow via the Cisco SCE 8000. (See [Figure 2-7](#).)
- Under failure conditions, the optical bypass shortcuts the interfaces that are connected to the traffic link, and all traffic flows through the optical bypass module, bypassing the SCE platform. (See [Figure 2-7](#).)

**Figure 2-7**      **Optical Bypass Module Connectivity**



## Optical Bypass Module (OPB-SCE8K)

There are two types of optical bypass modules to support different optic types:

- OPB-SCE8K-SM supports Single-Mode optics and should be used with Cisco SCE 8000 equipped with Single-Mode optics.
- OPB-SCE8K-MM supports Multi-Mode optics and should be used with Cisco SCE 8000 equipped with Multi-Mode optics.

The optical bypass module is installed either internally, in slot #4 of the Cisco SCE 8000 chassis or in an external mounting panel in the rack.

Up to two optical bypass modules can be mounted internally, supporting inline insertion into two links.

Up to four optical bypass modules can be mounted using an external mount panel (OPB-SCE8K-EXT-PNL). A single panel can serve two Cisco SCE 8000 platforms, each cutting two links or up to four Cisco SCE 8000 platforms, each cutting a single link. The optical bypass module is displayed in [Figure 2-8](#). [Table 2-8](#) lists the optical bypass module ports, and [Table 2-9](#) lists the optical bypass module LEDs.

**Figure 2-8**      **Optical Bypass Module**

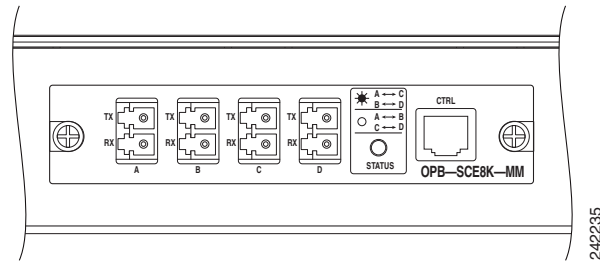


**Table 2-8**      **Optical Bypass Module Ports**

| Port             | Quantity | Description                                                                      | Connect This Port To                                                                                                                                                                                   |
|------------------|----------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 GBE Line port | 4        | 10 GBE ports A through D<br>Duplex LC, panel mount adaptor for LC/UPC connectors | SPA interfaces on the Cisco SCE 8000.<br><br>See the <a href="#">“Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module”</a> section on page 6-14 for further information. |
| CTRL             | 1        | RJ-11 port                                                                       | RJ-11 Optical Bypass port on the Cisco SCE 8000-SCM-E.                                                                                                                                                 |

**Table 2-9**      **Optical Bypass Module LEDs**

| LEDs   | Description                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | The Status LED indicates the operational status of the optical bypass module, as follows: <ul style="list-style-type: none"> <li>Green—Bypass module has been de-activated (traffic flows through the Cisco SCE 8000 platform)</li> <li>Off—Bypass module is active (traffic does not flow through the Cisco SCE 8000 platform)</li> </ul> |

## Optical Bypass Module Specifications

This section describes the following:

### Fiber Cable Type

The fiber cable type within the Optical Bypass Module area as follows:

- OPB-SCE8K-MM: 50 um core
- OPB-SCE8K-SM: SMF-28

Maximum optical path (fiber length of two ports) is 600 m.

### Switching Time

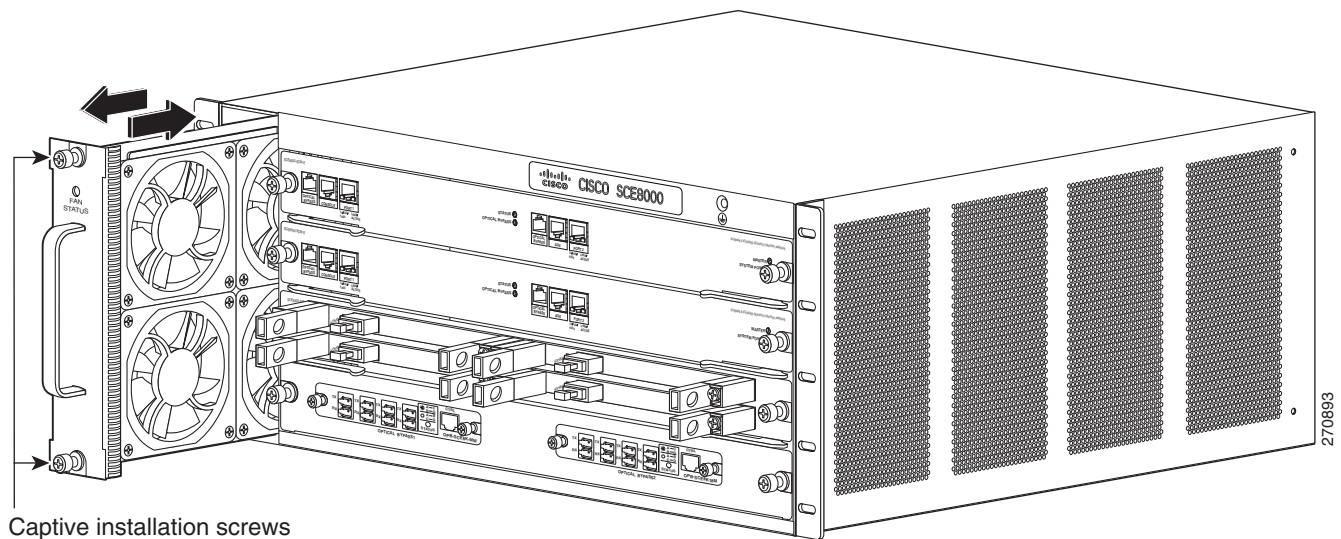
Switching time is measured from trigger to stable 90% optical output.

- Typical switching time: 3 ms
- Maximal switching time: 10 ms

## Fan Assembly

The system fan assembly, located in the chassis, provides cooling air for the installed modules (See [Figure 2-9](#)). Sensors on the fan assembly and within the system monitor the internal air temperatures. If the air temperature exceeds a preset threshold, the environmental monitor displays warning messages.

**Figure 2-9** Fan Assembly



If an individual fan within the assembly fails, the FAN STATUS LED turns red. To replace a fan assembly, see [“Removing and Replacing the Fan Assembly”](#) section on page 9-13.

## Power Supplies

The Cisco SCE 8000 platform supports redundant AC- or DC-input power supplies. The following power supplies are available for the Cisco SCE 8000 platform:

- 2700 W AC input (PWR-2700-AC/4): uses an external power cord directly connected to the AC power supply. (See [Figure 2-10](#).)
- 2700 W DC input (PWR-2700-DC/4): uses an external terminal block on the back side of the chassis for input power connection. (See [Figure 2-11](#).)

**Figure 2-10** *PWR-2700-AC/4*

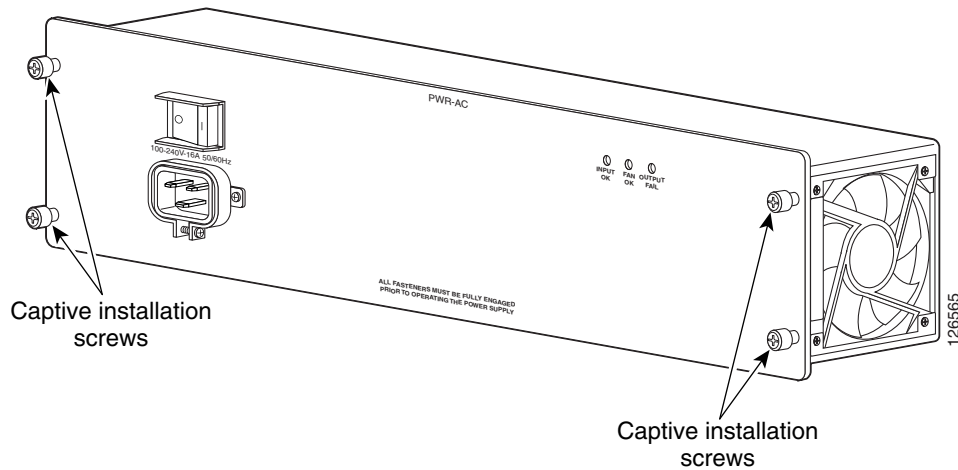
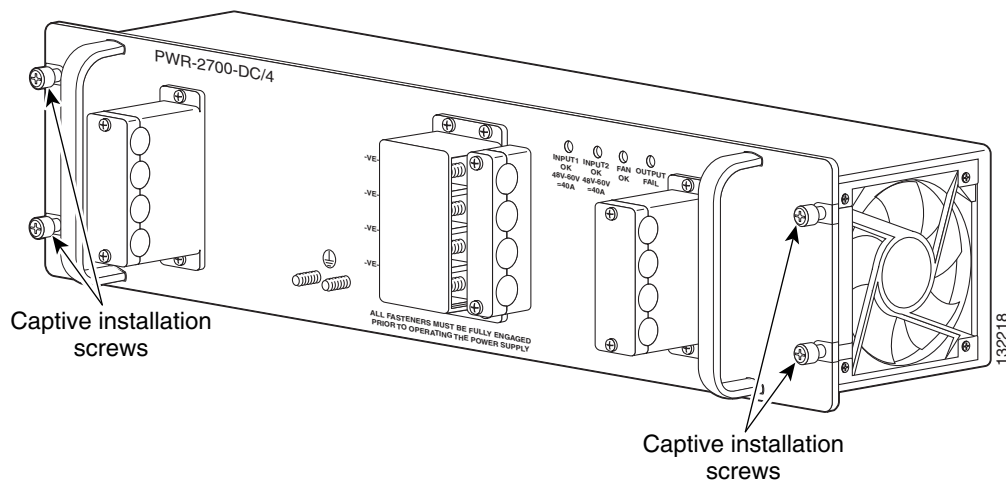


**Figure 2-11** *PWR-2700-DC/4*



The AC-input and DC-input power supplies support redundancy. When power is removed from one supply, the redundant power feature causes the second supply to produce full power.

## Power Supply Cooling

Power supplies have built-in fans and are completely self-cooling. Air enters from the right of the fan and exits through the left.

## Load Sharing

With two power supplies, each power supply concurrently provides approximately half of the required power to the system. If one power supply fails, the second power supply immediately assumes full power to maintain uninterrupted system operation. The second power supply enables load sharing and fault tolerance automatically; no software configuration is required.

# Checking the Shipping Container Contents

Use the Cisco SCE 8000 Component List to check the contents of the Cisco SCE 8000 platform shipping container.



**Tip**

Do not discard the shipping container when you unpack the Cisco SCE 8000. Flatten the shipping cartons and store them with the pallet. You need these containers to move or ship the Cisco SCE 8000.

## Cisco SCE 8000 Component and Accessory Lists

Table 2-10 lists the Cisco SCE 8000 components.

**Table 2-10**      *Cisco SCE 8000 Component List*

| Component                                         | Description                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------|
| Cisco SCE 8000-SCM-E                              | Cisco SCE 8000 Service Control Module.                                        |
| Cisco SCE 8000-SIP                                | Cisco SCE 8000 SPA Jacket card Interface Processor.                           |
| 2 or 4 SPA Jacket cards                           | SPA Interface. See the following list of supported SPA models.                |
| 2 or 4 XFP Optics                                 | XFP optic modules. See the following list of supported XFP models.            |
| 2 Cisco PWR-2700-AC/4 or<br>2 Cisco PWR-2700-DC/4 | Cisco power supply units, AC or DC.<br>Hot swappable, redundant power supply. |
| Cisco SCE 8000-FAN                                | Redundant fans unit.                                                          |

Table 2-11 lists the Cisco SCE 8000 accessories.

**Table 2-11**      *Cisco SCE 8000 Accessory List*

| Accessory                 | Description                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management cables         | <ul style="list-style-type: none"> <li>Gigabit Ethernet cable for connecting to the Management ports</li> <li>RS-232 serial cables (DB-9 to RJ-45 and DB-25 to RJ-45) for connecting to a local terminal</li> </ul> |
| Power cables              | Two AC power supply cords, if ordered with AC-input power supply units                                                                                                                                              |
| Grounding kit 69-0815-01  | <ul style="list-style-type: none"> <li>Grounding lug</li> <li>Two M4 hex-head screws with locking washers</li> </ul>                                                                                                |
| Optical Bypass module kit | <ul style="list-style-type: none"> <li>Optical Bypass Module</li> <li>Control Cable (2 m)</li> <li>Control Cable (40 cm)</li> </ul>                                                                                 |

**Note**

Cisco does not ship the entire Cisco SCE 8000 documentation set automatically with each system. You must specifically order the documentation as part of the sales order. If you ordered documentation and did not receive it, we will ship the documents to you within 24 hours. To order documents, contact a customer service representative.

# Cisco SCE 8000 Installation Checklist

To assist you with your installation and to provide a historical record of what was done by whom, photocopy the following Cisco SCE 8000 Installation Checklist (See [Table 2-12](#)). Indicate when each procedure or verification is completed. When the checklist is completed, place it in your site log along with the other records for your new Cisco SCE 8000 platform.

**Table 2-12** *Cisco SCE 8000 Installation Checklist*

| Task                                                                                                                                                                        | Verified By | Date |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------|
| Date Cisco SCE 8000 received                                                                                                                                                |             |      |
| Cisco SCE 8000 and all accessories unpacked                                                                                                                                 |             |      |
| Safety recommendations and guidelines reviewed                                                                                                                              |             |      |
| Topology verified: number of Cisco SCE 8000 platforms, number of links, and whether inline or receive-only                                                                  |             |      |
| Installation Checklist copied                                                                                                                                               |             |      |
| Site log established and background information entered                                                                                                                     |             |      |
| Site power voltages verified                                                                                                                                                |             |      |
| Site environmental specifications verified                                                                                                                                  |             |      |
| Required passwords, IP addresses, device names, and so on, needed for initial configuration available (see <a href="#">“Initial Setup Parameters” section on page 5-3</a> ) |             |      |
| Required tools available                                                                                                                                                    |             |      |
| Network connection equipment available                                                                                                                                      |             |      |
| Cisco SCE 8000 mounted in rack                                                                                                                                              |             |      |
| System grounding established, if required                                                                                                                                   |             |      |
| AC/DC power cables connected to AC/DC sources and Cisco SCE 8000 chassis                                                                                                    |             |      |
| Optical bypass modules installed (optional)                                                                                                                                 |             |      |
| Console port set for 9600 baud, 8 data bits, no parity, and 1 stop bit (9600 8N1)                                                                                           |             |      |
| ASCII terminal attached to console port                                                                                                                                     |             |      |
| Management port is operational                                                                                                                                              |             |      |
| Network interface cables and devices connected                                                                                                                              |             |      |
| System power turned on                                                                                                                                                      |             |      |
| System boot complete (Status LED is on)                                                                                                                                     |             |      |
| 10 GBE line ports operational                                                                                                                                               |             |      |
| Correct hardware configuration displayed after system banner appears                                                                                                        |             |      |



# Cisco SCE 8000 Topology and Topology-Related Parameters

---

Revised: February 18, 2015

## Introduction

This chapter describes the possible deployment topologies of the Cisco SCE 8000 and explains how to configure the relevant parameters correctly for each topology:

- [The Cisco SCE 8000 Platform, page 3-1](#)
- [Topology Considerations, page 3-2](#)
- [Physical Topologies, page 3-4](#)
- [Link Continuity, page 3-11](#)
- [Topology-Related Parameters, page 3-13](#)
- [Asymmetric Routing Topology, page 3-16](#)

## The Cisco SCE 8000 Platform

The Cisco SCE 8000 is a solution for dual links with load sharing and asymmetrical routing and support for fail-over between two SCE platforms.

The Cisco SCE 8000 is built to support wire speed processing of full-duplex 10 GBE streams. The Cisco SCE 8000 can, therefore, be deployed in a multi-link environment in several different topologies.

- **Single Cisco SCE 8000 topology**—Provides the ability to process both directions of a bi-directional flow, processing both the upstream and downstream paths of a flow, even if they traverse different links.
- **Dual Cisco SCE 8000 topology (cascade)**—Cascaded Cisco SCE 8000s provide high-availability and fail-over solution and maintain the line and service in case of Cisco SCE 8000 failure
- **Multi-Gigabit Service Control Platform (MGSCP) topology**—For scalability, the Cisco SCE 8000 platform supports the option to connect a multiple number of SCE platforms to a Cisco 7600 Series router used to perform load-balancing between the platforms.

# Topology Considerations

There are several issues that must be considered in order to arrive at the optimum configuration of the topology-related parameters:

- **Functionality**

Will the system be used solely to monitor traffic flow, with report functionality only, or will it be used for traffic flow control, with enforcement as well as report functionality?

- **Monitoring and Control**—The Cisco SCE 8000 monitors and controls traffic flow. Decisions are enforced by the Cisco SCE 8000 depending on the results of the monitoring functions of the Cisco SCE 8000 and the configuration of the Service Control Application for Broadband or Mobile solution.

To perform control functions, the Cisco SCE 8000 must be physically installed as an inline installation.

- **Monitoring only**—The Cisco SCE 8000 monitors traffic flow, but cannot control it.

Either an inline installation or an optical splitter or port SPAN installation may be used for monitoring only.

- **Size**

The Cisco SCE 8000 deployment can range from a single 10 GBE link to multiple platforms in a MGSCP topology.

A complete discussion on sizing the system is beyond the scope of this document. Information about the number of Cisco SCE 8000 platforms required is related to the design considerations 'per link' (topology and redundancy factors) rather than to overall sizing of the system.

- **Redundancy**

Must the system be designed to guarantee uninterrupted Cisco SCE 8000 functionality? If so, there must be a backup Cisco SCE 8000 platform (or a backup for each platform in an MGSCP topology) to assume operation in case of failure of the primary device.

A backup SCE platform is connected in a cascade configuration with the primary SCE platform so that, although all processing is performed only in the active Cisco SCE 8000, the standby Cisco SCE 8000 is constantly updated with all the necessary information so that it can instantly take over processing the traffic on the data links should the active Cisco SCE 8000 fail.

A MGSCP topology with multiple Cisco SCE 8000 platforms provides more sophisticated redundancy options, but the basic decision on each link is the same: does it require a standby SCE platform or not?

- **Link continuity**

How should the Cisco SCE 8000 respond to platform failure in relation to link continuity? Should traffic flow continue even though the unit is not operating, or should it be halted until the platform is repaired or replaced?

If link continuity is a high priority, an external optical bypass module can be installed on the link. (See [“Link Continuity” section on page 3-11](#) and [“The Cisco SCE 8000 Optical Bypass” section on page 2-12.](#))



**Note**

---

In cascade configuration, installation of an external optical bypass module is required.

---

These issues determine two important aspects of system deployment and configuration:

- Physical topology of the system—Actual physical placement and connection of the Cisco SCE 8000 platform or platforms in the system.
- Topology-related configuration parameters—Correct values for each parameter must be ascertained before configuring the system to make sure that the system functions in the desired manner.

# Physical Topologies

The following sections are descriptions of several physical topologies that Cisco SCE 8000 supports:

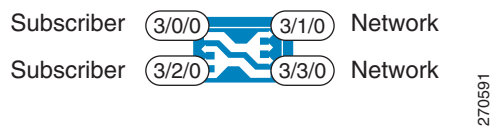
- [Cisco SCE 8000 Interface Numbering, page 3-4](#)
- [Single Cisco SCE 8000 Topologies, page 3-4](#)
- [Dual Cisco SCE 8000 Topology \(Cascade\), page 3-8](#)
- [Multi-Gigabit Service Control Platform \(MGSCP\) Topology, page 3-9](#)

## Cisco SCE 8000 Interface Numbering

[Figure 3-1](#) shows the numbering of the Cisco SCE 8000 interfaces as indicated in the topology diagrams in this chapter. The interface numbering is explained as follows:

- First digit is the slot number (always 3).
- Second digit is the number of the sub-slot or SPA module (0 to 3).
- Third digit is the number of the interface on the designated SPA module (always 0).
- Interfaces 3/0/0 and 3/2/0 are on the two left SPA modules and are the Subscriber-side interfaces.
- Interfaces 3/1/0 and 3/3/0 are on the two right SPA modules and are the Network-side interfaces.

**Figure 3-1** Cisco SCE 8000 Interface Numbering



## Single Cisco SCE 8000 Topologies

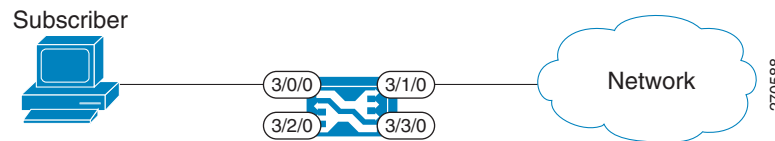
A single Cisco SCE 8000 supports both single 10 GBE link and dual 10 GBE link topologies:

- [Single Link: Inline Topology, page 3-5](#)
- [Dual Link: Inline Installation, page 3-5](#)
- [Single Link: Receive-only Topology, page 3-6](#)
- [Dual Link: Receive-Only Topology, page 3-7](#)

## Single Link: Inline Topology

Typically, the Cisco SCE 8000 is connected in a full duplex 10 GBE link between two devices (Router, BRAS, and so on). When the Cisco SCE 8000 is installed as an inline installation, it physically resides on the data link between the subscribers and the network (see [Figure 3-2](#)).

**Figure 3-2** *Single Link: Inline Topology*



When configuring the Cisco SCE 8000, an inline installation is referred to as “inline” connection mode.

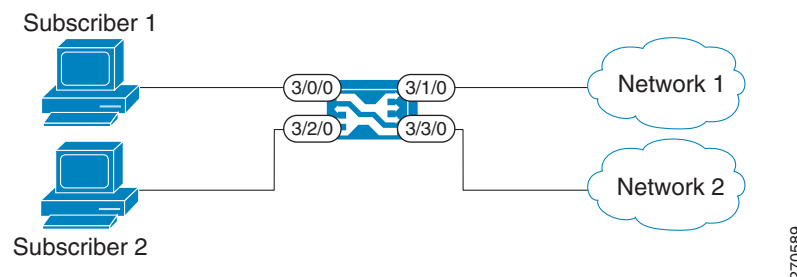
## Dual Link: Inline Installation

In this topology, one Cisco SCE 8000 is connected inline in two full duplex, 10 GBE links (see [Figure 3-3](#)).

In case the two links are load-shared, asymmetrical routing might occur, and some of the flows may be split, that is, the upstream packets of the flow go on one link, and the downstream packets go on the other link.

When installed in this topology, the Cisco SCE 8000 completely overcomes this phenomenon, and provides its normal functionality as if asymmetrical routing were not occurring in the two links.

**Figure 3-3** *Dual link: Inline Installation*

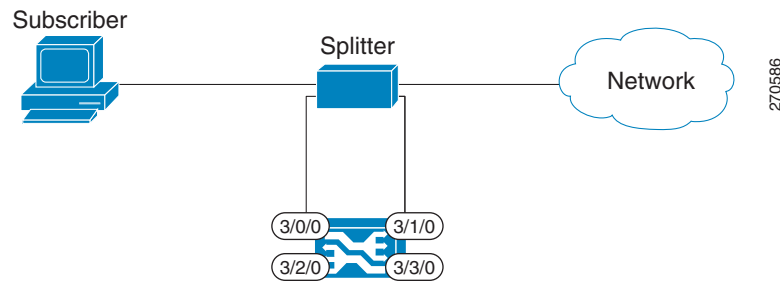


This topology supports both monitoring and control functionality, and is referred to as “inline” connection mode.

## Single Link: Receive-only Topology

In this topology, an optical splitter resides physically on the 10 GBE link between the subscribers and the network (see [Figure 3-4](#)). The traffic passes through the optical splitter, which splits traffic to the Cisco SCE 8000. The Cisco SCE 8000, therefore, only receives traffic and does not transmit.

**Figure 3-4**      **Single Link: Receive-only Topology**



When configuring the Cisco SCE 8000, an optical splitter topology is referred to as “receive-only” connection mode.

**Note**

In an optical splitter topology, the Cisco SCE 8000 only enables traffic monitoring functionality.

**Note**

When implementing receive-only topologies with a switch, the switch must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN-ports destinations.

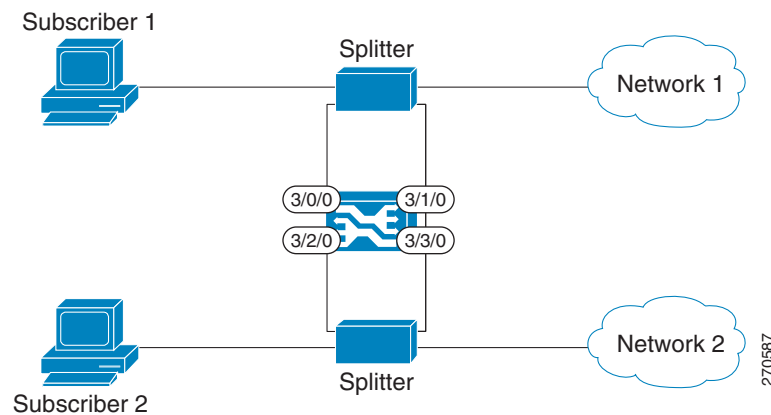
## Dual Link: Receive-Only Topology

In this topology, one Cisco SCE 8000 is connected in receive-only mode to two full duplex, 10 Gig links using optical splitters (see Figure 3-5). If the two links are load-shared, asymmetrical routing might occur, and some of the flows may be split, i.e. the upstream packets of the flow go on one link, and the downstream packets go on the other link.

When installed in this topology, the Cisco SCE 8000 completely overcomes this phenomenon, and provides its normal monitoring functionality as if asymmetrical routing were not occurring in the two links.

This installation supports monitoring functionality only, and is configured as “receive-only” connection mode.

**Figure 3-5** *Dual Link: Receive-Only Topology*



### Note

When implementing receive-only topologies with a switch, the switch must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN-ports destinations.

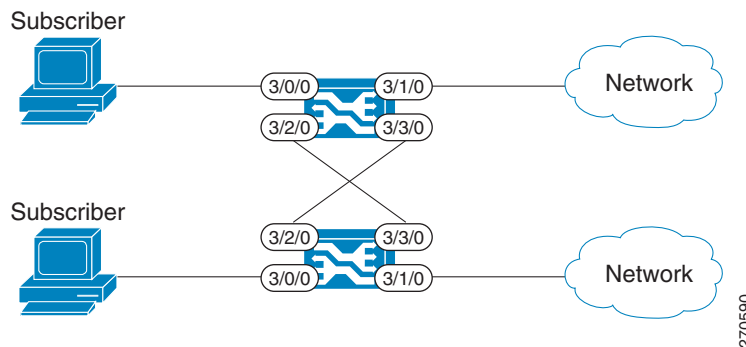
## Dual Cisco SCE 8000 Topology (Cascade)

In this topology, two cascaded Cisco SCE 8000s are used. This allows a switchover solution, where in case of a failure of one Cisco SCE 8000, the functionality that the Cisco SCE 8000 provides is preserved by the redundant platform (see [Figure 3-6](#)).

This topology allows both control and monitoring functionality where redundancy is required and “inline” connection is used. The two Cisco SCE 8000s are cascaded, so the primary Cisco SCE 8000 processes the traffic of the two links, while the secondary Cisco SCE 8000 only bypasses the traffic of its links to the primary Cisco SCE 8000 for processing, and then bypasses the processed traffic back to the link. The two Cisco SCE 8000s also exchange keep-alive messages and subscriber state information.

In case the primary Cisco SCE 8000 fails, the two Cisco SCE 8000s switch their roles, and this way switchover is provided.

**Figure 3-6 Two Cascaded Cisco SCE 8000 Platforms**



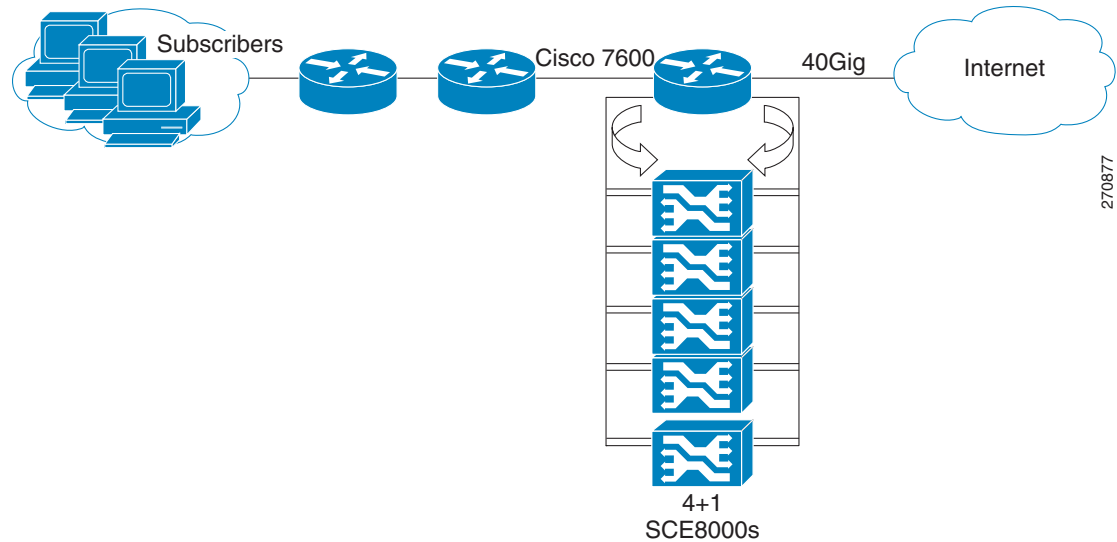
This switchover solution preserves the Cisco SCE 8000 functionality and the network link:

- The two Cisco SCE 8000s are simultaneously aware of the subscriber contexts, and subscriber states are constantly exchanged between them, such that if the primary Cisco SCE 8000 fails, the secondary can take over with minimum state loss.
- When one Cisco SCE 8000 fails (depending on the type of failure) its link traffic is still bypassed to the functioning Cisco SCE 8000 and processed there, so the traffic processing continues for both the links.
- The bypass of the traffic through the failed Cisco SCE 8000 is configurable, and the user may choose to always cutoff the line that goes through the failed Cisco SCE 8000. In this case network redundancy protocols like HSRP are responsible for identifying the line cutoff and switching all the traffic to go through the functioning Cisco SCE 8000.
- In addition, it is possible to configure the Cisco SCE 8000 to use the external optical bypass device so that if any failure of the Cisco SCE 8000 occurs, it is used to provide link continuity. This ensures full link continuity at the expense of providing asymmetric routing functionality.

## Multi-Gigabit Service Control Platform (MGSCP) Topology

In this topology, multiple Cisco SCE 8000 platforms are connected to a Cisco 7600 Series router, which acts as a dispatcher between the platforms (see [Figure 3-7](#)). The router contains two EtherChannels (ECs), one for the subscriber side and one for the network side, that perform load balancing for the SCE platform traffic. Traffic enters the first router, is distributed between the SCE platforms by the subscriber-side EC and then returns to the router so it can be forwarded to its original destination.

**Figure 3-7 Basic MGSCP Topology**



There are several variables to be considered in the MGSCP topology. Two of the main factors to be considered include:

- [Types of SCE Platform Redundancy, page 3-9](#)
- [Redundant Cisco 7600 Series Router, page 3-10](#)

### Types of SCE Platform Redundancy

- **All Active**

All ports in the EC and all SCE platforms are active. If there is a failure in one of the SCE platforms, the links on the related ports in the EC go down and the EC automatically excludes it from the load distribution. The load then is distributed between the remaining active SCE platforms.

Because the Cisco SCE 8000 supports two links, this configuration requires one SCE platform per two links (two EC ports).

- **N+1**

'N' SCE platforms are active and one platform is on standby. The EC ports connected to the standby SCE platform must be configured as standby ports. In the case of failure of one of the SCE platforms, the EC ports connected to the failing SCE platform are shut, and the standby EC ports that are connected to the standby SCE platform are activated.

Because the Cisco SCE 8000 supports two links, this configuration requires one SCE platform per two links (two EC ports), plus one extra SCE platform for standby.

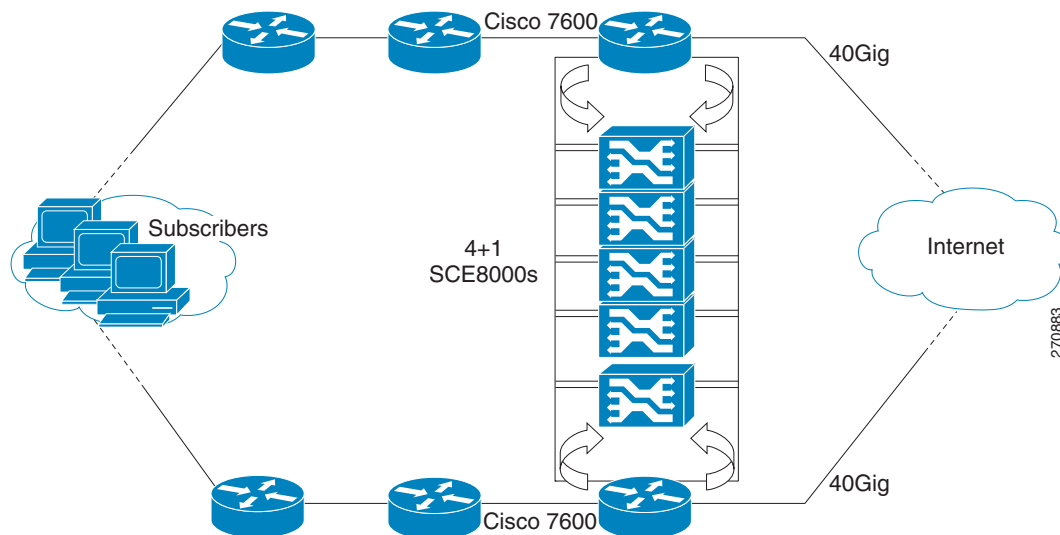
The standby SCE platform must be connected to the two highest-numbered ports, because EC behavior automatically designates these as the standby ports.

## Redundant Cisco 7600 Series Router

Two Cisco 7600 Series routers can be used to provide network redundancy (see [Figure 3-8](#)).

In this topology, one link on each Cisco SCE 8000 platform is connected to each router. Therefore, one SCE platform is required for each link.

**Figure 3-8** *MGSCP with Redundant Router*



# Link Continuity

The internal bypass mechanism of the Cisco SCE 8000 allows traffic to continue to flow, if desired, even if the device itself is not fully functioning. In addition, the Cisco SCE 8000 is designed with the ability to control up to two external optical bypass devices (one per link). This is needed because the internal bypass mechanism cannot maintain traffic flow in all cases.

When the Cisco SCE 8000 is connected to the network through an optical splitter, a failure of the Cisco SCE 8000 does not affect the traffic flow, as the traffic continues to flow through the optical splitter.

- [Internal Bypass Mechanism, page 3-11](#)
- [External Optical Bypass, page 3-11](#)

## Internal Bypass Mechanism

The Cisco SCE 8000-SIP module includes a bypass mechanism that is enabled upon Cisco SCE 8000 failure.

The Cisco SCE 8000-SIP supports the following three modes:

- **Bypass**—The bypass mechanism preserves the network link, but traffic is not processed for monitoring or for control.
- **Forwarding**—This is the normal operational mode, in which the Cisco SCE 8000 processes the traffic for monitoring and control purposes.
- **Cutoff**—There is no forwarding of traffic, and the physical link is forced down (cutoff functionality at layer 1).

The SPA Interface Processor card cannot preserve the link in the following circumstances:

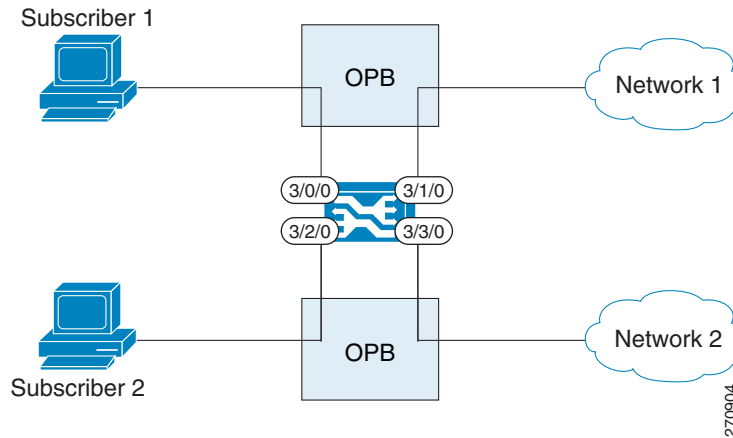
- During platform reboot (SW reload), there is an 11-second period during which the link is forced down (cutoff functionality). If any routing or spanning tree protocols are used in the network, this delay may be extended.
- During a power failure (The Cisco SCE 8000 has two power supplies. A power failure occurs only when both of them fail).
- Under certain types of failure within the SIP module, the SPA cards, or the XFP optic modules.

## External Optical Bypass

When a separate bypass mechanism is required, an external optical bypass device can be used to provide dependable link continuity. The external optical bypass device can be installed either inside the Cisco SCE 8000 chassis or be rack-mounted externally. The external optical bypass device can also be controlled manually by specific CLI commands.

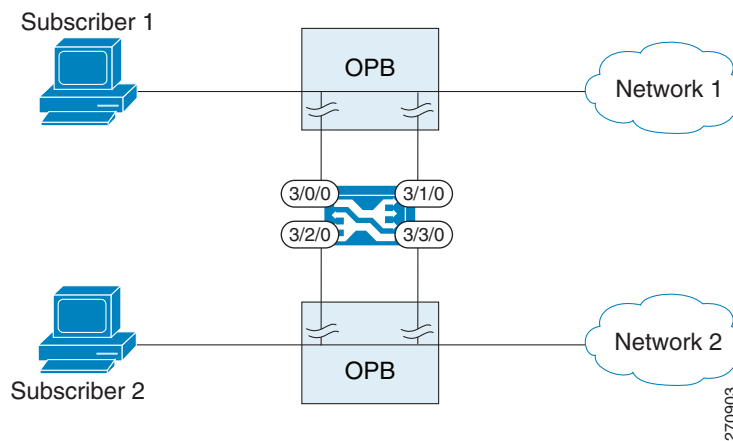
Under normal operating conditions, traffic flows through the link as usual, with the exception that the optical bypass module sits on the link (see [Figure 3-9](#)).

**Figure 3-9** *Optical Bypass Under Normal Operating Conditions*



If the Cisco SCE 8000 platform fails, traffic flows through the optical bypass module, bypassing the SCE 8000, so that traffic on the link is maintained (see [Figure 3-10](#)).

**Figure 3-10** *Optical Bypass Under Failure Conditions*



**Note**

In cascade configuration, installation of the optical bypass module is highly recommended.

This optical bypass module can be added to link without altering the basic characteristics of the topology. (The installation procedure and the actual connections are somewhat different when the optical bypass module is used, see [“Optical Bypass Module Connectivity”](#) section on page 6-9.)

For more information about the external bypass module, see [“The Cisco SCE 8000 Optical Bypass”](#) section on page 2-12.

# Topology-Related Parameters

See the following sections to determine the correct values for all topology-related parameters before beginning to run the initial setup of the Cisco SCE 8000:

- [Connection Mode Parameter, page 3-14](#)
- [sce-id Parameter, page 3-14](#)
- [Priority, page 3-14](#)
- [On-Failure Mode Parameter, page 3-15](#)

There are four topology-related parameters:

- **Connection mode**—Can be any one of the following, depending on the physical installation of the Cisco SCE 8000 (See [Connection Mode Parameter, page 3-14](#)):
  - Inline—single Cisco SCE 8000 inline
  - Receive-only—single Cisco SCE 8000 receive-only
  - Inline-cascade—two inline Cisco SCE 8000 platforms cascaded
  - Receive-only-cascade—two receive-only Cisco SCE 8000 platforms cascaded
- **sce-id**—In cascaded topologies, defines which link is connected to this SCE platform.

The sce-id parameter, which identifies the SCE platform, replaces the physically-connected-link parameter, which identified the link. This change was required with the introduction of the Cisco SCE 8000 GBE platform, which supports multiple links.

In the Cisco SCE 8000 10 GBE, the number assigned to the sce-id parameter (0 or 1) is defined as the of number of the physically connected link.

**Note**

For backward compatibility, the physically-connected-links parameter is currently still recognized.

- **Priority**—This parameter defines which is the primary Cisco SCE 8000 (See [Priority, page 3-14](#).) It is applicable only in a cascade topology
- **On-failure**—This parameter determines whether the system cuts the traffic or bypasses it when the Cisco SCE 8000 either has failed or is booting. Traffic bypass can be achieved either through the external optical bypass device or through the internal bypass mechanism of the SPA interface processor. It is not applicable to receive-only topologies. (See the “[On-Failure Mode Parameter](#)” section on page 3-15.)

These parameters are configured via the **connection-mode** command.

## Connection Mode Parameter

The connection mode parameter refers directly to the physical topology in which the Cisco SCE 8000 is installed. The connection mode depends on two factors:

- **Inline/Receive-only:**
  - **Inline**—Cisco SCE 8000 resides on the data link between the subscriber side and the network side, thus both receiving and transmitting packets.
  - **Receive-only**—Cisco SCE 8000 does not reside physically on the data link. Data is forwarded to the Cisco SCE 8000 via an external optical splitter. The Cisco SCE 8000 itself only receives and does not transmit.
- **Cascade**—Indicates a two Cisco SCE 8000 topology where the two Cisco SCE 8000 platforms are connected via the cascade ports.

The connection mode parameter is determined by the physical deployment of the Cisco SCE 8000, as follows:

- Single Cisco SCE 8000 inline installation = **Inline** connection mode.
- Single Cisco SCE 8000 optical splitter installation = **Receive-only** connection mode.
- Two-platform cascaded Cisco SCE 8000 inline installation = **Inline-cascade** connection mode.
- Two-platform cascaded Cisco SCE 8000 optical splitter installation = **Receive-only-cascade** connection mode.

## sce-id Parameter

A cascade topology supports two traffic links. In the Cisco SCE 8000 10 GBE, this parameter defines which link is connected to which Cisco SCE 8000 platform. The name of the parameter refers to its use in the Cisco SCE 8000 GBE platform, for which it actually defines a specific SCE platform. However, in the case of the Cisco SCE 8000 10 GBE, simply specify the number of the physically connected link for this parameter. Assign a value of 0 or 1.



**Tip**

Alternatively, you can still use the physically-connected-links parameter, which is still supported for backward compatibility. Assign a value of link-0 or link-1.

## Priority

In a cascade topology, the user must define the priority of each Cisco SCE 8000:

- **Primary**—Primary Cisco SCE 8000 is active by default
- **Secondary**—Secondary Cisco SCE 8000 is the default standby

These defaults apply only when both devices are started together. However, if the primary Cisco SCE 8000 fails and then recovers, it does not revert to active status, but remains in standby status, while the secondary device remains active.

## On-Failure Mode Parameter

The *on-failure* mode parameter configures the action taken by a failed box when a failure is detected.

As described in the “[Internal Bypass Mechanism](#)” section on page 3-11, the SPA Interface Processor card supports three different modes. The **Bypass** and **Cutoff** modes are possible when the Cisco SCE 8000 is not operational because of platform failure or boot. The **Forwarding** mode enables control of traffic flow and is not compatible with the non-operational status.

The following *on-failure* modes are possible:

- **Bypass**—The SPA interface card forwards traffic between the two ports of each link with no intervention of the control application running in the Cisco SCE 8000 platform. This is also known as 'electrical bypass'.

In a cascade setup, this allows the traffic of the link connected to the failed box to be passed to the active box for processing.

- **Cutoff**—There is no forwarding of traffic. The link is forced down, resulting in traffic cutoff at Layer1.
- **External-bypass**—The external optical bypass device is used to bypass traffic, maintaining link continuity at all times.

In a single Cisco SCE 8000 topology, the value of this parameter is determined by whether or not the link can be completely cut when the Cisco SCE 8000 fails, or whether traffic flow should continue across the link in spite of platform failure. In the latter case, the **External-bypass** mode is the recommended setting, and is therefore the default value for the *on-failure* mode parameter.

In a dual cascaded Cisco SCE 8000 topology, the default on-failure mode is Bypass, because it preserves full traffic processing functionality on both links in most single box failures (as long as the SPA interface card is functioning properly).

- **Cutoff** mode is suggested for the following:
  - Non-redundant inline topology if value-added services (such as security) are crucial and are more important than maintaining connectivity.
- **Bypass** mode is suggested for the following:
  - Non-redundant inline topology if connectivity is of high importance.
  - In redundant inline setups, if cutoff or traffic loss on a single link for a period of up to 10 minutes (during a rare event of a SPA interface card failure) can be tolerated.
- **External-bypass** mode is suggested for the following:
  - Non-redundant inline topology if connectivity is crucial.
  - Redundant inline setups, if connectivity is crucial. When this mode is used, the link connected to the failed box is not serviced, and the other link operates with asymmetric routing functionality.

## Asymmetric Routing Topology

In some Service Control deployments, asymmetrical routing occurs between potential service control insertion points. Asymmetrical routing can cause a situation in which the two directions of a bi-directional flow pass through different SCE platforms, resulting in each SCE platform seeing only one direction of the flow (either the inbound traffic or the outbound traffic).

This problem is typically solved by connecting the two SCE platforms in cascade mode (or through an MGSCP cluster), thereby making sure that both directions of a flow run through the same SCE platform. However, this is sometimes not feasible, because the SCE platforms sharing the split flow are geographically remote (especially common upon peering insertion). In this type of scenario, the asymmetric routing solution enables the SCE platform to handle such traffic, allowing SCA BB to classify traffic based on a single direction and to apply basic reporting and global control features to uni-directional traffic.

## Asymmetric Routing and Other Service Control Capabilities

Asymmetric routing can be combined with most other Service Control capabilities; however, there are some exceptions.

Service Control capabilities that cannot be used in an asymmetric routing topology include the following:

- Subscriber redirect.
- Subscriber notification.
- Any kind of subscriber integration. (Use subscriber-less mode or anonymous subscriber mode instead.)



# Installing the Cisco SCE 8000 Chassis

Revised: February 18, 2015

## Introduction

This chapter describes how to install a Cisco SCE 8000 chassis.

  
**Warning**

**Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**  
Statement 1030

  
**Warning**

**There is the danger of explosion if the battery is replaced incorrectly. The battery is not a user-serviceable part.**  
Statement 1015

  
**Warning**

**Class 1 laser product.**  
Statement 1008

  
**Warning**

**Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.**  
Statement 1056

  
**Warning**

**Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**  
Statement 1029

  
**Note**

Before you install, operate, or service the system, see the [Regulatory Compliance and Safety Information for the Cisco SCE8000 Platform](#). This guide contains important safety information you should know before working with the system.

**Caution**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

**Note**

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

**Note**

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

This chapter contains the following sections:

- [Preparing for Installation, page 4-3](#)
- [Installing the Cisco SCE 8000 Chassis in the Rack, page 4-15](#)
- [Connecting the System Ground, page 4-20](#)
- [Installing the Power Supplies in the Cisco SCE 8000 Chassis, page 4-22](#)

# Preparing for Installation

This section provides information about the following:

- [Safety, page 4-3](#)
- [Site Requirements, page 4-3](#)
- [Power Connection Guidelines, page 4-5](#)

## Safety



### Warning

**Read the installation instructions before connecting the system to the power source.**

Statement 1004



### Note

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.



### Note

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

## Site Requirements

This section provides site power requirements for the Cisco SCE 8000 chassis. Verify the site power before installation:

- [Preventing Electrostatic Discharge Damage, page 4-3](#)
- [Environmental Requirements, page 4-4](#)
- [Power Requirements, page 4-5](#)

## Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Port adapters and blades consist of printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Following are guidelines for preventing ESD damage:

- Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to an unfinished chassis surface.

- When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.
- When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.
- Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.
- Place a removed component board-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Never attempt to remove the printed circuit board from the metal carrier.

**Caution**

For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohm (Mohm).

## Environmental Requirements

Ensure adequate spacing between racks using the information in the following table. Keep all of the vents clear of obstructions, including dust and foreign conductive material, and away from the exhaust ports of other equipment. [Table 4-1](#) lists the chassis airflow requirements, and [Table 4-2](#) lists the Cisco SCE 8000 environmental requirements.

**Table 4-1 Chassis Airflow Requirements**

| Airflow Intake | Airflow Exhaust | Air Filter Option | Minimum Clearance (walls) | Minimum Horizontal Separation |
|----------------|-----------------|-------------------|---------------------------|-------------------------------|
| Right side     | Left side       | Not applicable    | 6 in (15 cm)              | 12 in (30.5 cm)               |

**Table 4-2 Ambient Temperature and Humidity Requirements for the Cisco SCE 8000**

| Specification | Acceptable Range                       |
|---------------|----------------------------------------|
| Temperature   | Nominal: 32°F to 104°F (0°C to 40°C)   |
|               | Storage: -4°F to 149°F (-20°C to 65°C) |

**Table 4-2 Ambient Temperature and Humidity Requirements for the Cisco SCE 8000**

| Specification     | Acceptable Range                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Relative humidity | Operating: 10% to 85%<br>Storage: 5% to 95% (non-condensing)                                                                                                                                                                                                                                                                                                                 |
| Heat dissipation  | <ul style="list-style-type: none"> <li>Single Cisco SCE 8000-SCM-E module: <ul style="list-style-type: none"> <li>AC Power: 950 W / 3250 BTUs</li> <li>DC Power: 1000 W / 3450 BTUs</li> </ul> </li> <li>Dual Cisco SCE 8000-SCM-E modules: <ul style="list-style-type: none"> <li>AC Power: 1350 W / 4600 BTUs</li> <li>DC Power: 1430 W / 4880 BTUs</li> </ul> </li> </ul> |

## Power Requirements



### Warning

**Read the installation instructions before connecting the system to the power source.**

Statement 1004

Follow these requirements when preparing your site for the Cisco SCE 8000 installation:

- The redundant power configuration provides a second, identical power supply to ensure that power to the chassis continues uninterrupted if one power supply fails or input power on one line fails.
- Connect each of the two power supplies to a separate input power source. If you fail to do this, your system might be susceptible to total power failure because of a fault in the external wiring or a tripped circuit breaker.
- To prevent a loss of input power, be sure that the total maximum load on each circuit supplying the power supplies is within the current ratings of the wiring and breakers.
- In some systems, you might use an uninterruptible power supply (UPS) to protect against power failures at your site. Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems like the Cisco SCE 8000, which can have substantial current draw fluctuations because of bursty data traffic patterns.

## Power Connection Guidelines

This section provides the guidelines for connecting the Cisco SCE 8000 AC and DC power supplies to the site power source:

- [AC-Powered Systems, page 4-5](#)
- [DC-Powered Systems, page 4-12](#)
- [Site Planning Checklist, page 4-14](#)

## AC-Powered Systems

- Each chassis power supply should have its own dedicated branch circuit.
- Circuits must be protected by a dedicated two-pole circuit breaker.

- For North America, the circuit breaker should be rated at 20A.
- For everywhere else, the circuit breaker should be sized according to the power supply input rating and local or national code requirements.
- AC power receptacles used to plug in the chassis must be the grounding type. The grounding conductors that connect to the receptacles should connect to protective earth ground at the service equipment.

**Warning**

**This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Statement 1024

**Note**

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

**Note**

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Table 4-3 lists the Cisco SCE 8000 AC power specifications.

**Table 4-3 Cisco SCE 8000 AC Power Specifications**

| Specification                    | Acceptable Range                                                                                                                                                                                                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PWR-2700-AC/4 minimum capability | 1350 W output (1650 W input)                                                                                                                                                                                                        |
| AC-input power consumption       | <ul style="list-style-type: none"> <li>• Single Cisco SCE 8000-SCM-E module:<br/>1000 W (8.3 A @ 120 VAC, 4.5 A @ 220 VAC)</li> <li>• Dual Cisco SCE 8000-SCM-E modules:<br/>1600 W (13.3 A @ 120 VAC, 7.27 A @ 220 VAC)</li> </ul> |
| AC-input voltage rating          | Low-line (120 VAC nominal)-85 VAC (min) to 132 VAC (max)<br>High-line (230 VAC nominal)-170 VAC (min) to 264 VAC (max)                                                                                                              |
| AC-input current rating          | 16 A maximum at 120 VAC<br>16 A maximum at 230 VAC                                                                                                                                                                                  |
| AC-fusing requirements           | For North America, the circuit breaker should be rated at 20 A.<br>For everywhere else, the circuit breaker should be sized according to the input current rating and local or national code requirements.                          |
| AC-input frequency rating        | 50/60 Hz (nominal) ( $\pm 3\%$ for full range)                                                                                                                                                                                      |

Table 4-4 lists the AC-input power cord options, specifications, and Cisco product numbers for the 2700 W AC-input power supplies. It also references power cord illustrations.

**Table 4-4 AC-Input Power Cord Options**

| Locale                                                      | Part Number         | Length                  | Plug Rating | Power Cord Reference Illustration |
|-------------------------------------------------------------|---------------------|-------------------------|-------------|-----------------------------------|
| North America (locking)                                     | CAB-GSR16-US(=)     | 14 feet (4.3m)          | 250VAC, 20A | <a href="#">Figure 4-1</a>        |
| Europe                                                      | CAB-GSR16-EU(=)     | 14 feet (4.3m)          | 250VAC, 16A | <a href="#">Figure 4-1</a>        |
| International                                               | CAB-AC16A-90L-IN(=) | 14 feet (4.3m)          | 250VAC, 16A | <a href="#">Figure 4-1</a>        |
| China                                                       | CAB-AC16A-CH=       | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-2</a>        |
| Continental Europe                                          | CAB-AC-2500W-EU=    | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-3</a>        |
| International                                               | CAB-AC-2500W-INT=   | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-4</a>        |
| Israel                                                      | CAB-AC-2500W-ISRL=  | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-5</a>        |
| Japan, North America (nonlocking plug) 200–240VAC operation | CAB-AC-2500W-US1=   | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-6</a>        |
| Japan, North America (locking plug) 200–240VAC operation    | CAB-AC-C6K-TWLK=    | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-7</a>        |
| Japan, North America 100–120VAC operation <sup>1</sup>      | CAB-7513AC=         | 14 feet (4.3 m)         | 125VAC, 20A | <a href="#">Figure 4-8</a>        |
| South Africa                                                | CAB-7513ACSA=       | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-9</a>        |
| Switzerland                                                 | CAB-ACS-16=         | 8 feet 2 inches (2.5 m) | 250VAC, 16A | <a href="#">Figure 4-10</a>       |
| Australia, New Zealand                                      | CAB-AC-16A-AUS=     | 14 feet (4.3 m)         | 250VAC, 16A | <a href="#">Figure 4-11</a>       |
| Power Distribution Unit (PDU)(=) <sup>1</sup>               | CAB-C19-CBN         | 9 feet (2.7 m)          | 250VAC, 16A | <a href="#">Figure 4-12</a>       |

1. The PDU power cable is designed for users who power their switch from a PDU. The end of the cable that plugs into the Cisco SCE 8000 chassis has a C19 connector; the other end of the cable that plugs into the PDU has a C20 connector.

**AC Power Cord Illustrations**

This section contains AC power cord illustrations.

**Figure 4-1 AC Power Cord Plugs and Appliance Coupler for the 2700 W Power Supply**

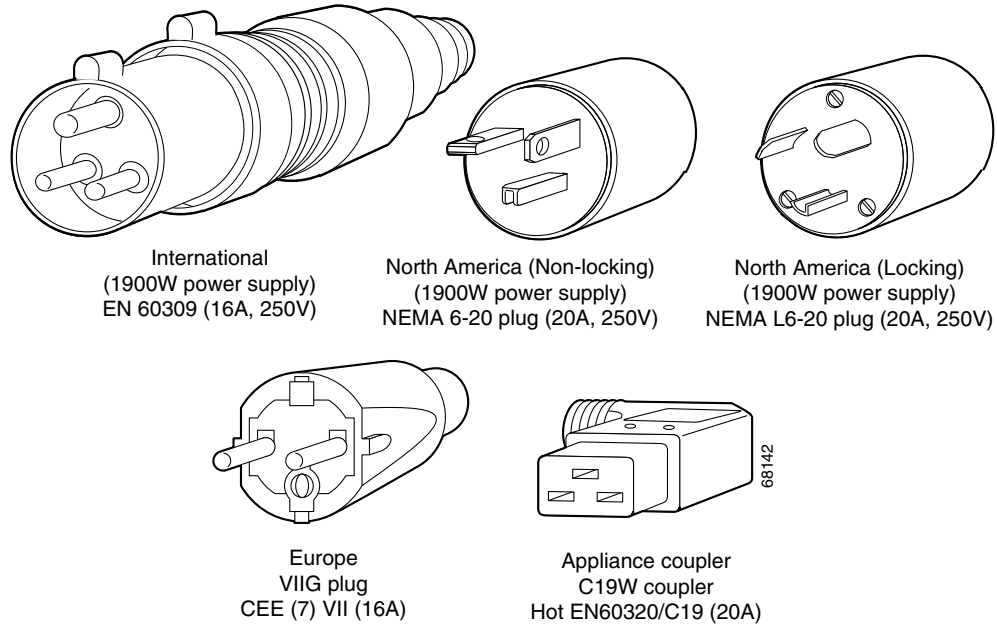
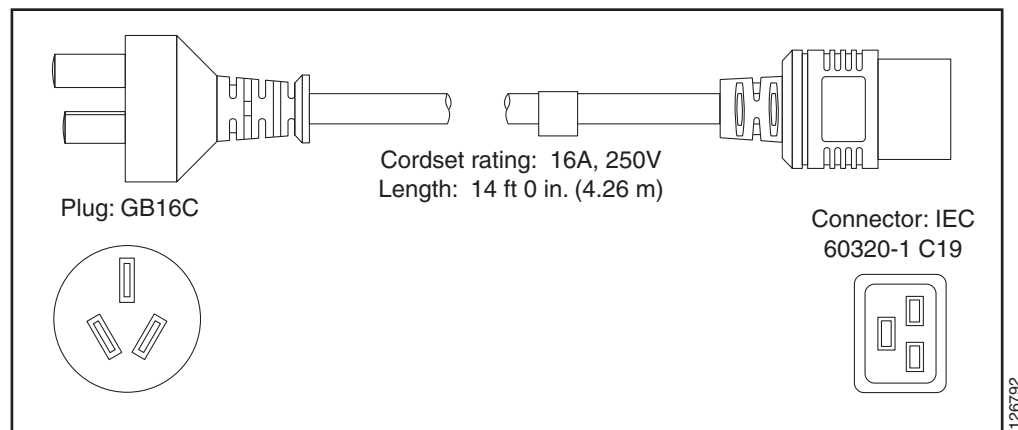


**Figure 4-2 CAB-AC16A-CH=**



126792

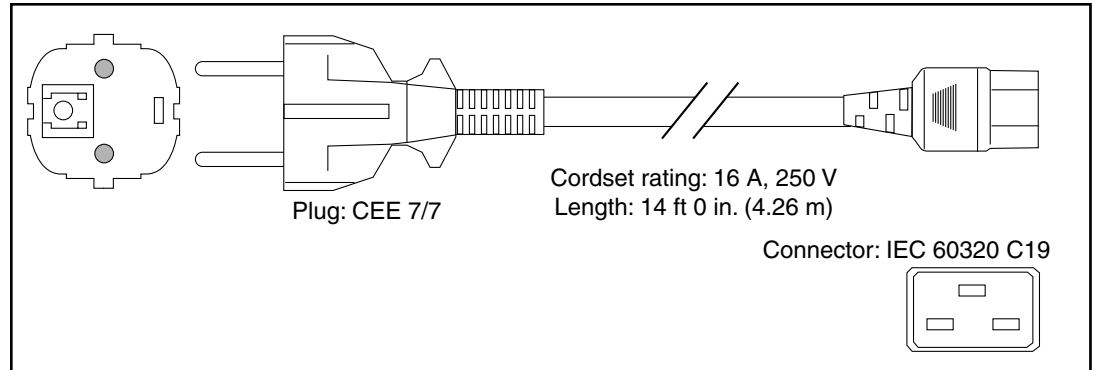
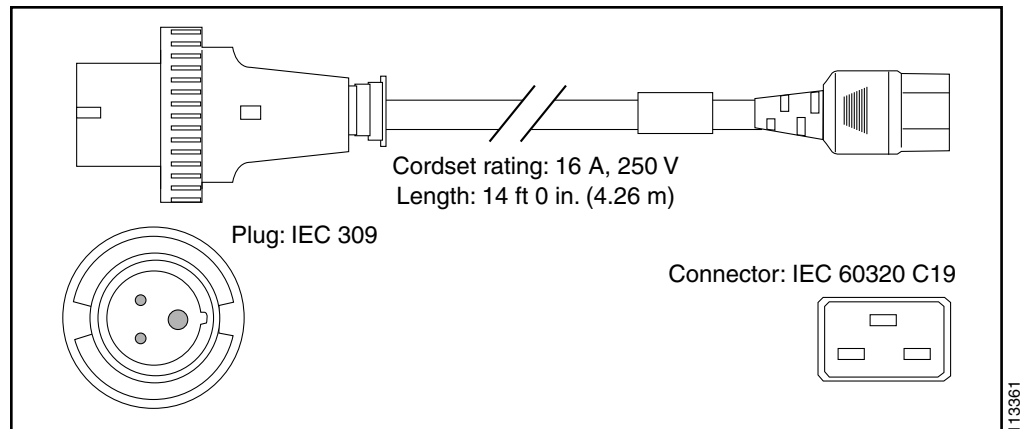
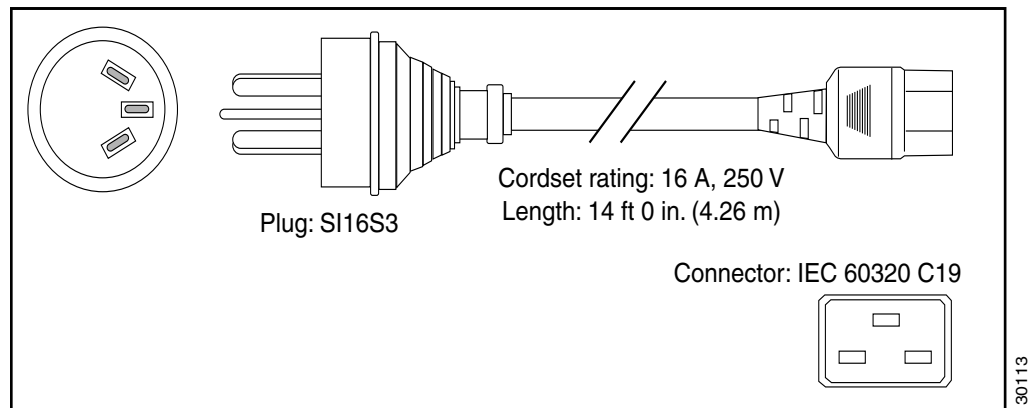
**Figure 4-3 CAB-AC-2500W-EU=****Figure 4-4 CAB-AC-2500W-INT=****Figure 4-5 CAB-AC-2500W-ISRL=**

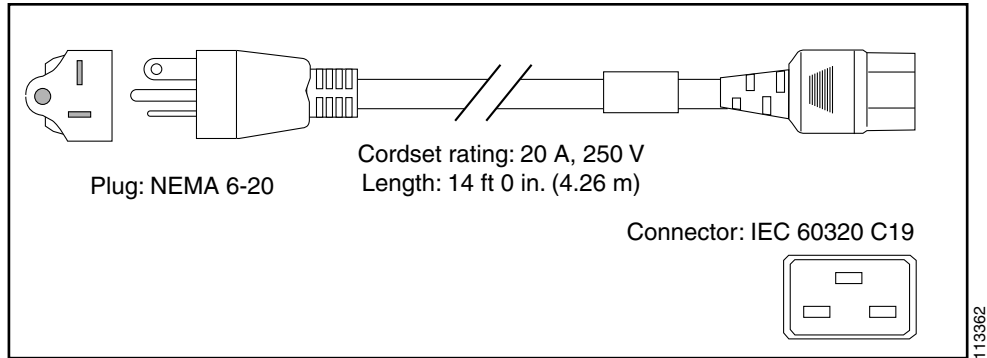
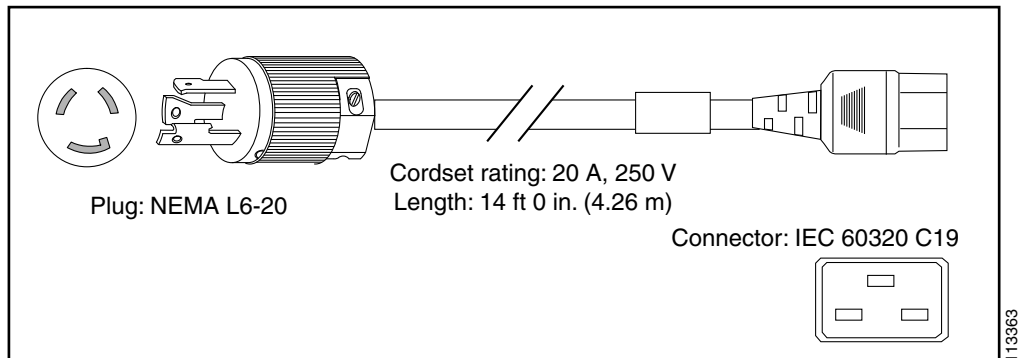
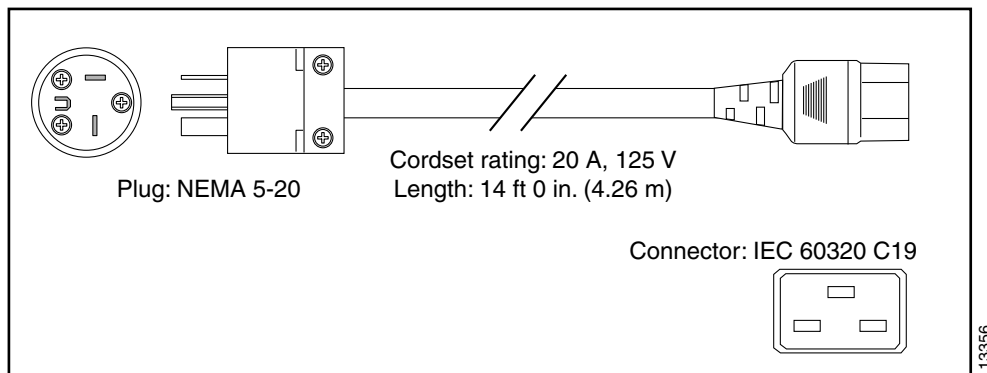
**Figure 4-6 CAB-AC-2500W-US1=****Figure 4-7 CAB-AC-C6K-TWLK=****Figure 4-8 CAB-7513AC=**

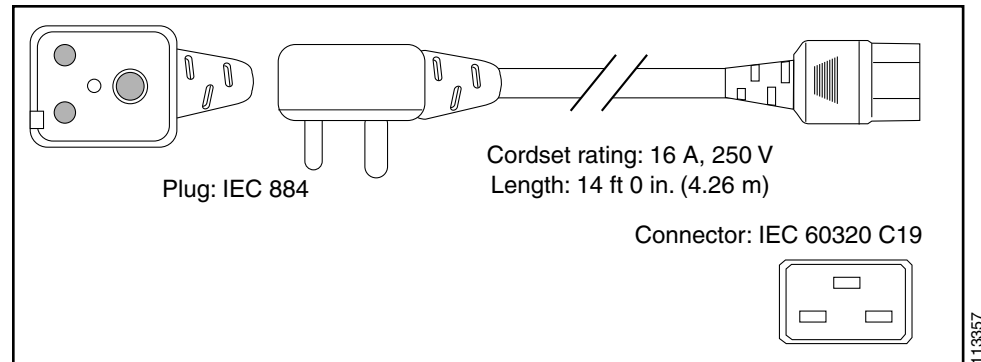
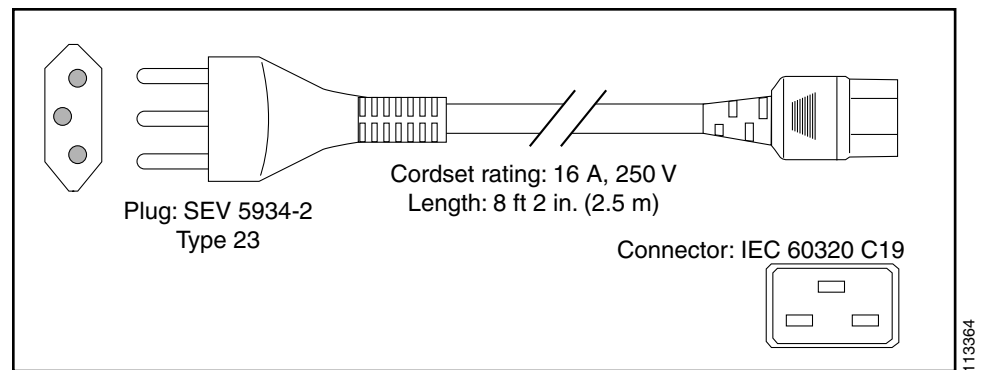
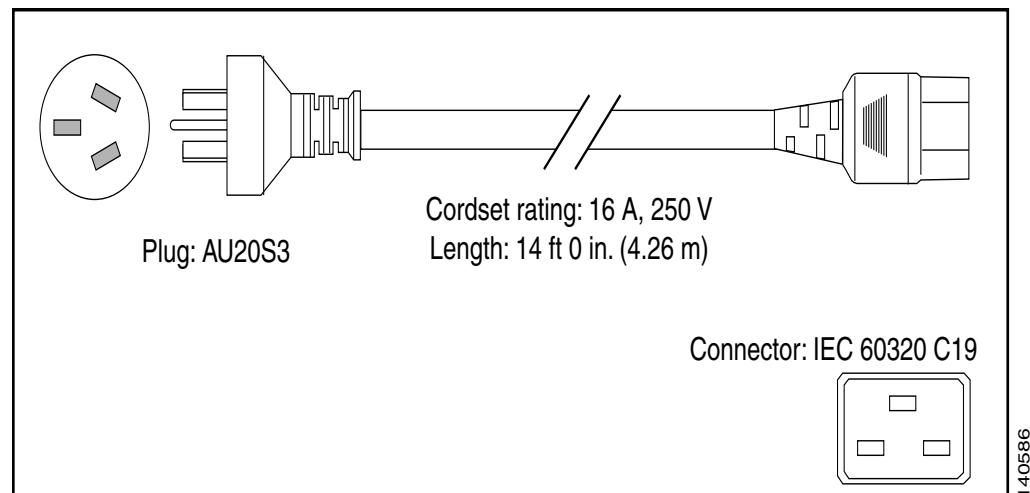
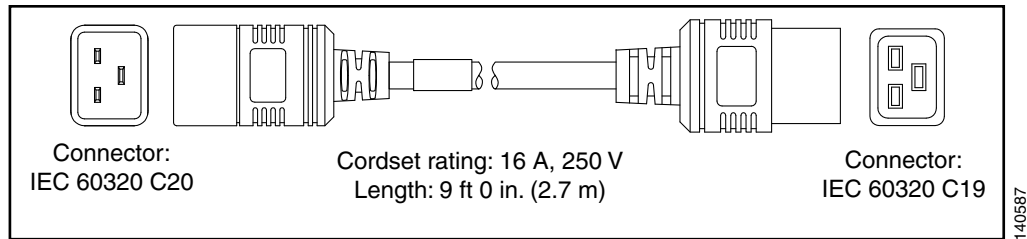
**Figure 4-9 CAB-7513ACSA=****Figure 4-10 CAB-ACS-16=****Figure 4-11 CAB-AC-16A-AUS**

**Figure 4-12 CAB-C19-CBN**

## DC-Powered Systems

Basic guidelines for DC-powered systems include the following:

- Each chassis power supply should have its own dedicated input power source. The source must comply with the safety extra-low voltage (SELV) requirements in the UL 60950, CSA 60950, EN 60950, and IEC 60950 standards.
- The DC supplies each have the provision for a dual connection to the power source in order to permit high-power operation without exceeding current ratings. For the Cisco SCE 8000, it is not necessary to connect both of these inputs to DC power sources; it is sufficient to connect only the 'I' connections.
- Each circuit must be protected by a dedicated two-pole circuit breaker. The circuit breaker should be sized according to the power supply input rating and local or national code requirements.
- The circuit breaker is considered the disconnect device and should be easily accessible.
- The system ground is the power supply and chassis ground.



### Caution

Do not connect the DC-return wire to the system frame or to the system grounding equipment.

Table 4-5 lists the Cisco SCE 8000 DC power specifications.

**Table 4-5 Cisco SCE 8000 DC Power Supply Specification**

| Specification                    | Acceptable Range                                                                                                                                                                                                          |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PWR-2700-DC/4 minimum capability | 1350 W output (1750 W input)                                                                                                                                                                                              |
| DC-input power consumption       | <ul style="list-style-type: none"> <li>• Single Cisco SCE 8000-SCM-E module:<br/>1000 W (21 A @ 48 VDC, 17 A @ 60 VDC)</li> <li>• Dual Cisco SCE 8000-SCM-E modules:<br/>1430 W (30 A @ 48 VDC, 24 A @ 60 VDC)</li> </ul> |
| DC-input voltage rating          | -48 VDC to -40 VDC<br>(operating range: -40.5 VDC to -72 VDC)                                                                                                                                                             |
| DC-input current rating          | 45 A maximum at 120 VAC                                                                                                                                                                                                   |

**Table 4-5** *Cisco SCE 8000 DC Power Supply Specification (continued)*

| Specification            | Acceptable Range                                                                                                                                                                                                                                                                   |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DC-input cable           | Accepts 2-14 AWG copper conductors. Actual size of the wire needed is determined by the installer or local electrician.<br>Terminal block material rated at 150°C (302°F).                                                                                                         |
| DC-input circuit breaker | For multiple DC input power supplies, each DC input must be protected by a dedicated two-pole circuit breaker or a fuse.<br>The circuit breaker or the fuse must be sized according to the power supply input power rating and any local or national electrical code requirements. |

**Note**

The DC supplies each have the provision for a dual connection to the power source in order to permit high-power operation without exceeding current ratings. For the Cisco SCE 8000, it is not necessary to connect both of these inputs to DC power sources; it is sufficient to connect only the 'I' connections.

# Site Planning Checklist

Table 4-6 lists the site planning activities that you should perform before installing the Cisco SCE 8000 chassis. Completing each activity helps ensure a successful installation.

**Table 4-6 Site Planning Checklist**

| Task No. | Planning Activity                                                                                                                                                                                                                                                                                                   | Verified By | Time | Date |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------|------|
| 1        | Space evaluation: <ul style="list-style-type: none"> <li>• Space and layout</li> <li>• Floor covering</li> <li>• Impact and vibration</li> <li>• Lighting</li> <li>• Maintenance access</li> </ul>                                                                                                                  |             |      |      |
| 2        | Environmental evaluation: <ul style="list-style-type: none"> <li>• Ambient temperature</li> <li>• Humidity</li> <li>• Altitude</li> <li>• Atmospheric contamination</li> <li>• Airflow</li> </ul>                                                                                                                   |             |      |      |
| 3        | Power evaluation: <ul style="list-style-type: none"> <li>• Input power type</li> <li>• Power receptacles</li> <li>• Receptacle proximity to the equipment</li> <li>• Dedicated (separate) circuits for redundant power supplies</li> <li>• UPS for power failures</li> </ul> DC systems: Proper gauge wire and lugs |             |      |      |
| 4        | Grounding evaluation: <ul style="list-style-type: none"> <li>• Circuit breaker size</li> <li>• CO ground (AC- and DC-powered systems)</li> </ul>                                                                                                                                                                    |             |      |      |
| 5        | Cable and interface equipment evaluation: <ul style="list-style-type: none"> <li>• Cable type</li> <li>• Connector type</li> <li>• Cable distance limitations</li> </ul>                                                                                                                                            |             |      |      |
| 6        | EMI evaluation: <ul style="list-style-type: none"> <li>• Distance limitations for signaling</li> <li>• Site wiring</li> <li>• RFI levels</li> </ul>                                                                                                                                                                 |             |      |      |

# Installing the Cisco SCE 8000 Chassis in the Rack

This section describes how to install a Cisco SCE 8000 platform in a rack. For first-time installations, perform the procedures in the following sections in the order listed:

1. [Unpacking the Cisco SCE 8000 Chassis, page 4-15](#)
2. [Installation Guidelines, page 4-16](#)
3. [Required Tools, page 4-16](#)
4. [Installing the Chassis Brackets, page 4-17](#)
5. [Installing the Chassis in the Rack, page 4-17](#)
6. [Installing an Optical Bypass Module, page 4-19](#)

**Note**

Before starting the installation procedures in this chapter, see the [“Site Planning Checklist” section on page 4-14](#) to verify that all site planning activities were completed.

## Unpacking the Cisco SCE 8000 Chassis

**Tip**

Do not discard the shipping container when you unpack the Cisco SCE 8000. Flatten the shipping cartons and store them with the pallet. You need these containers to move or ship the Cisco SCE 8000.

Perform the following to check the contents of the shipping container:

- Check the contents of the accessories kit against the list of accessories in the [“Cisco SCE 8000 Component and Accessory Lists” section on page 2-18](#) and the packing slip. Verify that you received all listed equipment, which should include the following:
  - Hardware and software documentation, if ordered
  - Optional equipment that you ordered, such as network interface cables, transceivers, or special connectors
- Check the modules in each slot. Ensure that the configuration matches the packing list and that all the specified interfaces are included.

## Installation Guidelines

Before installing the chassis, ensure that the equipment rack complies with the following guidelines:

- Width of the rack, measured between the two front mounting strips or rails, must be 17.75 in (45.09 cm).
- Depth of the rack, measured between the front and rear mounting strips, must be at least 19.25 in (48.9 cm) but not more than 32 in (81.3 cm).
- Rack must have sufficient vertical clearance to insert the chassis. The height of the Cisco SCE 8000 chassis is 8.7 in (22.09 cm) (5 RU).

If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

**Note**

We recommend that you maintain a minimum air space of 6 in (15 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 in (30.5 cm) between two chassis to prevent overheating.

The installation hardware is not suitable for use with racks with obstructions (such as a power strip) that could impair access to field-replaceable units (FRUs).

**Note**

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

## Required Tools

These tools and equipment are required to install the chassis in the rack:

- Number 1 and number 2 Phillips-head screwdrivers
- 3/16-inch flat-blade screwdriver
- Tape measure and level
- Masking tape or some other method of marking the desired installation height in the rack

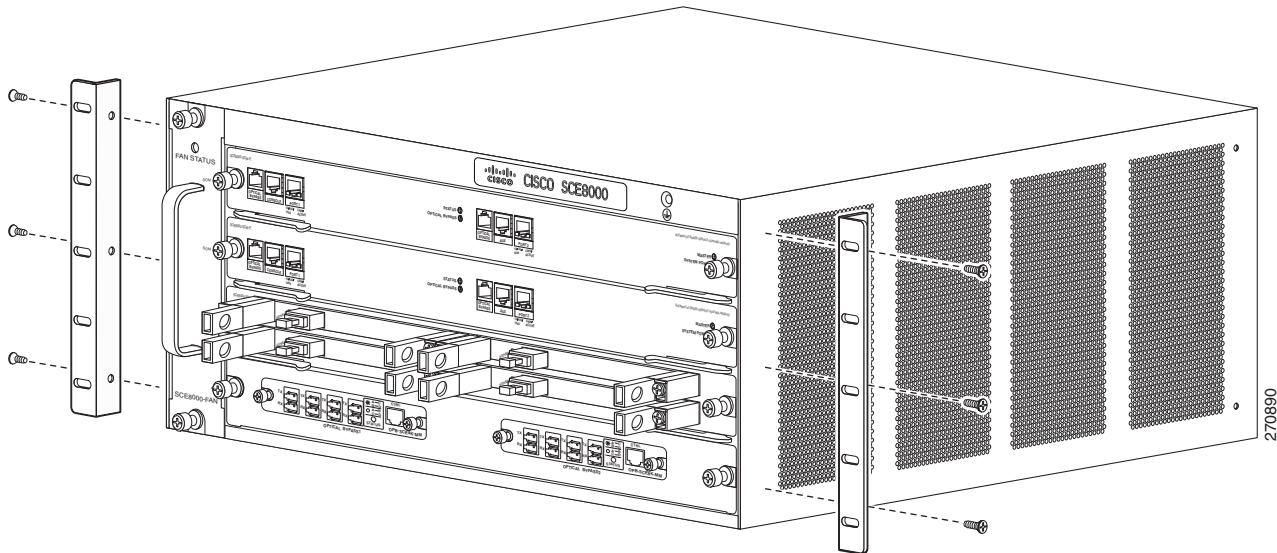
## Installing the Chassis Brackets

The chassis is shipped with the mounting brackets installed on the front of the chassis. These brackets can be installed on the rear of the chassis.

To install the brackets on the rear of the chassis, perform these steps:

- 
- Step 1** Remove the screws that secure the brackets to the chassis. (See [Figure 4-13](#).)

**Figure 4-13** Brackets on Cisco SCE 8000 Chassis



- Step 2** Position one of the brackets against the chassis side, and align the screw holes.
- Step 3** Secure the bracket to the chassis with the screws removed in Step 1.
- Step 4** Repeat [Step 2](#) and [Step 3](#) for the other bracket.
- 

## Installing the Chassis in the Rack



### Caution

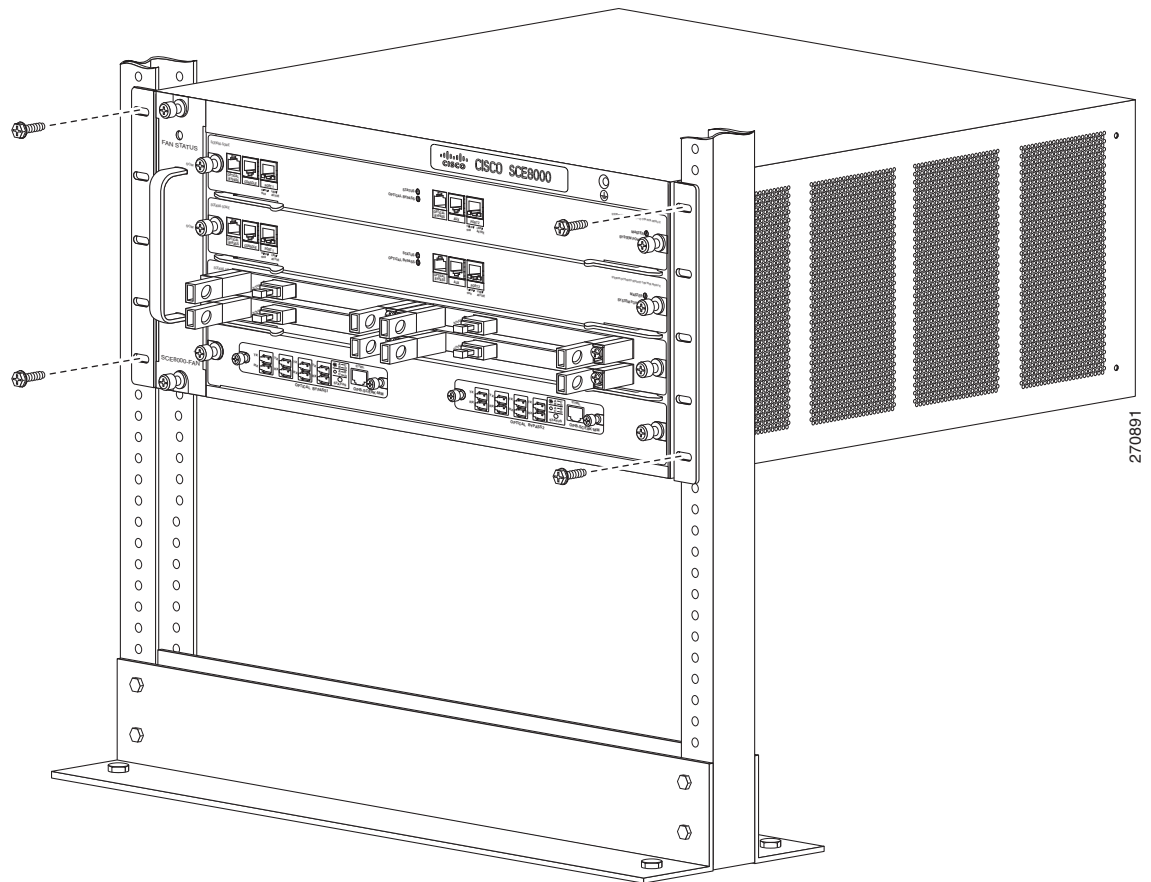
To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit. Lift the unit only by grasping the chassis underneath its lower edge.

To install the Cisco SCE 8000 chassis in the equipment rack, perform these steps:

- 
- Step 1** Position the chassis in the rack as follows:
- If the front of the chassis (front panel) is at the front of the rack, insert the rear of the chassis between the mounting posts.
  - If the rear of the chassis is at the front of the rack, insert the front of the chassis between the mounting posts.

- Step 2** Align the mounting holes in the bracket (and optional cable guide) with the mounting holes in the equipment rack. (See [Figure 4-14](#).)
- Step 3** Use a tape measure and level to choose and mark the position that the chassis is to be installed in the rack. Make a mark at equal height on both sides of the rack. This helps ensure that the chassis is installed straight and level.

**Figure 4-14** *Installing the Cisco SCE 8000 Chassis in the Rack*



- Step 4** Install the eight (four per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws through the holes in the bracket and into the threaded holes in the equipment rack posts.
- Step 5** Use a tape measure and level to verify that the chassis is installed straight and level.

## Installing an Optical Bypass Module

There are two installation options for the external bypass modules:

- Chassis mount panel—This panel is mounted on slot 4 of the Cisco SCE 8000 chassis. It hosts two optical bypass modules, which will serve the two traffic links supported by one Cisco SCE 8000 chassis.
- External mounting panel—This panel can be mounted in any 19" rack. It hosts up to four optical bypass modules, which will serve the four traffic links supported by two Cisco SCE 8000 platforms.

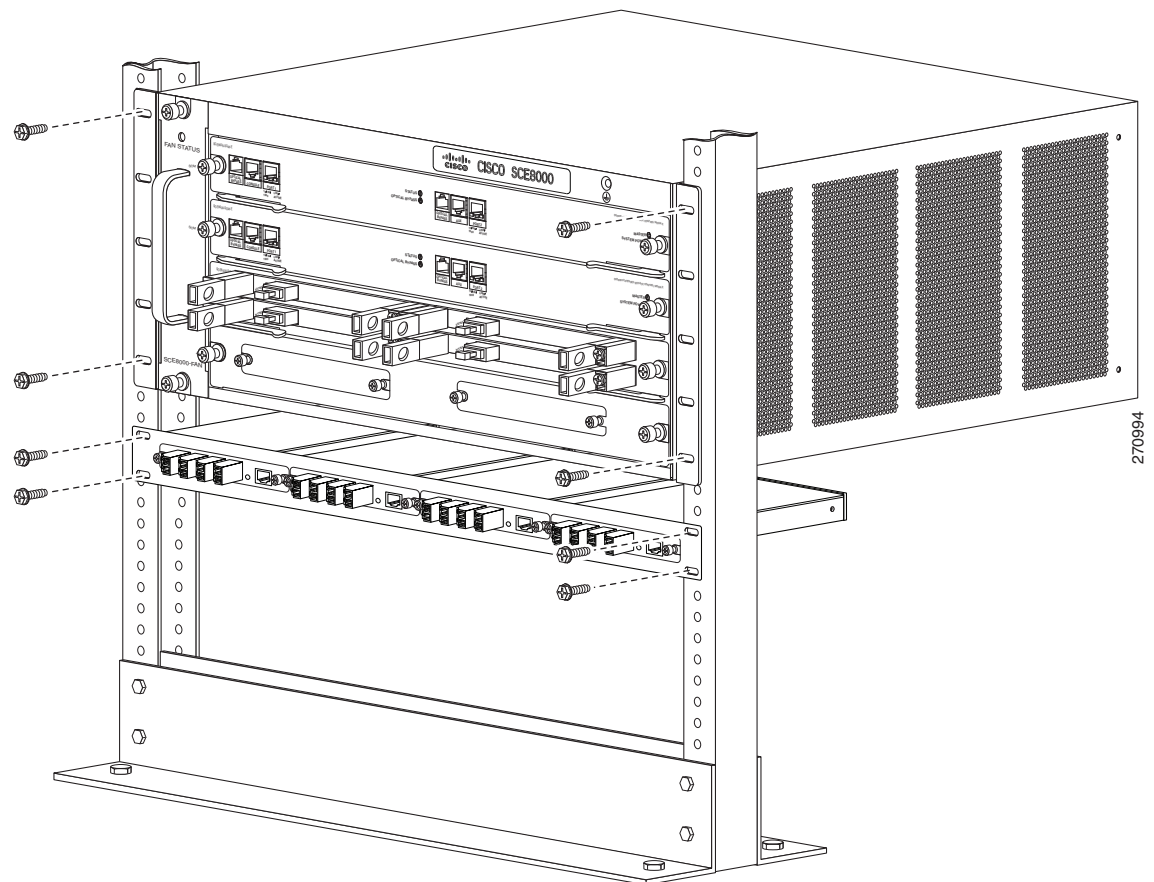
**Step 1** For external mounting, install the external mounting panel in the 19" rack. Screw the mounting panel to the rack using four 3/4-inch screws, two on each side, through the holes in the mounting panel and into the threaded holes in the rack posts.

For internal mounting, the Cisco SCE 8000 chassis is shipped with the chassis mounting panel already installed in slot 4.

**Step 2** Remove the module filler plate covering the subslot in the mounting panel by loosening the two screws.

**Step 3** Carefully insert the optical bypass module into the subslot (there are no guide rails) and tighten the captive screws on either side of the module. (See [Figure 4-15](#).)

**Figure 4-15** Optical Bypass Modules in the External Mounting Panel



# Connecting the System Ground

This section describes how to connect a system (earth) ground to the Cisco SCE 8000 chassis.

Two threaded M4 holes are provided on the chassis frame to attach the ground cable.

**Note**

Connect the system ground on both AC- and DC-powered systems to an earth ground if this equipment is installed in a US or European Central Office.

**Note**

For DC-powered systems, the system ground is also the power supply ground. The DC ground must be installed with a permanent connection to an earth ground according to NEC guidelines.

**Note**

Complete this procedure before connecting system power or turning on the Cisco SCE 8000 chassis.

## Required Tools and Equipment

To connect the system ground, you need the following tools and materials:

- One grounding lug.
- Two M4 (metric) hex-head screws with locking washers.

**Note**

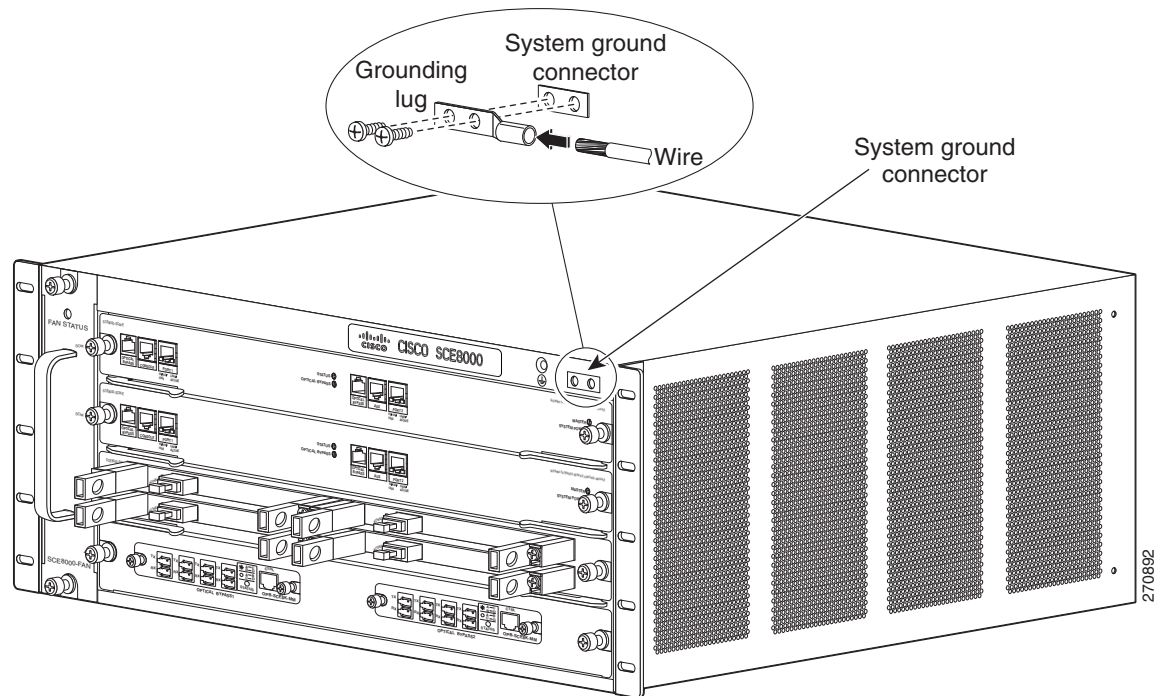
The grounding lug and M4 hex-head screws with locking washers are provided in kit 69-0815-01.

- One grounding wire.  
The grounding wire must be sized according to local and national installation requirements. Depending on the power supply and system, a 12 AWG conductor or larger size wire is required for U.S. installations.
- Number 2 Phillips-head screwdriver.
- Crimping tool (must be large enough to accommodate the girth of the grounding lug when crimping the grounding cable into the lug).
- Wire-stripping tool.

- 
- Step 1** Use a wire-stripping tool to remove approximately 0.75 inch (19 mm) of the covering from the end of the grounding wire.
- Step 2** Insert the stripped end of the grounding wire into the open end of the grounding lug.
- Step 3** Use the manufacturer recommended crimping tool to secure the grounding wire in place in the grounding lug.

- Step 4** Locate and remove the adhesive label from the system grounding pad on the chassis. (See [Figure 4-16](#).)

**Figure 4-16** *Installing the System Ground*



- Step 5** Place the grounding wire lug against the grounding pad, making sure there is solid metal-to-metal contact.
- Step 6** Secure the grounding lug to the chassis with two M4 screws. Ensure that the grounding lug will not interfere with other hardware or rack equipment.
- Step 7** Prepare the other end of the grounding wire, and connect it to an appropriate grounding point in your site to ensure adequate earth ground for the Cisco SCE 8000 chassis.

# Installing the Power Supplies in the Cisco SCE 8000 Chassis

The Cisco SCE 8000 chassis is shipped with the power supplies (AC or DC) already installed. Should it be necessary to install a power supply module, see the [““Removing and Replacing the Power Supply” section on page 9-4”](#).



# Connecting the Management Interfaces

---

Revised: February 18, 2015

## Introduction

This chapter explains how to connect the Cisco SCE 8000 Service Control Module (Cisco SCE 8000-SCM-E) to a local console and perform the initial system configuration.

Additionally, this chapter contains instructions for cabling the 10/100/1000 Ethernet management interfaces.

The Console interface (CON) as well as the management interfaces (Port1 and Port2) are located on the Cisco SCE 8000-SCM-E located in slot 1 of the Cisco SCE 8000 chassis (see the [““Service Control Module \(Cisco SCE 8000-SCM-E\)” section on page 2-4”](#)).

This chapter contains the following sections:

- [How to Set Up the Local Console, page 5-2](#)
- [Initial Setup Parameters, page 5-3](#)
- [Connecting the Management Interfaces, page 5-5](#)

# How to Set Up the Local Console

Connect the unit to a local console and configure the initial settings for the Cisco SCE 8000 to support remote management even if you are managing the Cisco SCE 8000 from a remote location. When the initial connection is established, the setup utility runs 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 Cisco SCE 8000 system using the setup utility.

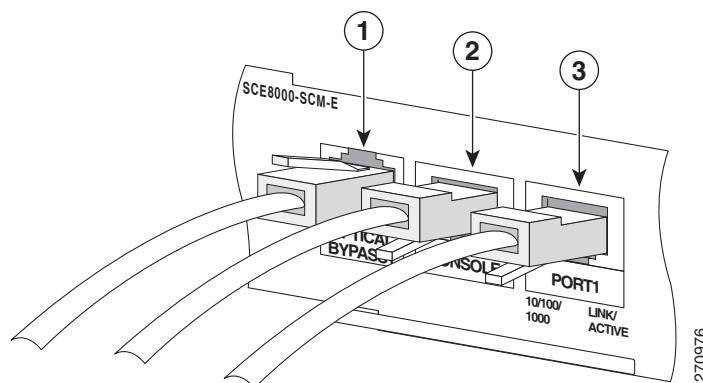
Make sure that the terminal configuration is as follows:

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

The preceding Cisco SCE 8000 port parameters are fixed and are not configurable.

- 
- Step 1** Plug the RS-232 serial cable provided with the Cisco SCE 8000 into the CON port on the front panel of the Cisco SCE 8000-SCM-E. (See item 2 in [Figure 5-1](#).)

**Figure 5-1** Connecting the Local Console to the Cisco SCE 8000-SCM-E CON Port



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 or DB-25 connector) to the VT100 compatible local (serial) terminal.
- Step 3** Ensure the local terminal is configured as a VT-100 terminal, according to the fixed Cisco SCE 8000 CON port parameters.
- Step 4** Ensure the Cisco SCE 8000 is powered-on, and has been allowed to complete booting (this process may take several minutes).
- Step 5** Press **Enter** several times until the Cisco logo appears on the local terminal.
-

# Initial Setup Parameters

At this point, there are several basic global parameters that must be correctly configured for the SCE platform to communicate properly with the outside world. The following is a very brief summary of the initial setup parameters and commands. For more information, see the [Cisco SCE8000 10GBE Software Configuration Guide](#).

- IP address and subnet mask of the Cisco SCE 8000 platform itself. This is the IP address used by the management interface.
- IP address of the default gateway.
- Hostname—The hostname is used to identify the SCE platform. 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 *SCE8000*.
- Passwords for user, admin, and root level access. These are authorization-level passwords, not individual passwords. These passwords may be encrypted.

Passwords must meet the following criteria:

- Minimum length — 4 characters
- Maximum length — 100 characters
- Begin with an alpha character
- May contain only printable characters
- The default password for all levels is *cisco*.
- System clock— Current date and time. The clock and the calendar must always be synchronized.
- Time zone—Name or ID of the time zone along with the number of hours offset from UTC.
- Domain name server—Default domain name, which is used to complete unqualified host names, as well as up to three domain name servers, which are used for DNS lookup.

You must also enable DNS lookup.

- RDR formatter destination—SCE platform generates Raw Data Records and sends them to the specified destinations (external collection systems) via the RDR formatter. You can configure up to eight RDR formatter destinations. Specify the IP address and port number for each destination.

[Table 5-1](#) lists commands both for displaying the currently configured values and for configuring these parameters. It also lists the command mode for each configuration command. All **show** commands are executed from the User Exec command mode.

**Table 5-1 Initial Setup Configuration**

| Parameter                             | show command                                                                                                           | configuration command                        | Configuration Command Mode                                                   |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------|
| Management IP address and subnet mask | <b>show interface GigabitEthernet (1/1   1/2) ip address</b><br>OR<br><b>show interface MNG (0/1   0/2) ip address</b> | <b>ip address</b> <i>x.x.x.x subnet-mask</i> | GigabitEthernet Interface Configuration<br>or<br>MNG Interface Configuration |
| Default gateway                       | <b>show ip default-gateway</b>                                                                                         | <b>ip default-gateway</b> <i>x.x.x.x</i>     | Global Configuration                                                         |

Table 5-1 Initial Setup Configuration (continued)

| Parameter                     | show command                              | configuration command                                                                                                                                                     | Configuration Command Mode |
|-------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Hostname                      | <b>show hostname</b>                      | <b>hostname</b> <i>host-name</i>                                                                                                                                          | Global Configuration       |
| Authorization level passwords | —                                         | <b>enable password level</b> <i>level</i><br><i>[encryption-type] password</i>                                                                                            | Global Configuration       |
| Clock                         | <b>show clock</b><br><b>show calendar</b> | <b>calendar set</b> <i>hh:mm:ss day month year</i><br><b>clock read-calendar</b><br>or<br><b>clock set</b> <i>hh:mm:ss day month year</i><br><b>clock update-calendar</b> | Privileged EXEC            |
| Time zone                     | <b>show timezone</b>                      | <b>clock timezone</b> <i>zone-name</i><br><i>offset-hours</i>                                                                                                             | Global Configuration       |
| Domain name server            | <b>show hosts</b>                         | <b>ip domain-lookup</b><br><b>ip domain-name</b> <i>domain-name</i><br><b>ip name-server</b> <i>server-address1</i><br><i>[server-address2] [server-address3]</i>         | Global Configuration       |
| RDR formatter destination     | <b>show rdr-formatter destination</b>     | <b>rdr-formatter destination</b><br><i>ip-address</i> <b>port</b> <i>port-number</i>                                                                                      | Global Configuration       |

# Connecting the Management Interfaces

The Cisco SCE 8000-SCM-E is equipped with two active RJ-45 management ports. These 10/100/1000 Ethernet interfaces provide access from a remote management console to the Cisco SCE 8000 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 Cisco SCE 8000 and the remote management host are explained in the following sections:

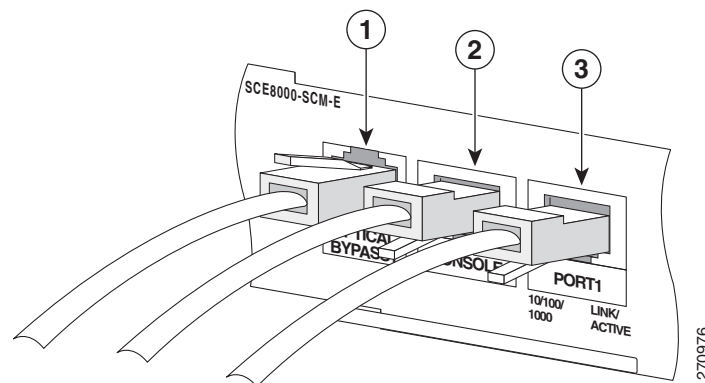
- [Cabling the Management Port, page 5-5](#)
- [Verifying Management Interface Connectivity, page 5-6](#)

## Cabling the Management Port

The Cisco SCE 8000-SCM-E has two 10/100/1000 Ethernet ports that are used as the management ports, located in slot 1 of the Cisco SCE 8000 chassis, and labeled Port1 and Port2.

- Step 1** Plug the Ethernet cable provided (with attached RJ-45 connector) into the desired 10/100/1000 Ethernet port on the front panel of the Cisco SCE 8000-SCM-E in slot 1. (See item 3 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 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 Link LED 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 Cisco SCE 8000 platform has been powered up, test to verify that connectivity has been established between the Cisco SCE 8000 and the remote management host. If the Cisco SCE 8000 platform is not powered up, perform this procedure after starting the Cisco SCE 8000 platform.

**Step 1** After you connect the cable to the appropriate management port and to your network, check the relevant port LEDs.

There are two LEDs — Link/Active, and 10/100/1000 (see the [“Service Control Module \(Cisco SCE 8000-SCM-E\)”](#) section on page 2-4).

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, as follows:

- Off—10 Mbps
- Green—100 Mbps
- Orange—1000 Mbps

**Step 2** Test connectivity. From the host that you intend to use for remote management, ping to the Cisco SCE 8000 by typing **ping** and the Cisco SCE 8000 IP address, and pressing **Enter** (see the following example).



### Note

Only this step (Step 2), is performed from the remote management host (connected by LAN to Port1 or Port2).

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

The **ping** command 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 10.10.10.20:

```
C:\>ping 10.10.10.20
pinging 10.10.10.20 ...
PING 10.10.10.20: 56 data bytes
64 bytes from host (10.10.10.20): icmp_seq=0. time=0. ms
64 bytes from host (10.10.10.20): icmp_seq=1. time=0. ms
64 bytes from host (10.10.10.20): icmp_seq=2. time=0. ms
64 bytes from host (10.10.10.20): icmp_seq=3. time=0. ms
----10.10.10.20 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```





# Cabling the Line Ports and Completing the Installation

---

Revised: February 18, 2015

## Introduction

This chapter provides instructions for cabling the Cisco SCE 8000 10 Gigabit Ethernet ports for single, cascaded, and MGSCP topologies. In a cascade topology, this includes the cascade ports as well as the line ports.

The 10 Gigabit Ethernet ports are located on the 10G SPA modules, which are installed in the Cisco SCE 8000-SIP module in slot 3 of the Cisco SCE 8000 chassis.



### Note

When installing a cascaded system, it is extremely important to follow the sequence of procedures outlined in the [“Cascaded Systems” section on page 6-19](#).



### Note

When installing an External Optical Bypass module, the Cisco SCE 8000 line ports are connected to the module. See the [“Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module” section on page 6-14](#) for complete instructions.

This chapter contains the following sections:

- [Connecting the Line Ports to the Network, page 6-2](#)
- [The Optical Bypass Module, page 6-9](#)
- [Cabling the 10 GBE Line Interface Ports, page 6-11](#)
- [How to Install a Service Control Application, page 6-18](#)
- [Cascaded Systems, page 6-19](#)

# Connecting the Line Ports to the Network

This section describes the following topics:

- [Single Link: Inline Topology, page 6-2](#)
- [Single Link: Receive-only Topology, page 6-2](#)
- [Dual Link: Single Cisco SCE 8000 Topologies, page 6-3](#)
- [Dual Link: Two Cisco SCE 8000s Topology, page 6-3](#)
- [Multi-Gigabit Service Control Platforms \(MGSCP\) Topologies, page 6-4](#)

## Single Link: Inline Topology

In the inline topology, the Cisco SCE 8000 resides physically on the 10 GBE (Ten Gigabit Ethernet) link between the subscribers and the network. The subscribers are usually connected through either a BRAS (in DSL access), a PDSN (in wireless access), a CMTS (in the Cable access), or a switch or router aggregator (in other topologies). The network is a router or Layer 3 switch network element connecting the Cisco SCE 8000 toward the core of the network.

Guidelines for single link inline topologies:

- If only two SPA modules are installed (only two SPA modules are required for a single link), they must be installed in bays 0 and 1 of the SPA jacket card.
- Inline topologies require both Receive and Transmit fibers.
- To maintain link continuity at all times, an optical bypass module should be installed.

### Single link inline connectivity

- Port 3/0/0: Link 0, Subscribers side
- Port 3/1/0: Link 0, Network side

## Single Link: Receive-only Topology

In this topology, an optical splitter unit resides physically on the 10 GBE link that the Cisco SCE 8000 should monitor. The optical splitter unit is connected to the Cisco SCE 8000 Rx links only. For each link monitored, there are two Rx connections to the Cisco SCE 8000, one for each direction of traffic flow in the link. The traffic passes through the optical splitter, which allows the Cisco SCE 8000 to monitor traffic without affecting the normal optic and data path between subscriber and network.



### Note

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

Guidelines for single link receive-only topologies:

- If only two SPA modules are installed (only two SPA modules are required for a single link), they must be installed in bays 0 and 1 of the SPA jacket card.
- Receive-only topologies use only Receive fibers.

### Single Link Receive-only Connectivity:

- Port 3/0/0: Link 0, Split of optic signal transmitted by subscribers side

- Port 3/1/0: Link 0, Split of optic signal transmitted by network side

## Dual Link: Single Cisco SCE 8000 Topologies

In this topology, one Cisco SCE 8000 is connected to two full duplex, 10 GBE links. The Cisco SCE 8000 may be either inline, to support both monitoring and traffic control functionality, or receive-only for traffic monitoring functionality only.

Guidelines for dual link topologies:

- SPA modules 0 and 1 are connected to the first link (Link 0).
- SPA modules 2 and 3 are connected to the second link (Link 1).
- Dual link inline topologies require both Receive and Transmit fibers.
- Dual link receive-only topologies use only Receive fibers.
- To maintain link continuity at all times on both links when using the inline topology, two optical bypass modules should be installed.

### Dual Link Connectivity:

- Port 3/0/0: Link 0, Subscribers side
- Port 3/1/0: Link 0, Network side
- Port 3/2/0: Link 1, Subscribers side
- Port 3/3/0: Link 1, Network side

**Note**

Receive-only topologies can be implemented using either an optical splitter or a switch. If a switch is used, it must support SPAN functionality that includes separation between ingress and egress traffic and multiple SPAN-ports destinations.

## Dual Link: Two Cisco SCE 8000s Topology

In this topology, two Cisco SCE 8000s are connected to two full duplex, 10 GBE links, providing full redundancy through cascading the two Cisco SCE 8000s. The Cisco SCE 8000s must be inline.

**Note**

When installing a cascaded system, it is extremely important to follow the sequence of procedures outlined in the [“Cascaded Systems” section on page 6-19](#).

When two Cisco SCE 8000s are used, the ports 3/0/0 and 3/1/0 in each Cisco SCE 8000 are connected to the links, whereas ports 3/2/0 and 3/3/0 are the cascade ports that are used for communicating between the two Cisco SCE 8000s as follows:

### Cisco SCE 8000 #1

- Port 3/0/0: Link 0, Subscribers side
- Port 3/1/0: Link 0, Network side
- Port 3/2/0: Cascade, connect to Port 3/3/0 in Cisco SCE 8000 #2
- Port 3/3/0: Cascade, connect to Port 3/2/0 in Cisco SCE 8000 #2

**Cisco SCE 8000 #2**

- Port 3/0/0: Link 1, Subscribers side
- Port 3/1/0: Link 1, Network side
- Port 3/2/0: Cascade, connect to Port 3/3/0 in Cisco SCE 8000 #1
- Port 3/3/0: Cascade, connect to Port 3/2/0 in Cisco SCE 8000 #1

Inline topologies require connecting both Receive and Transmit fibers to the Cisco SCE 8000. Cascade ports always require both Receive and Transmit fibers to be connected.

To maintain link continuity at all times, it is recommended to install two optical bypass modules, and the traffic ports should be connected to these bypass modules.

## Multi-Gigabit Service Control Platforms (MGSCP) Topologies

In this topology, multiple Cisco SCE 8000 platforms are connected to a Cisco 7600 Series router used as a load-balancer (“dispatcher”) between the platforms. Traffic enters the router, is distributed between the Cisco SCE 8000 platforms by the router EtherChannel, and returns to the router to be forwarded to its original destination.

General guidelines for MGSCP topologies:

- Because there are two links per Cisco SCE 8000 platform, the minimum number of platforms required is half the number of links used.
- Each link corresponds to one port on the EtherChannel (EC) on the Cisco 7600 Series router. Each EC supports a maximum of eight active ports. Therefore, if all eight EC ports are configured, four Cisco SCE 8000 platforms are required.
- For N+1 redundancy, two additional ports (connected to the standby platform) must be configured as standby ports on both ECs.

Therefore, for N+1 redundancy, one router and five Cisco SCE 8000 platforms are used to support eight links.

- If two Cisco 7600 Series routers are used (for network redundancy), one link on each Cisco SCE 8000 platform is connected to each router. This requires twice the number of Cisco SCE 8000 platforms, one platform for each link.
  - A minimum of eight Cisco SCE 8000 platforms are required to support eight ports.
  - For N+1 redundancy, nine Cisco SCE 8000 platforms are used to support eight active links.

When cabling to the EC, follow these guidelines:

- Cisco SCE platform ports **MUST** be connected to the EC ports in the same order on both sides.
- EC ports should be sorted in an ascending order by their physical interface numbers.
- In a topology with two Cisco 7600 Series routers, the order of connection to the EC ports must be the same on both routers. For both routers to send the traffic of a given subscriber to the same SCE platform, the SCE platforms must be connected to both routers in exactly the same order (one SCE platform connected to the first link on both routers, another SCE platform connected to the second link on both routers, and so on).
- See the [“MGSCP Connectivity Examples” section on page 6-5](#) for specific examples explaining how to connect the Cisco SCE 8000 ports to the EC ports in various topologies.
- See the [“Dual Link: Single Cisco SCE 8000 Topologies” section on page 6-3](#) and the [“Single Link: Inline Topology” section on page 6-2](#) for further information on specific cabling schemes.

**MGSCP Connectivity Examples**

- [The First Step-Ordering the EC Ports, page 6-5](#)
- [Single Router MGSCP Connectivity, page 6-5](#)
- [Single Router with N+1 Redundancy MGSCP Connectivity, page 6-5](#)
- [Dual Routers MGSCP Connectivity, page 6-6](#)
- [Dual Routers with N+1 Redundancy MGSCP Connectivity, page 6-7](#)

**The First Step-Ordering the EC Ports**

This section explains how to order the EC ports and assign them to links. This example is the basis for all following examples:

1. Sort the EC ports in an ascending order by their physical interface numbers. Take the following EC interfaces as an example:
  - EC1 (subscriber side): 0/1, 0/2, 1/3, 1/5
  - EC2 (network side): 2/2, 3/1, 3/2, 3/4
2. Order the ports in subscriber/network pairs according to their order in the ECs (the first port in EC1 (subscriber side) is paired with the first port in EC2 (network side) and so on):
  - Link 1. S=0/1, N=2/2
  - Link 2. S=0/2, N=3/1
  - Link 3. S=1/3, N=3/2
  - Link 4. S=1/5, N=3/4

**Single Router MGSCP Connectivity**

Four links require two Cisco SCE 8000 platforms. Connect the ordered pairs, each pair of EC ports to a pair of Subscriber/Network ports in a Cisco SCE 8000 platform:

- Cisco SCE 8000 #1: Links 1 and 2
- Cisco SCE 8000 #2: Links 3 and 4

The actual connections might look like this:

- S=0/1, Cisco SCE 8000 #1 3/0/0
- N=2/2, Cisco SCE 8000 #1 3/1/0
- S=0/2, Cisco SCE 8000 #1 3/2/0
- N=3/1, Cisco SCE 8000 #1 3/3/0
- S=1/3, Cisco SCE 8000 #2 3/0/0
- N=3/2, Cisco SCE 8000 #2 3/1/0
- S=1/5, Cisco SCE 8000 #2 3/2/0
- N=3/4, Cisco SCE 8000 #2 3/3/0

**Single Router with N+1 Redundancy MGSCP Connectivity**

To achieve N+1 redundancy, add one extra SCE platform as the standby platform. Also, add two more ports on each EC to be used as standby ports. In this case, use three SCE platforms, two on the traffic links and one for redundancy, which would be connected to the standby ports.

If you add ports 0/3 and 2/3 on EC1 and 2/4 and 4/4 on EC2, the ECs would look like this:

- EC1: 0/1, 0/2, 0/3, 1/3, 1/5, 2/3
- EC2: 2/2, 2/4, 3/1, 3/2, 3/4, 4/4

The standby ports must be the two highest-numbered ports:

- EC1 standby ports: 1/5, 2/3
- EC2 standby ports: 3/4, 4/4

The traffic ports would be assigned to the links as follows:

- Link 1. S=0/1, N=2/2
- Link 2. S=0/2, N=2/4
- Link 3. S=0/3, N=3/1
- Link 4. S=1/3, N=3/2

The standby ports would be assigned to the links as follows:

- Link 5 (standby). S=1/5, N=3/4
- Link 6 (standby). S= 2/3, N=4/4

If Cisco SCE 8000 #3 is the redundant platform, Links 5 and 6 would be connected to it and the actual connections might look like this:

- S=0/1, Cisco SCE 8000 #1 3/0/0
- N=2/2, Cisco SCE 8000 #1 3/1/0
- S=0/2, Cisco SCE 8000 #1 3/2/0
- N=2/4, Cisco SCE 8000 #1 3/3/0
- S=0/3, Cisco SCE 8000 #2 3/0/0
- N=3/1, Cisco SCE 8000 #2 3/1/0
- S=1/3, Cisco SCE 8000 #2 3/2/0
- N=3/2, Cisco SCE 8000 #2 3/3/0
- S=1/5, Cisco SCE 8000 #3 3/0/0
- N=3/4, Cisco SCE 8000 #3 3/1/0
- S=2/3, Cisco SCE 8000 #3 3/2/0
- N=4/4, Cisco SCE 8000 #3 3/3/0

### Dual Routers MGSCP Connectivity

Four links on each router would require four Cisco SCE 8000 platforms. For the sake of simplicity, we assume that the EC ports are the same on both routers.

Connect the ordered pairs, each pair of EC ports to a pair of Subscriber/Network ports in a Cisco SCE 8000 platform:

- Cisco SCE 8000 #1: Link 1 on both routers
- Cisco SCE 8000 #2: Link 2 on both routers
- Cisco SCE 8000 #3: Link 3 on both routers
- Cisco SCE 8000 #4: Link 4 on both routers

The actual connections might look like this:

- Router 1: S=0/1, Cisco SCE 8000 #1 3/0/0
- Router 2: S=0/1, Cisco SCE 8000 #1 3/2/0
- Router 1: N=2/2, Cisco SCE 8000 #1 3/1/0
- Router 2: N=2/2, Cisco SCE 8000 #1 3/3/0
- Router 1: S=0/2, Cisco SCE 8000 #2 3/0/0
- Router 2: S=0/2, Cisco SCE 8000 #2 3/2/0
- Router 1: N=3/1, Cisco SCE 8000 #2 3/1/0
- Router 2: N=3/1, Cisco SCE 8000 #2 3/3/0
- Router 1: S=1/3, Cisco SCE 8000 #3 3/0/0
- Router 2: S=1/3, Cisco SCE 8000 #3 3/2/0
- Router 1: N=3/2, Cisco SCE 8000 #3 3/1/0
- Router 2: N=3/2, Cisco SCE 8000 #3 3/3/0
- Router 1: S=1/5, Cisco SCE 8000 #4 3/0/0
- Router 1: S=1/5, Cisco SCE 8000 #4 3/2/0
- Router 1: N=3/4, Cisco SCE 8000 #4 3/1/0
- Router 1: N=3/4, Cisco SCE 8000 #4 3/3/0

#### **Dual Routers with N+1 Redundancy MGSCP Connectivity**

To achieve N+1 redundancy, add one extra SCE platform as the standby platform. Also, add another port on each EC to be used as standby ports. In this case, use five SCE platforms, four on the traffic links and one for redundancy, which would be connected to the standby ports.

Again, for the sake of simplicity, assume that the EC ports are the same on both routers.

If you add ports 0/3 on EC1 and 2/4 on EC2, the ECs would look like this:

- EC1: 0/1, 0/2, 0/3, 1/3, 1/5
- EC2: 2/2, 2/4, 3/1, 3/2, 3/4

The standby ports must be the highest-numbered ports:

- EC1 standby port: 1/5
- EC2 standby port: 3/4

The traffic ports would be assigned to the links as follows:

- Link 1. S=0/1, N=2/2
- Link 2. S=0/2, N=2/4
- Link 3. S=0/3, N=3/1
- Link 4. S=1/3, N=3/2

The standby ports would be assigned to the links as follows:

- Link 5 (standby). S=1/5, N=3/4

If Cisco SCE 8000 #5 is the redundant platform, Link 5 from both routers is connected to it and the actual connections might look like this:

- Router 1: S=0/1, Cisco SCE 8000 #1 3/0/0
- Router 2: S=0/1, Cisco SCE 8000 #1 3/2/0
- Router 1: N=2/2, Cisco SCE 8000 #1 3/1/0
- Router 2: N=2/2, Cisco SCE 8000 #1 3/3/0
- Router 1: S=0/2, Cisco SCE 8000 #2 3/0/0
- Router 2: S=0/2, Cisco SCE 8000 #2 3/2/0
- Router 1: N=2/4, Cisco SCE 8000 #2 3/1/0
- Router 2: N=2/4, Cisco SCE 8000 #2 3/3/0
- Router 1: S=0/3, Cisco SCE 8000 #3 3/0/0
- Router 2: S=0/3, Cisco SCE 8000 #3 3/2/0
- Router 1: N=3/1, Cisco SCE 8000 #3 3/1/0
- Router 2: N=3/1, Cisco SCE 8000 #3 3/3/0
- Router 1: S=1/3, Cisco SCE 8000 #4 3/0/0
- Router 2: S=1/3, Cisco SCE 8000 #4 3/2/0
- Router 1: N=3/2, Cisco SCE 8000 #4 3/1/0
- Router 2: N=3/2, Cisco SCE 8000 #4 3/3/0
- Router 1: S=1/5, Cisco SCE 8000 #5 3/0/0
- Router 2: S=1/5, Cisco SCE 8000 #5 3/2/0
- Router 1: N=3/4, Cisco SCE 8000 #5 3/1/0
- Router 2: N=3/4, Cisco SCE 8000 #5 3/3/0

# The Optical Bypass Module

The external optical bypass module is an optional component that provides additional protection by enabling automatic preservation of the network 10 GBE link. For more information about the external bypass module, see [“The Cisco SCE 8000 Optical Bypass” section on page 2-12](#).

There are two installation options for the optical bypass module:

- Chassis mount—The optical bypass module may be installed in the panel in slot 4 of the Cisco SCE 8000 chassis. This panel hosts up to two optical bypass modules.
- External mounting panel—The optical bypass module may be installed in a panel that is mounted in a 19" rack. This panel can host up to four optical bypass modules.

**Note**

Make sure to use the correct type of optical bypass module (single-mode or multi-mode) according to the transceivers and cabling that are used for the subscriber and network links.

**Note**

Because the optic bypass module will directly connect the subscriber and network side optic paths when bypassing the Cisco SCE 8000, the subscriber and network optic links must be of the same type (single-mode or multi-mode) and wavelength.

**Warning**

**Invisible laser radiation may be emitted from disconnected fibers or connectors. Avoid exposure to radiation and do not stare into open aperture.**

Statement 1056

## Optical Bypass Module Connectivity

This section describes the following topics:

- [Single-Link Topology, page 6-9](#)
- [Dual-Link Topology, page 6-10](#)

### Single-Link Topology

A single link requires only one bypass module.

- Subscriber side network element <->Port A on the bypass module
- Cisco SCE 8000 port 3/0/0 <->Port C on the bypass module
- Network side network element <->Port B on the bypass module
- Cisco SCE 8000 port 3/1/0 <->Port D on the bypass module
- CTRL <->left-hand 'Optical Bypass' port on Cisco SCE 8000-SCM-E module

**Dual-Link Topology**

A dual link requires two bypass modules:

- Subscriber side network element <->Port A on bypass module 1
- Cisco SCE 8000 port 3/0/0 <->Port C on bypass module 1
- Network side network element <->Port B on bypass module 1
- Cisco SCE 8000 port 3/1/0 <->Port D on bypass module 1
- CTRL on bypass module #1 <->left-hand 'Optical Bypass' port on Cisco SCE 8000-SCM-E module
- Subscriber side network element <->Port A on bypass module 2
- Cisco SCE 8000 port 3/2/0 <->Port C on bypass module 2
- Network side network element <->Port B on bypass module 2
- Cisco SCE 8000 port 3/3/0 <->Port D on bypass module 2
- CTRL on bypass module 2 <->right-hand 'Optical Bypass' port on Cisco SCE 8000-SCM-E module

# Cabling the 10 GBE Line Interface Ports



## Note

When installing an External Optical Bypass module, the Cisco SCE 8000 line ports are connected to the module. See the [Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module, page 6-14](#) for complete instructions.



## Warning

**Class 1 laser. Avoid exposure to radiation and do not stare into open aperture.**  
Statement 1008

This section describes the following topics:

- [XFP Module Cabling and Connection Equipment, page 6-11](#)
- [Optical Device Maintenance, page 6-12](#)
- [How to Cable the 10 GBE Line Interface Ports, page 6-13](#)
- [Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module, page 6-14](#)

## XFP Module Cabling and Connection Equipment

[Table 6-1](#) and [Table 6-2](#) provide cabling specifications for the XFP modules that can be installed on the 10 Gigabit Ethernet SPA. All XFP ports have LC-type connectors.

**Table 6-1 XFP Transceiver Port Cabling Specifications**

| XFP Product Number | Nominal Wavelength (nm) | Cable Type | Core Size (microns) | Maximum Cabling Distance                                                                                                                         |
|--------------------|-------------------------|------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| XFP-10GLR-OC192SR  | 1310                    | SMF        | G.652               | <ul style="list-style-type: none"> <li>• 10 km (6.2 miles)<br/>10-Gigabit Ethernet</li> <li>• 2 km (1.24 miles)<br/>OC-192/STM-64 SR1</li> </ul> |
| XFP-10GER-OC192IR  | 1550                    | SMF        | G.652               | 40 km (24.86 miles)                                                                                                                              |
| XFP-10GZR-OC192IR  | 1550                    | SMF        | G.652               | 80 km (10 miles)                                                                                                                                 |
| XFP-10G-MM-SR      | 850                     | MMF        | G.652               | 26 m to 300 m<br>(85.3 to 984.3 feet)                                                                                                            |

## Optical Device Maintenance

**Table 6-2** XFP Transceiver Optical Transmit and Receive Specifications

| XFP Product Number | Transceiver Operating Mode                          | Transmit Power (dBm) |                                  | Receive Power (dBm) |                      | Transmit Wavelength (nm) | Receive Wavelength (nm) |
|--------------------|-----------------------------------------------------|----------------------|----------------------------------|---------------------|----------------------|--------------------------|-------------------------|
|                    |                                                     | Min                  | Max                              | Min                 | Max                  |                          |                         |
| XFP-10GLR-OC192SR  | 10GBASE-LR, 1310-nm SMF<br>(10.3125-Gbps line rate) | -8.2                 | +0.5                             | -14.4               | +0.5                 | 1260 to 1355             | 1260 to 1565            |
| XFP-10GER-OC192IR  | 10GBASE-ER, 1550-nm SMF<br>(10.3125-Gbps line rate) | -4.7                 | +4.0                             | -15.8               | -1.0                 | 1530 to 1565             | 1260 to 1565            |
| XFP-10GZR-OC192IR  | 10GBASE-ZR, 1550-nm SMF<br>(10.3125-Gbps line rate) | 0                    | +4.0                             | -24                 | -7                   | 1530 to 1565             | 1260 to 1565            |
| XFP-10G-MM-SR      | 10GBASE-SR, 850-nm MMF<br>(10.3125-Gbps line rate)  |                      | -1.0<br>-3.8<br>OMA <sup>1</sup> |                     | -1.0<br>-11.1<br>OMA | 840 to 860               | 840 to 860              |

1. At 840nm and a spectral width of 0.29nm

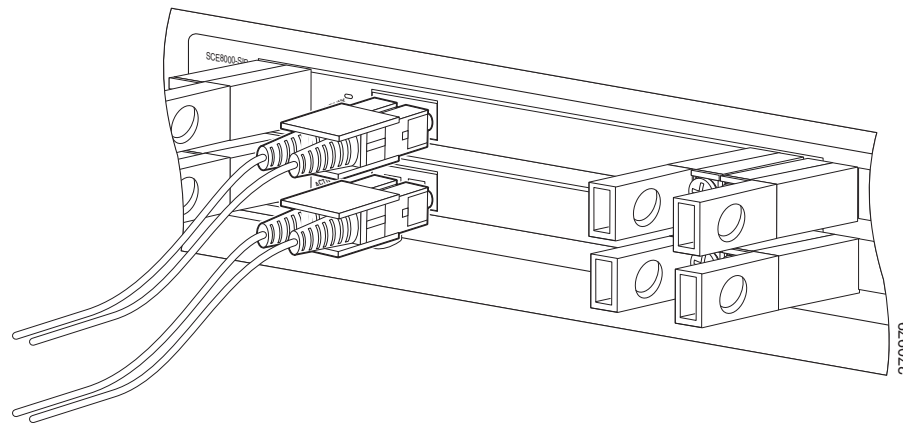
Any contamination of the fiber connection can cause failure of the component or failure of the whole system. A particle that partially or completely blocks the core generates strong back reflections, which can cause instability in the laser system. Inspection, cleaning, and reinspection are critical steps to take before making fiber-optic connections.

## How to Cable the 10 GBE Line Interface Ports

- Step 1** Take the appropriate fiber optic cable (see [XFP Module Cabling and Connection Equipment, page 6-11](#)) and plug it into the appropriate port on the 10 GBE interface on the SPA module in slot #3 of the Cisco SCE 8000. (See [Figure 6-1](#).)

Make sure to push on the connector until you hear a click, which indicates that the connector is fully inserted and secured in the receptacle. Always make sure that you insert the connector completely into the socket.

**Figure 6-1**      *Cabling the 10 GBE Interface*

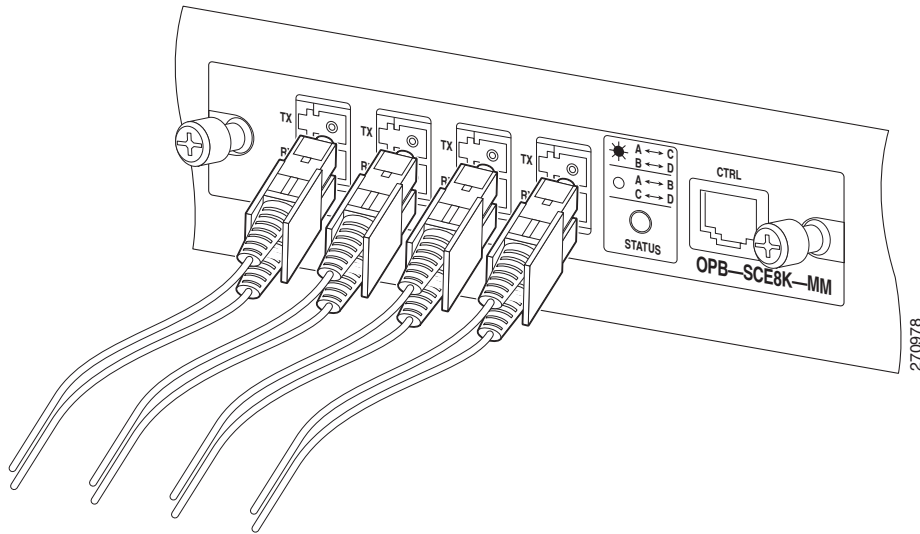


- Step 2** Verify that the link LED is green.
- If the link LED does not light, try removing the network cable plug and reinserting it firmly into the module socket.

## Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module

See [Optical Bypass Module Connectivity, page 6-9](#) for specific connectivity ([Figure 6-2](#)).

**Figure 6-2** External Optical Bypass Module Line Interfaces



- Step 1** Take the appropriate fiber optic cable (see [XFP Module Cabling and Connection Equipment, page 6-11](#)) and plug it into the appropriate port (A or B) on the external bypass module.
- Step 2** Using a cable with LC connectors on both ends, plug one end into the appropriate port (C or D) on the external bypass module and the other end into the appropriate 10 GBE interface in slot 3 of the Cisco SCE 8000 chassis.

- Step 3** Using the control cable provided, which has RJ11 connectors on both ends, plug one end into the CTRL interface on the external bypass module (see [Figure 6-3](#)) and plug the other end into the External Bypass interface on the Cisco SCE 8000-SCM-E in slot 1 of the Cisco SCE 8000 chassis (see item 1 in [Figure 6-4](#)). If using only one external bypass module, use External Bypass port 1. If using two external bypass modules, use both External Bypass ports on the Cisco SCE 8000-SCM-E in slot 1.
- Step 4** Complete the installation and powering up of the Cisco SCE 8000.
- By its nature, the optic bypass module does not connect the link to the Cisco SCE 8000-SIP module until the entire Cisco SCE 8000 system is fully functional. It is necessary to bring the Cisco SCE 8000 to fully operational and non-bypassed status to confirm correct functioning of the link through the optic bypass module to the Cisco SCE 8000-SIP module.
- Step 5** Verify link connectivity by checking that the link LED on the 10 GBE interface is green, or by using the Cisco SCE 8000 command line.

**Figure 6-3** Cabling the CTRL Interface on the External Bypass Module

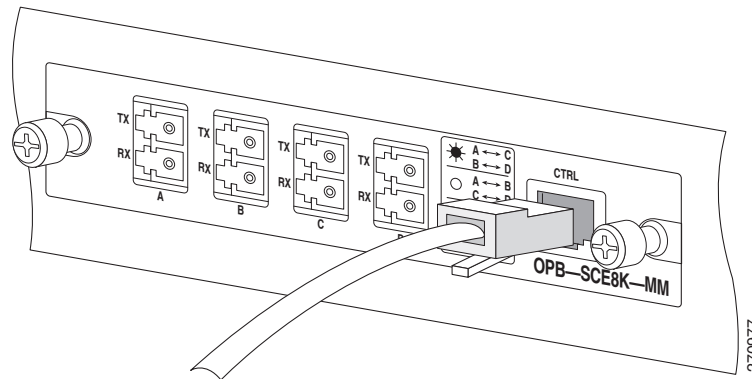
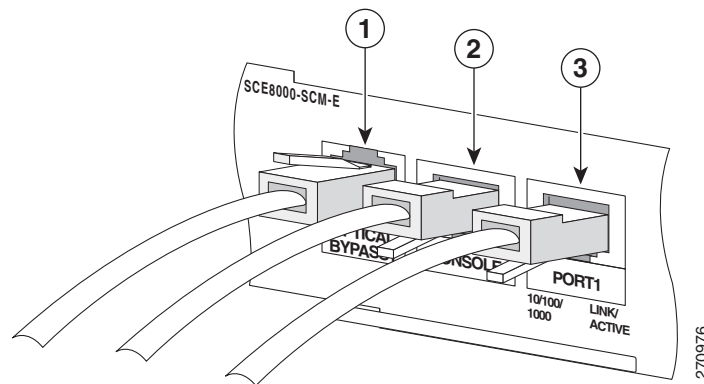


**Figure 6-4** Cabling the Cisco SCE 8000-SCM-E Module



## Testing Connectivity: Examining Link LEDs and Counters

If the Cisco SCE 8000 platform has been powered up, verify that connectivity has been established on all links. If the Cisco SCE 8000 platform is not powered up, perform this step after starting the Cisco SCE 8000 platform.

This section contains the following topics:

- [Examining the LEDs, page 6-16](#)
- [How to View the Ten Gigabit Ethernet Port Status, page 6-16](#)
- [How to View the Ten Gigabit Ethernet Counters, page 6-16](#)
- [How to View the User Log Counters, page 6-17](#)

### Examining the LEDs

The 10 GBE Link LED should be green, verifying that an active connection exists.

### How to View the Ten Gigabit Ethernet Port Status

To view the ten gigabit ethernet port status, enter **show interface TenGigabitEthernet 3/baynumber/0** at the **SCE>** prompt. This displays the port link status.

The following example displays a system response:

```
SCE# show interface TenGigabitEthernet 3/1/0
Actual Status:
Link is on
Bandwidth: 10000000Kbps
Burst-size: 500000bytes
```

### How to View the Ten Gigabit Ethernet Counters

In an inline topology, you can monitor traffic via the platform counters for both the Rx and Tx connections. The counters increase as packets flow through the Cisco SCE 8000 for both Rx and Tx.

However, in receive-only topologies, the counters for the Tx do not increment, as the Cisco SCE 8000 is only monitoring traffic, and not re-transmitting it.

To view the ten gigabit ethernet counters, enter **show interface TenGigabitEthernet 3/baynumber/0 counters** at the **SCE>** prompt. This displays the TenGigabitEthernet counters. This command enables you to verify that traffic is taking place. The counters increase together with real-time packet flow through the Cisco SCE 8000.

Remember, in bump-in-the-wire topology, both the Rx and Tx counters apply as traffic monitors. For receive-only topologies, using an external splitter, only the Rx counters apply.

The following example shows the counters of the first Ten Gigabit Ethernet interface:

```
SCE> show interface TenGigabitEthernet 3/0/0 counters
In total octets: 100
In good unicast packets: 90
In good multicast packets: 0
In good broadcast packets: 10
In packets discarded: 0
In packets with CRC/Alignment error: 0
In undersized packets: 0
In oversized packets: 0
Out total octets: 93*2^32+1022342538
Out unicast packets: 858086051
Out non unicast packets: 0
Out packets discarded: 0
```

## How to View the User Log Counters

You should view the user log for errors that occurred during the installation process.

- 
- Step 1** To view the user log counters, enter **show logger device User-File-Log counters** at the **SCE>** prompt and press **Enter**.
- 

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

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

## How to Install a Service Control Application

The Service Control solution requires that the Service Control application be installed on the SCE platform. This is a pqi file that is installed and configured using the Cisco Service Control Application for Broadband (SCA BB) console.

For an explanation of how to install the pqi file, see [Installing the Application and Protocol Pack on the SCE Platform](#) in the *Cisco Service Control Product Installation Guide*.

For information on initial configuration of the application, see [Initial SCA BB Configuration](#) in the *Cisco Service Control Product Installation Guide*.

For complete instructions on how to install and configure the SCA BB application, see the *Cisco Service Control Application for Broadband User Guide*.

# Cascaded Systems

This section contains the following topics:

- [How to Install a Cascaded System, page 6-19](#)
- [CLI Commands for Cascaded Systems, page 6-20](#)

## How to Install a Cascaded System

This section outlines the installation procedures for a redundant solution with two cascaded Cisco SCE 8000 platforms. See the [Cisco SCE8000 CLI Command Reference](#) for details of the CLI commands.

When working with two Cisco SCE 8000 platforms with split-flow and redundancy, it is extremely important to follow this installation procedure.

- 
- Step 1** Install both Cisco SCE 8000 platforms, power them up, and perform the initial system configuration. (See [Chapter 4, “Installing the Cisco SCE 8000 Chassis”](#) and [Chapter 5, “Connecting the Management Interfaces”](#) and the “Starting the Cisco SCE 8000 Platform” section on page 7-2.)
- To maintain link continuity at all times, including during the reload sequence and power failure events, it is recommended to install optical bypass modules.
- Step 2** Connect both Cisco SCE 8000 platforms to the management station. (See [Connecting the Management Interfaces, page 5-5.](#))
- Step 3** Connect the cascade ports. (See [Dual Link: Two Cisco SCE 8000s Topology, page 6-3.](#))
- The cascade ports must be either be connected directly in Layer 1 (dark fibers), or using the following procedure to connect through a switch:
- a. Connect port 3/2/0 from box A and port 3/3/0 from box B to a single switch. Configure them both on the same access VLAN, which is used only by the interfaces connected to these ports. No other interfaces in the switch should reside on that VLAN.
  - b. Connect port 3/3/0 from box A and port 3/2/0 of box B to a switch on a different VLAN. Again, the access ports should be configured as access ports on this VLAN, which are used only by the interfaces connected to these ports. No other interfaces in the switch reside on the VLAN.
- Step 4** Set topology configurations for each Cisco SCE 8000 platform via the connection-mode options. (See [How to Configure the Connection Mode, page 6-21.](#))
- Step 5** Make sure that the Cisco SCE 8000 platforms have synchronized and the active Cisco SCE 8000 platform was selected.
- Use the **show interface linecard 0 connection-mode** command.
- Step 6** If you want to start with bypass, change the link mode to your required mode in both Cisco SCE 8000 platforms on both links. The bypass mode is applied only to the active Cisco SCE 8000 platform. (See [How to Set the Link Mode, page 6-21.](#))
- Step 7** Ensure that the link mode complies with what you required. (See [Monitoring a Cascaded System, page 6-22.](#))
- Use the **show interface linecard 0 link mode** command.
- Step 8** Connect the traffic port of Cisco SCE 8000 platform 1. This causes a momentary down time until the network elements from both sides of the Cisco SCE 8000 platform auto-negotiate with it and starts working (when working inline). (See [Dual Link: Two Cisco SCE 8000s Topology, page 6-3.](#))

- Step 9** Connect the traffic port of Cisco SCE 8000 platform 2. This causes a momentary down time until the network elements from both sides of the Cisco SCE 8000 platform auto-negotiate with it and starts working (when working inline). (See [Dual Link: Two Cisco SCE 8000s Topology, page 6-3](#).)
- Step 10** When full control is needed, change the link mode on both Cisco SCE 8000 platforms on both links to ‘forwarding’. It is recommended to first configure the active Cisco SCE 8000 platform and then the standby. (See [How to Set the Link Mode, page 6-21](#).)

## CLI Commands for Cascaded Systems

This section presents CLI commands relevant to the configuration and monitoring of a redundant system.

- [Topology-Related Parameters for Redundant Topologies, page 6-20](#)
- [How to Configure the Connection Mode, page 6-21](#)
- [How to Set the Link Mode, page 6-21](#)
- [Monitoring a Cascaded System, page 6-22](#)

### Topology-Related Parameters for Redundant Topologies

All four of the topology-related parameters are required when configuring a redundant topology:

- **Connection mode**—Redundancy is achieved by cascading two SCE platforms. Therefore the connection mode for both SCE platforms is:
  - Inline-cascade
- **sce-id**—In cascaded topologies, defines which link is connected to this SCE platform.

The sce-id parameter, which identifies the SCE platform, replaces the physically-connected-link parameter, which identified the link. This change was required with the introduction of the Cisco SCE 8000 GBE platform, which supports multiple links.

In the Cisco SCE 8000 10 GBE, the number assigned to the sce-id parameter (0 or 1) is defined as the of number of the physically connected link.



#### Note

For backward compatibility, the physically-connected-links parameter is still recognized.

- **Priority**—For each of the cascaded SCE platforms, this parameter defines whether it is the primary or secondary device.
- **On-failure**—For each of the cascaded SCE platforms, this parameter determines whether the system cuts the traffic or bypasses it via an external optical bypass module when the SCE platform either has failed or is booting.

If either the *bypass* or *external-bypass* option is configured, the optical bypass module must be properly installed. If an optical bypass device is not detected, the command is executed but a warning is issued. The system then enters warning mode until either the command is changed, or the presence of an optical bypass device is detected.

## How to Configure the Connection Mode

Use the following procedure to configure the connection mode, including the following parameters:

- inline
- sce-id (or physically connected links)
- behavior upon failure of the SCE platform
- primary/secondary

To configure the connection mode, enter **connection-mode** *inline-cascade* **physically-connected-links** (*link-0link-1*) **priority** (*primarysecondary*) **on-failure** (*external-bypassbypasscutoff*) from the SCE(config if)# prompt and press **Enter**.

### EXAMPLE 1

Use the following command to configure the primary SCE platform in a two-SCE platform inline topology. Link 1 is connected to this SCE platform. If a failure occurs, the behavior of the SCE platform is bypass.

```
SCE(config if)# connection-mode inline-cascade physically-connected-links link-1 priority  
primary on-failure bypass
```

### EXAMPLE 2

Use the following command to configure the SCE platform that might be cascaded with the SCE platform in Example 1. This SCE platform would be the secondary SCE platform. Because Link 1 was connected to the primary, Link 0 would be connected to this SCE platform. The connection mode would be the same as the first. If a failure occurs, the behavior of the SCE platform is also bypass.

```
SCE(config if)# connection-mode inline-cascade physically-connected-links link-0 priority  
secondary on-failure bypass
```

## How to Set the Link Mode

The SCE platform has an internal hardware card used to maintain the links even when the SCE platform fails. This hardware card has three possible modes of operation:

- bypass
- forwarding
- cutoff

Normally, the link mode is selected by the SCE platform software according to the configured connection-mode. However, the **link mode** command can be used to enforce a specific desired mode. This may be useful when debugging the network, or in cases where we would like the SCE platform just to forward the traffic. (This is only relevant to inline topologies even though the configuration is available also when in receive-only mode.)

The following link mode options are available:

- **Forwarding**—Forwards traffic on the specified link to the SCE platform for processing.
- **Bypass**—Stops all forwarding of traffic on the specified link to the SCE platform. Traffic still flows on the link, but is not processed in any way by the SCE platform.

This does not affect the redundancy states.

- **Cutoff**—Completely cuts off flow of traffic through the specified link.

Note the following recommendations and restrictions:

- Link mode is relevant only to inline topologies.
- It is recommended that in cascaded topologies, both SCE platforms be configured for the same link mode, otherwise the service is unpredictable.
- The default link mode is forwarding. When other link modes are selected, active service control is not available and any service control configuration is not applicable.

To set the link mode, enter **link mode [forwarding|bypass|cutoff]** from the **SCE(config if)#** prompt and press **Enter**.

## Monitoring a Cascaded System

Use the following commands to monitor a cascaded system. They provide information about the connection status and link configuration.

### How to View the Current Connection Mode

From the **SCE>** prompt, enter **show interface linecard 0 connection-mode** and press **Enter**.

### How to View the SCE-ID

From the **SCE>** prompt, enter **show interface linecard 0 sce-id** and press **Enter**.

### How to View the Current Link Mode

From the **SCE>** prompt, enter **show interface linecard 0 link mode** and press **Enter**.

### How to View the Current Redundancy Status of the SCE Platform

From the **SCE>** prompt, enter **show interface linecard 0 cascade redundancy-status** and press **Enter**.

### How to View Information about the Peer SCE Platform

From the **SCE>** prompt, enter **show interface linecard 0 cascade peer-sce-information** and press **Enter**.

### How to View Information about the Cascade Connections

From the **SCE>** prompt, enter **show interface linecard 0 cascade connection-status** and press **Enter**.

### How to View the Current Link Mappings

From the **SCE>** prompt, enter **show interface linecard 0 physically-connected-links** and press **Enter**.



# Basic Cisco SCE 8000 Platform Operations

---

Revised: February 18, 2015

## Introduction

This chapter describes how to start up the Cisco SCE 8000 platform, reboot, and shutdown. It also describes how to manage configurations, and contains the following sections:

- [Starting the Cisco SCE 8000 Platform, page 7-2](#)
- [Managing Cisco SCE 8000 Configurations, page 7-6](#)
- [Displaying the SCE Platform Version Information, page 7-12](#)
- [Displaying the SCE Platform Inventory, page 7-15](#)
- [Displaying the System Uptime, page 7-19](#)
- [Rebooting and Shutting Down the SCE Platform, page 7-20](#)

# Starting the Cisco SCE 8000 Platform

The procedures for starting the Cisco SCE 8000 platform are explained in the following sections:

- [Checking Conditions Before System Startup, page 7-2](#)
- [Performing Complex Configurations, page 7-2](#)
- [Starting the System and Observing Initial Conditions, page 7-3](#)
- [Final Tests, page 7-3](#)

## Checking Conditions Before System Startup

Check the following conditions before you start your Cisco SCE 8000 platform:

- Both power supply units are installed and connected. (If only one power supply is connected it puts the box in warning state.)
- First-time startup at installation:
  - Cisco SCE 8000 platform connected to local console (CON port).
  - The console terminal is turned on and properly configured.
- Subsequent startups
  - Line interfaces are properly cabled (optional).
  - Cisco SCE 8000 platform is connected to at least one of the following types of management stations:
    - Direct connection to local console (CON port).
    - Remote management station via the LAN (Mng port).

## Performing Complex Configurations

After you have installed your Cisco SCE 8000 platform hardware, checked all external connections, turned on the system power, allowed the system to boot up, and performed the initial system configuration, you might need to perform more complex configurations, which are beyond the scope of this publication.

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

- [Cisco SCE8000 10GBE Software Configuration Guide](#)
- [Cisco SCE8000 CLI Command Reference](#)

## Starting the System and Observing Initial Conditions

After installing your Cisco SCE 8000 platform and connecting cables, complete the following steps to start the Cisco SCE 8000 platform:

- 
- Step 1** Ensure the power cables are connected to the Cisco SCE 8000 platform.
- Step 2** Plug the AC power supply cables into the AC power source, or make sure the circuit breakers at the DC panels are turned to the on position. Turn on the switches on both power supplies.
- Step 3** Listen for the fans; you should immediately hear them operating.
- Step 4** During the boot process, observe the following LEDs on the Cisco SCE 8000-SCM-E:
- The Power LEDs should be green.
  - Optical Bypass LED should be green while the Cisco SCE 8000 is in bypass and unlit when the optical bypass is turned off.
  - The Status LED should be a constant amber while booting. After a successful boot, the Status LED is steady green.

**Note**

It takes a several minutes for the Cisco SCE 8000 to boot and for the status LED to change from amber to green.

---

## What to Do Next

If the system does not complete each of the steps in the startup procedure, proceed to [Identifying Startup Problems, page 8-7](#) for troubleshooting recommendations and procedures.

## Final Tests

The procedures for performing the final tests to verify that the Cisco SCE 8000 is functioning properly are explained in the following sections:

- [Verifying Operational Status, page 7-4](#)
- [Viewing the User Log Counters, page 7-4](#)
- [Viewing the Ten Gigabit Ethernet Port Status, page 7-4](#)
- [Viewing the Ten Gigabit Ethernet Counters, page 7-5](#)

## Verifying Operational Status

After all the ports are connected, verify that the Cisco SCE 8000 is not in a Warning state.

---

**Step 1** On the front panel of the Service Control module, examine the Status LED; it should be green.

**Step 2** To display the operation status of the system, at the Cisco SCE 8000# prompt, enter **show system operation-status** and press **Enter**.

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

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

If the Status LED is red or flashing amber, the following message appears:

```
System Operation status is Warning
```

```
Description:
```

```
1. Power Supply problem
```

```
2. Line feed problem
```

```
3. Amount of External bypass devices detected is lower than expected amount
```

---

## Viewing the User Log Counters

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

At the SCE# prompt, enter **show logger device user-file-log counters** and press **Enter**.

### Example for Viewing the User Log Counters

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

```
SCE# show logger device user-file-log counters
```

```
Logger device User-File-Log counters:
```

```
Total info messages: 1
```

```
Total warning messages: 0
```

```
Total error messages: 0
```

```
Total fatal messages: 0
```

If there are “Total error messages” or “Total fatal messages”, use the **show logger device user-file-log** command to display details about the errors.

## Viewing the Ten Gigabit Ethernet Port Status

At the Cisco SCE8000# prompt, enter **show interface TenGigabitEthernet 3/ baynumber /0**.

This displays the port link status.

The following example displays a system response:

```
Cisco SCE8000# show interface TenGigabitEthernet 3/1/0
```

```
Actual Status:
```

```
Link is on
```

```
Bandwidth: 10000000Kbps
```

```
Burst-size: 500000bytes
```

## Viewing the Ten Gigabit Ethernet Counters

In an inline topology, you can monitor traffic via the platform counters for both the Rx and Tx connections. The counters increase as packets flow through the Cisco SCE 8000 for both Rx and Tx.

However, in receive-only topologies, the counters for the Tx do not increment, as the Cisco SCE 8000 is only monitoring traffic, and not re-transmitting it

At the Cisco SCE8000# prompt, enter **show interface TenGigabitEthernet 3/ baynumber /0 counters**.

This displays the TenGigabitEthernet counters. This command enables you to verify that there is traffic on the line. You can see that the counters increase, together with real-time packet flow through the Cisco SCE 8000.

Remember, in bump-in-the-wire topology, both the Rx and Tx counters apply as traffic monitors. For receive-only topologies, using an external splitter, only the Rx counters apply.

The following example shows the counters of the first Ten Gigabit Ethernet interface:

```
Cisco SCE8000# show interface TenGigabitEthernet 3/0/0 counters
In total octets: 100
In good unicast packets: 90
In good multicast packets: 0
In good broadcast packets: 10
In packets discarded: 0
In packets with CRC/Alignment error: 0
In undersized packets: 0
In oversized packets: 0
Out total octets: 93*2^32+1022342538
Out unicast packets: 858086051
Out non unicast packets: 0
Out packets discarded: 0
```

# Managing Cisco SCE 8000 Configurations

After you have installed your Cisco SCE 8000 platform hardware, checked all external connections, turned on the system power, and allowed the system to boot up, you are ready to install the Service Control application. However, before you install the application, you might need to configure the SCE platform. Instructions for configuring the Cisco SCE 8000 platform are beyond the scope of this publication.

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

- [Cisco SCE8000 10GBE Software Configuration Guide](#)
- [Cisco SCE8000 CLI Command Reference](#)

The procedures for managing Cisco SCE 8000 configurations are explained in the following sections:

- [Viewing Configurations, page 7-6](#)
- [Saving or Changing the Configuration Settings, page 7-8](#)
- [Restoring a Previous Configuration, page 7-9](#)

## Viewing Configurations

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

The SCE platform provides commands for:

- Viewing the running configuration with only user-configured (non-default) values: **show running-config**
- Viewing the running configuration with all the SCE platform running configuration values, whether default or not: **show running-config all-data**
- Viewing the startup configuration: **show startup-config**

After configuring the SCE platform, you may query for the running configuration using the command **show running-config**.

**Step 1** At the Cisco SCE8000# prompt, enter **show running-config**.

The system shows the running configuration.

```
SCE8000#> show running-config
#This is a general configuration file (running-config).
#Created on 12:06:13 UTC SUN May 11 2008
#cli-type 1
#version 1
no management-agent notifications notification-list
1417,1418,804,815,1404,1405,1406,1407,1408,400
no management-agent notifications notification-list
402,421,440,441,444,445,446,450,437,457
no management-agent notifications notification-list 3593,3594,3595,10040
snmp-server community "public" ro
RDR-formatter forwarding-mode multicast
RDR-formatter destination 10.56.96.26 port 33000 category number 1 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 2 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 3 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 4 priority 100
interface LineCard 0
connection-mode inline on-failure external-bypass
no silent
no shutdown
attack-filter subscriber-notification ports 80
replace spare-memory code bytes 3145728
interface GigabitEthernet 1/1
ip address 10.56.96.46 255.255.252.0
interface TenGigabitEthernet 3/0/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/1/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/2/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/3/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"

exit
ip default-gateway 10.56.96.1
line vty 0 4
exit
management-agent property "com.pcube.management.framework.install.activation.operation"
"Install"
management-agent property "com.pcube.management.framework.install.activated.package" "SCA
BB"
management-agent property "com.pcube.management.framework.install.activated.version"
"3.1.6 build 79"
management-agent property "com.pcube.management.framework.install.activation.date" "Sun
May 11 08:44:04 GMT+00:00 2008"
flow-filter partition name "ignore_filter" first-rule 4 num-rules 32
flow-filter partition name "udpPortsToOpenBySw" first-rule 40 num-rules 21
```

## Saving or Changing the Configuration Settings

When you make changes to the current running configuration and you want those changes to continue to be in effect when the system restarts, you must save the changes before leaving the management session. This can be done by saving the running configuration to the startup configuration file.

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

For backup purposes, the old startup-config file is saved under the directory: `/system/prevconf`. See [Restoring a Previous Configuration, page 7-9](#) for an explanation on how to restore a previous configuration.

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

- 
- Step 1** At the **SCE#** prompt, enter **show running-config** to view the running configuration.  
The running configuration is displayed.
- Step 2** Check the displayed configuration to make sure that it is set the way you want. If not, make the changes you want before saving.
- Step 3** Enter **copy running-config startup-config**.  
The system saves all running configuration information to the configuration file, which is used when the system reboots.  
The configuration file holds all information that is different from the system default in a file called *config.txt* located in the directory: `/system`.
- 

## Example for Saving or Changing the Configuration Settings

The following example shows how to save the running configuration file (first displaying the file to review the settings):

```
SCE# show running-config
#This is a general configuration file (running-config).
#Created on 12:06:13 UTC SUN May 11 2008
#cli-type 1
#version 1
no management-agent notifications notification-list
1417,1418,804,815,1404,1405,1406,1407,1408,400
no management-agent notifications notification-list
402,421,440,441,444,445,446,450,437,457
no management-agent notifications notification-list 3593,3594,3595,10040
snmp-server community "public" ro
RDR-formatter forwarding-mode multicast
RDR-formatter destination 10.56.96.26 port 33000 category number 1 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 2 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 3 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 4 priority 100
interface LineCard 0
connection-mode inline on-failure external-bypass
no silent
no shutdown
attack-filter subscriber-notification ports 80
```

```

replace spare-memory code bytes 3145728
interface GigabitEthernet 1/1
ip address 10.56.96.46 255.255.252.0
interface TenGigabitEthernet 3/0/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/1/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/2/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/3/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"

exit
ip default-gateway 10.56.96.1
line vty 0 4
exit
management-agent property "com.pcube.management.framework.install.activation.operation"
"Install"
management-agent property "com.pcube.management.framework.install.activated.package" "SCA
BB"
management-agent property "com.pcube.management.framework.install.activated.version"
"3.1.6 build 79"
management-agent property "com.pcube.management.framework.install.activation.date" "Sun
May 11 08:44:04 GMT+00:00 2008"
flow-filter partition name "ignore_filter" first-rule 4 num-rules 32
flow-filter partition name "udpPortsToOpenBySw" first-rule 40 num-rules 21
SCE# copy running-config startup-config
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
SCE#

```

**Tip**


---

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

---

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

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

## Restoring a Previous Configuration

When you save a new configuration, the system automatically backs up the old configuration in the directory `/system/prevconf/`. Up to nine versions of the startup configuration file are saved, namely `config.tx1-config.tx9`, where `config.tx1` is the most recently saved file.

View the old startup configuration files using the CLI command **more**.

Restoring a previous startup configuration means renaming the file so it overwrites the startup configuration (`config.txt`) file.

- 
- Step 1** At the **SCE#** prompt, enter **more /system/prevconf/config.tx1** to view the configuration file.  
The system displays the configuration information stored in the file.
- Step 2** Read the configuration information to make sure it is the configuration you want to restore.  
You cannot undo the configuration restore command.
- Step 3** Enter **copy /system/config.tx1 /system/config.txt**.  
The system sets the startup configuration to the configuration from *config.tx1*.
- 

## Example for Restoring a Previous Configuration

The following example displays a saved configuration file and then restores the file to overwrite the current configuration:

```
SCE# more /system/prevconf/config.tx1
#This is a general configuration file (running-config).
#Created on 12:07:41 UTC SUN May 11 2008
#cli-type 1
#version 1
no management-agent notifications notification-list
1417,1418,804,815,1404,1405,1406,1407,1408,400
no management-agent notifications notification-list
402,421,440,441,444,445,446,450,437,457
no management-agent notifications notification-list 3593,3594,3595,10040
snmp-server community "public" ro
RDR-formatter forwarding-mode multicast
RDR-formatter destination 10.56.96.26 port 33000 category number 1 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 2 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 3 priority 100
RDR-formatter destination 10.56.96.26 port 33000 category number 4 priority 100
interface LineCard 0
connection-mode inline on-failure external-bypass
no silent
no shutdown
attack-filter subscriber-notification ports 80
replace spare-memory code bytes 3145728
interface GigabitEthernet 1/1
ip address 10.56.96.46 255.255.252.0
interface TenGigabitEthernet 3/0/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/1/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/2/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"
interface TenGigabitEthernet 3/3/0
bandwidth 10000000 burst-size 50000
global-controller 0 name "Default Global Controller"

exit
ip default-gateway 10.56.96.1
line vty 0 4
exit
```

```
management-agent property "com.pcube.management.framework.install.activation.operation"
"Install"
management-agent property "com.pcube.management.framework.install.activated.package" "SCA
BB"
management-agent property "com.pcube.management.framework.install.activated.version"
"3.1.6 build 79"
management-agent property "com.pcube.management.framework.install.activation.date" "Sun
May 11 08:44:04 GMT+00:00 2008"
flow-filter partition name "ignore_filter" first-rule 4 num-rules 32
flow-filter partition name "udpPortsToOpenBySw" first-rule 40 num-rules 21
SCE# copy /system/config.tx1 /system/config.txt
```

## Displaying the SCE Platform Version Information

Use this command to display global static information on the SCE platform, such as software and hardware version, image build time, system uptime, last open packages names and information on the SLI application assigned.

From the **SCE>** prompt, enter **show version** and press **Enter**.

### Example for Displaying the SCE Platform Version Information

The following example shows how to display the SCE platform version information:

```
SCE> show version
System version: Version 3.1.6S Build 279
Build time: Jun 10 2008, 19:27:47 (Change-list 335658)
Software version is: Version 3.1.6S Build 279
Hardware information is:
-----
Firmware
-----
kernel : [kernel] 1.0.0/5 (inactive: [kernel] 1.0.0/5)
u-boot : [uboot] 1.0.0/6 (field: [uboot] 0.8.1/13)
select : [ubs-cf1] 1.0.0/5 (secondary: [ubs-cf1] 1.0.0/5)
-----
Slot 1: SCM-8000
-----
serial-num : CAT1202G07D
part-num : 73-10598-01 38
cpld : 0x8162
vtpld : 0xc001
summit-0 : 0x10008
summit-1 : 0x10008
dpt/tx : 0x4837
cls/ff : 0x2047
cls flow cap: 33554432

-----
TVR
-----
#cpus : 1
cpu SVR : 0x80900120
cpu PVR : 0x80040202
cpu freq : 1000MHz
cpu (eeprom): 2.1, 1000MHz
cpld : 0xa1b7
cpld-ufm : 0xa803
summit : 0x10007
cf : Model=SMART CF, FwRev=0x20060811, Size=4062240KB
-----
CFC-0
-----
board type : P2
#cpus : 3
cpu-0 SVR : 0x80900121
cpu-0 PVR : 0x80040202
cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
```

```
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb20e
cpld-1 : 0xb20e
cpld-2 : 0xb20e
cpld-0-ufm : 0xb803
cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1044
-----
CFC-1
-----
board type : P2
#cpus : 3
cpu-0 SVR : 0x80900121
cpu-0 PVR : 0x80040202
cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb20e
cpld-1 : 0xb20e
cpld-2 : 0xb20e
cpld-0-ufm : 0xb803
cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1044
-----
Slot 3: SIP-8000
-----
serial-num : CAT1204G01H
part-num : 73-10947-01
cpld : 0x9162
summit-0 : 0x10006
summit-1 : 0x10006
dpt-0 : 0x3033
dpt-1 : 0x3033
spa[0] : SPA-1X10GE-L-V2
spa[1] : SPA-1XTENGE-XFP
spa[2] : SPA-1X10GE-L-V2
spa[3] : SPA-1XTENGE-XFP
-----
SCE8000 Chassis
-----
product-num : CISCO7604
serial-num : FOX10420BKZ
part-num : 73-9789-02
part-rev : A0
vid : V01
Part number: 73-10598-01 38
Revision:
Software revision:
LineCard S/N : CAT1202G07D
Power Supply type: AC
SML Application information is:
```

**Example for Displaying the SCE Platform Version Information**

```
No application is configured.  
Logger status: Enabled
```

```
Platform: SCE8000 - 4x10GBE  
Management agent interface version: SCE Agent 3.1.6 Build 134  
Software package file: ftp://ftpserver/simba.pkg  
SCE8000 uptime is 9 minutes, 54 seconds
```

# Displaying the SCE Platform Inventory

Unique Device Identification (UDI) is a Cisco baseline feature that is supported by all Cisco platforms. This feature allows network administrators to remotely manage the assets in their network by tracing specific devices through either CLI or SNMP. The user can display inventory information for a remote device through one of the following:

- Entity MIB (see *ENTITY-MIB* that is described in the “*Cisco Service Control MIBs*” appendix of *Cisco SCE8000 10GBE Software Configuration Guide*)

- CLI **show inventory** command

This command displays the UDIs only for field replaceable units (FRU).

- CLI **show inventory raw** command

This command displays all UDIs on the Cisco SCE 8000 platform.

The **show inventory** CLI commands display the following information:

- Device name
- Description
- Product identifier
- Version identifier
- Serial number

From the **SCE>** prompt, enter **show inventory [raw]** and press **Enter**.

## Examples for Displaying the SCE Platform Inventory

- [Displaying the SCE Platform Inventory: FRUs Only, page 7-15](#)
- [Displaying the Complete SCE Platform Inventory, page 7-16](#)

### Displaying the SCE Platform Inventory: FRUs Only

The following example shows how to display the inventory (UDIs) for the FRUs only:

```
SCE> show inventory
NAME: "SCE8000 Chassis", DESCR: "CISCO7604"
PID: CISCO7604 , VID: V0 , SN: FOX105108X5
NAME: "SCE8000 Service Control Module (SCM) in slot 1", DESCR: "SCE8000-SCM-E"
PID: SCE8000-SCM-E , VID: V0 , SN: CAT1122584N
NAME: "SCE8000 SPA Interface Processor (SIP) in slot 3", DESCR: "SCE8000-SIP"
PID: SCE8000-SIP , VID: V0 , SN: CAT1150G07F

NAME: "SPA-1X10GE-L-V2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2 , VID: V02, SN: JAE11517RMR

NAME: "SPA-1X10GE-L-V2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2 , VID: V02, SN: JAE11496E1P

NAME: "SPA-1X10GE-L-V2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2 , VID: V02, SN: JAE11517RIO

NAME: "SPA-1X10GE-L-V2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2 , VID: V02, SN: JAE115295HH
```

```

NAME: "SCE8000 FAN 1", DESCR: "FAN-MOD-4HS"
PID: FAN-MOD-4HS , VID: V0 , SN: DCH11013744

NAME: "SCE8000 AC or DC power supply 0", DESCR: "PWR-2700-AC/4"
PID: PWR-2700-AC/4 , VID: V0 , SN: APQ105000MV

NAME: "SCE8000 AC or DC power supply 1", DESCR: "PWR-2700-AC/4"
PID: PWR-2700-AC/4 , VID: V0 , SN: APQ105000MV

NAME: "XFP-10GLR-OC192SR ", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1142N4B7

NAME: "XFP-10GLR-OC192SR ", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1142N4AL

NAME: "XFP-10GLR-OC192SR ", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1141N43R

NAME: "XFP-10GLR-OC192SR ", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1143N4JN

```

## Displaying the Complete SCE Platform Inventory

The following example shows how to display the complete inventory (UDIs) of the SCE platform:

```

SCE> show inventory raw
"SCE8000 Chassis", DESCR: "CISCO7604"
PID: CISCO7604 , VID: V01, SN: FOX105108X5

NAME: "SCE8000 Physical Slot 1", DESCR: "Container SCE8000 Service Control Module (SCM)
slot"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Physical Slot 2", DESCR: "Container SCE8000 Service Control Module (SCM)
slot"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Physical Slot 3", DESCR: "Container SCE8000 SPA Interface Processor (SIP)
slot"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Physical Slot 4", DESCR: "Container SCE8000 Optical Bypass slot"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Fan Module", DESCR: "Container SCE8000 Fan Module"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 AC and DC power supply", DESCR: "Container SCE8000 AC and DC power supply"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Link", DESCR: "Container SCE8000 Link"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Backplane", DESCR: "Container SCE8000 Backplane "
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 Service Control Module (SCM) in slot 1", DESCR: "SCE8000-SCM-E"
PID: SCE8000-SCM-E , VID: V01, SN: CAT1122584N

NAME: "SCE8000 SPA Interface Processor (SIP) in slot 3", DESCR: "SCE8000-SIP"

```

```
PID: SCE8000-SIP          , VID: V01, SN: CAT1150G07F

NAME: "SCE8000 Link 0", DESCR: "SCE8000 Link"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 Link 1", DESCR: "SCE8000 Link"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 SIP bay 3/0", DESCR: "SCE8000 SIP bay"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 SIP bay 3/1", DESCR: "SCE8000 SIP bay"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 SIP bay 3/2", DESCR: "SCE8000 SIP bay"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 SIP bay 3/3", DESCR: "SCE8000 SIP bay"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 SPA module 3/0", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2    , VID: V02, SN: JAE11517RMR

NAME: "SCE8000 SPA module 3/1", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2    , VID: V02, SN: JAE11496E1P

NAME: "SCE8000 SPA module 3/2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2    , VID: V02, SN: JAE11517RIO

NAME: "SCE8000 SPA module 3/3", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2    , VID: V02, SN: JAE115295HH

NAME: "TenGigabitEthernet3/0/0", DESCR: "SCE8000 SPA port"
PID: ""                  , VID: "" , SN: ""

NAME: "TenGigabitEthernet3/1/0", DESCR: "SCE8000 SPA port"
PID: ""                  , VID: "" , SN: ""

NAME: "TenGigabitEthernet3/2/0", DESCR: "SCE8000 SPA port"
PID: ""                  , VID: "" , SN: ""

NAME: "TenGigabitEthernet3/3/0", DESCR: "SCE8000 SPA port"
PID: ""                  , VID: "" , SN: ""

NAME: "SCE8000 FAN 1", DESCR: "FAN-MOD-4HS"
PID: FAN-MOD-4HS        , VID: V01, SN: DCH11013744

NAME: "SCE8000 AC power supply 0", DESCR: "PWR-2700-AC/4"
PID: PWR-2700-AC/4      , VID: V02, SN: APQ105000MV

NAME: "SCE8000 DC power supply 1", DESCR: "PWR-2700-DC/4"
PID: PWR-2700-DC/4      , VID: V03, SN: APQ1049000S

NAME: "SCE8000 optic 3/0/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1142N4B7

NAME: "SCE8000 optic 3/1/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1142N4AL

NAME: "SCE8000 optic 3/2/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1141N43R

NAME: "SCE8000 optic 3/3/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: AGA1143N4JN
```

```
NAME: "SCE8000 traffic processor 1", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 2", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 3", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 4", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 5", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 6", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 7", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 8", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 9", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 10", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 11", DESCR: "SCE8000 traffic processor"
PID: " " , VID: " " , SN: " "

NAME: "SCE8000 traffic processor 12", DESCR: "SCE8000 traffic processor"
```

## Displaying the System Uptime

Use this command to see how long the system has been running since the last reboot.

At the **SCE>** prompt, enter **show system-uptime** and press **Enter**.

### Example for Displaying the System Uptime

The following example shows how to display the system uptime of the SCE platform.

```
SCE# show system-uptime
Cisco SCE8000 uptime is 21 minutes, 37 seconds
```

# Rebooting and Shutting Down the SCE Platform

This section describes the following topics:

- [Rebooting the SCE Platform, page 7-20](#)
- [How to Shut Down the SCE Platform, page 7-20](#)

## Rebooting the SCE Platform

Rebooting the SCE platform is required after installing a new package, in order for that package to take effect. There might be other occasions where rebooting the SCE platform is necessary.

**Note**

When the SCE restarts, it loads the startup configuration, so all changes made in the running configuration are lost. Save the running configuration before performing reload, as described in [Saving or Changing the Configuration Settings, page 7-8](#).

- 
- Step 1** At the **SCE#** prompt, enter **reload** and press **Enter**.  
A confirmation message appears.
- Step 2** Enter **y** to confirm the reboot request and press **Enter**.
- 

## Examples for Rebooting the SCE Platform

The following example shows the commands for system reboot:

```
SCE# reload
Are you sure? y
the system is about to reboot, this will end your CLI session
```

## How to Shut Down the SCE Platform

Shutting down the SCE platform is required before turning the power off. This helps to ensure that non-volatile memory devices in the SCE platform are properly flushed in an orderly manner.

**Note**

When the SCE platform restarts, it loads the startup configuration, so all changes made in the running configuration are lost. Save the running configuration before performing reload, as described in [Saving or Changing the Configuration Settings, page 7-8](#).

- 
- Step 1** Connect to the serial console port (The CON connector on the front panel of the Service Control module in slot 1, 9600 baud).  
The **SCE#** prompt appears.
- Step 2** Enter **reload shutdown**.  
A confirmation message appears.

**Step 3** Enter **y** to confirm the shutdown request and press **Enter**.

---

## Examples for Shutting Down the SCE Platform

The following example shows the commands for system shutdown:

```
SCE# reload shutdown
You are about to shut down the system.
The only way to resume system operation after this
is to cycle the power off, and then back on.
Continue?
Y
IT IS NOW SAFE TO TURN THE POWER OFF.
```



### Note

Because the SCE platform can recover from the power-down state only by being physically turned off (or cycling the power), this command can only be executed from the serial CLI console. This limitation helps prevent situations in which a user issues this command from a Telnet session, and then realizes that the SCE platform cannot be accessed physically.

---





# Troubleshooting

---

Revised: February 18, 2015

## Introduction

Your Cisco SCE 8000 platform went through extensive testing before leaving the factory. However, if you encounter problems starting it, use the information in this chapter to help isolate the cause of the problems. The procedures in this chapter assume that you are troubleshooting the initial system startup, and that your Cisco SCE 8000 platform is in the original factory configuration. If you have removed or replaced components or changed any default settings, the recommendations in this chapter might not apply. Make sure to review the safety warnings listed in [Regulatory Compliance and Safety Information for the Cisco SCE8000](#) that accompanied your Cisco SCE 8000 platform before using the troubleshooting procedures in this chapter.

This chapter contains the following sections:

- [Troubleshooting Overview, page 8-2](#)
- [Troubleshooting with the User Log, page 8-13](#)

# Troubleshooting Overview

This section describes the troubleshooting methods used in this chapter and describes how the Cisco SCE 8000 platform is divided into subsystems for more efficient problem solving. If you are unable to easily solve the problem, contact a customer service representative for assistance and further instructions.

Provide the representative with the following information:

- Date you received the Cisco SCE 8000
- Chassis serial number
- Type of software and release number
- Brief description of the problem you are having
- Brief explanation of the steps you have taken to isolate and resolve the problem
- Maintenance agreement or warranty information

[Table 8-1](#) shows the general troubleshooting strategy described in this chapter. See this table, as necessary, to follow the steps to isolate problems to a specific subsystem and resolve the problem if possible.

**Table 8-1**      **Troubleshooting Strategy for Startup Problems**

|               | Action                                                                                                                                                                               | Yes                                                                                                                 | No                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Turn power on. Go to <a href="#">Step 2</a> .                                                                                                                                        | —                                                                                                                   | —                                                                                                               |
| <b>Step 2</b> | Check the following: <ul style="list-style-type: none"> <li>• Front panel power LED on?</li> <li>• Power supply 'Input OK' LEDs on?</li> <li>• 'Output fail' LEDs not on?</li> </ul> | Go to <a href="#">Step 3</a> .                                                                                      | See <a href="#">Troubleshooting the Power Subsystem</a> , page 8-8 and go to <a href="#">Step 3</a> .           |
| <b>Step 3</b> | Status LED red (failure)?                                                                                                                                                            | See <a href="#">Troubleshooting the Firmware Package Installation</a> , page 8-8 and go to <a href="#">Step 4</a> . | Go to <a href="#">Step 4</a> .                                                                                  |
| <b>Step 4</b> | Management interface operational?                                                                                                                                                    | Go to <a href="#">Step 5</a> .                                                                                      | See <a href="#">Troubleshooting the Management Subsystem</a> , page 8-9 and go to <a href="#">Step 5</a> .      |
| <b>Step 5</b> | Link interfaces operational?                                                                                                                                                         | Go to <a href="#">Step 6</a> .                                                                                      | See <a href="#">Troubleshooting the Link Interface Subsystem</a> , page 8-11 and go to <a href="#">Step 6</a> . |
| <b>Step 6</b> | System startup successful (all interfaces operating normally).                                                                                                                       | —                                                                                                                   | —                                                                                                               |

## Information About Troubleshooting Tools

There are two tools that will help you to successfully troubleshoot your Cisco SCE 8000 installation:

- [CLI Commands for Troubleshooting](#), page 8-3
- [Checking the LEDs](#), page 8-5

## CLI Commands for Troubleshooting

Use the following commands to provide information to help you troubleshoot installation of your Cisco SCE 8000 platform. See the [Cisco SCE8000 10GBE Software Configuration Guide](#) or the [Cisco SCE8000 CLI Command Reference](#) document for more information.

**Note**

Remember that if the management interface is not operational, you should connect the Cisco SCE 8000 platform to a local console so that you can enter CLI commands for troubleshooting.

- **Troubleshooting firmware package installation:**

- **boot system <filename>**—Specifies and verifies the package file to be installed. Error messages or other output identify problems with the package file.

Following is a sample output from the **boot system** command:

```
SCE(config)# boot system ftp://cisco:cisco@10.10.10.10/downloads/SENum.pkg.pkg
Verifying package file SENUM.pkg.pkg...
Package file verified OK.
```

- **Troubleshooting the management subsystem:**

- **show interface GigabitEthernet 1/1**—Displays IP address and auto-negotiation information for the management interfaces.

Following is a sample output from the **show interface GigabitEthernet 1/1** command:

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

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

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

```
Default gateway: 10.1.1.1
```

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

Following is a sample output from the **show ip route** command:

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

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

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

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

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

Following is a sample output from the **show telnet** command:

```
show telnet sessions
There is 1 active telnet session:
Index | Source
-----
0      | 10.1.1.201

show telnet status
Telnet daemon is enabled.
```

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

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

```
Timeout is 30 minutes
```

- **Troubleshooting the link interface subsystem:**

- **show interface TenGigabitEthernet 3/#/0**—Displays information for a specific 10 GBE Interface.

Following is a sample output from the **show interface** command:

```
Auto negotiation configured: Disabled
Actual status:
Link is: ON
Auto negotiation: Disabled
Bandwidth (L1): 10000000 Kbps, Burst-size: 500000 bytes
Pseudo IP Address: Not Configured
```

- **show interface TenGigabitEthernet 3/#/0 counters**—Displays the values of counters of a GBE interface.

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

```
L2 In total octets: 792000
In good unicast packets: 12000
In good multicast packets: 0
In good broadcast packets: 0
In packets discarded: 0
In packets with CRC/Alignment error: 0
In undersized packets: 0
In oversized packets: 0
Rx pause packets: 0
L2 Out total octets: 0
Out unicast packets: 0
Out good multicast packets: 0
Out good broadcast packets: 0
Out packets discarded: 0
Tx pause packets: 0
Tx regular collision events: 0
L2 Bandwidth Kbps (Rx + Tx): 0
# of packets received of length (in octets):
64: 0, 65-127: 12000, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0,
1519+: 0
```

See [Troubleshooting with the User Log](#), page 8-13 for an explanation of commands related to the user log.

## Checking the LEDs

The LEDs on the Cisco SCE 8000-SMC-E front panel, along with the LEDs on the power supplies and fan assembly are the most immediate problem-detection mechanism of the platform. See the following sections for information on Cisco SCE 8000 platform LEDs:

- [Table 2-3 on page 2-5](#)
- [Examining the LEDs, page 6-16](#)
- [Starting the System and Observing Initial Conditions, page 7-3](#)
- [Cisco SCE 8000 Operational Status, page 8-5](#)

### Cisco SCE 8000 Operational Status

[Table 8-2](#) lists the operational states of the Cisco SCE 8000. The Status LED on the Service Control module reflects the current Cisco SCE 8000 operational status (see [Table 8-3](#) and [Table 8-4](#)). Once boot is complete, the operational status can be displayed using CLI command **show system operation-status**.

**Table 8-2**      *Cisco SCE 8000 Operational States*

| Cisco SCE 8000 Operational Status | Description                                                                                                                                                                                                                                               | Status LED State |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Booting                           | Initial state after reset.                                                                                                                                                                                                                                | Amber            |
| Operational                       | Cisco SCE 8000 becomes operational after completing the following process: <ul style="list-style-type: none"><li>• Boot is completed.</li><li>• Power-on self-tests are completed without failure.</li><li>• Platform configuration is applied.</li></ul> | Steady green     |

**Table 8-2** Cisco SCE 8000 Operational States (continued)

| Cisco SCE 8000 Operational Status | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Status LED State |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Warning                           | <p>Cisco SCE 8000 is fully operational (as above) but one of the following occurred:</p> <ul style="list-style-type: none"> <li>• GBE Management port link is down.</li> <li>• Internal temperature above threshold.</li> <li>• Internal voltage not in expected range.</li> <li>• Fan problem.</li> <li>• Power supply problem.</li> <li>• Insufficient space on the disk.</li> </ul> <p><b>Note</b> If the condition that caused the Cisco SCE 8000 to be in Warning state is resolved (for example, link is up) the Cisco SCE 8000 reverts to Operational state.</p>                                                                | Flashing amber   |
| Failure                           | <p>System is in Failure state after Boot because of one of the following conditions:</p> <ul style="list-style-type: none"> <li>• Power-on test failure.</li> <li>• Three abnormal reboots in less than 30 minutes.</li> <li>• Platform configured to enter Failure mode consequent to failure-induced reboot (this is configurable using CLI command).</li> <li>• Severe system health problem, such as extensive overheating or voltage out of correct operating range.</li> </ul> <p><b>Note</b> Depending on the cause of failure, the management interface and the platform configuration may or may not be active/available.</p> | Red              |

**Table 8-3** Power Supply LEDs

| LED Label           | Color | State  | Function                                                       |
|---------------------|-------|--------|----------------------------------------------------------------|
| INPUT OK            | Green | On     | Input voltage is present and within the required range.        |
| —                   | —     | Off    | Input voltage is not present or not within the required range. |
| OUTPUT FAIL         | Green | On     | Output voltage is not within the required range.               |
| —                   | —     | Off    | Output voltage is in the required range.                       |
| FAN OK              | Green | On     | Power supply internal fan is operational.                      |
| —                   | —     | Off    | Power supply internal fan is not operational.                  |
| Power (front panel) | Green | Steady | Installed power supplies are functioning normally.             |

**Table 8-3**      *Power Supply LEDs (continued)*

| LED Label | Color | State  | Function                                                         |
|-----------|-------|--------|------------------------------------------------------------------|
| —         | Amber | Steady | One of the power supply units is disconnected or malfunctioning. |
| —         | —     | Off    | No power.                                                        |

**Table 8-4**      *Fan Assembly LED*

| LED Label  | Color | State | Function                                                |
|------------|-------|-------|---------------------------------------------------------|
| FAN STATUS | Green | On    | All fans are operational.                               |
|            |       | Off   | One or more of the individual fans are not operational. |

## Problem Solving Using a Subsystems Approach

This section describes the following topics:

- [Identifying Startup Problems, page 8-7](#)
- [Troubleshooting the Power Subsystem, page 8-8](#)
- [Troubleshooting the Firmware Package Installation, page 8-8](#)
- [Troubleshooting the Management Subsystem, page 8-9](#)
- [Troubleshooting the Link Interface Subsystem, page 8-11](#)

### Identifying Startup Problems

Startup problems usually occur because of a source power issue or to a poor cable connection.

When you start up the Cisco SCE 8000 platform for the first time, you should observe the startup sequence described in [Starting the Cisco SCE 8000 Platform, page 7-2](#). This section contains a more detailed description of the normal startup sequence and describes the steps to take if the system does not perform that sequence as expected. LEDs indicate all system states in the startup sequence. By checking the state of the LEDs, you can determine when and where the system failed in the startup sequence. Use the following descriptions to isolate the problem to a subsystem, and then proceed to the appropriate sections to try to resolve the problem.

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

- You should immediately hear the fans operating.
- If the Status LED is flashing orange, indicating a warning state, check the user log:

At the prompt, enter **more user log**.

If any of the following warning messages appear, and the root cause is not obvious and easily solved (such as obstruction of external air-flow), turn the Cisco SCE 8000 platform off and call technical support:

- Voltage problem
- Fan problem
- Abnormal raise in interior temperature

## Troubleshooting the Power Subsystem

In the normally configured Cisco SCE 8000 platform with redundant power supply units, it is unlikely that the device will not start at all. At startup, verify that both power supply units are operational. If the Power LED on the front panel remains unlit when the Cisco SCE 8000 platform is powered up, consult [Table 8-5](#) to help isolate a problem in the power subsystem.


**Note**

If the system powers off because of an environmental shutdown, wait at least 1 minute before manually rebooting the system, otherwise it pauses indefinitely.

**Table 8-5**      *Troubleshooting the Power Subsystem*

| Symptom                                                                                                        | Possible Cause                          | Possible Solution                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power LED on the front panel and LEDs on the power supply unit are not lit, or do not remain lit continuously. | Power cable not fully seated at system. | Turn the power switch to the off position and reseal the power cable in the system.                                                                                                                     |
| —                                                                                                              | Power cable not fully seated at source. | Turn the switch to the off position and reseal the power cable at the power source.                                                                                                                     |
| —                                                                                                              | Power source is faulty.                 | Turn the switch to the off position, connect the power cable to another power source, if available, and turn the switch back on.                                                                        |
| —                                                                                                              | Faulty power cable.                     | Turn the switch to the off position, remove the cable and replace it.                                                                                                                                   |
| —                                                                                                              | Faulty power supply.                    | If the system still fails to come up when the power supply is connected to a different power source with a new power cable, the power supply unit is probably faulty. Contact a service representative. |

## Troubleshooting the Firmware Package Installation

See [Table 8-6](#) to help isolate a problem in the installation of the firmware package.

Problems related to the installation of the firmware package could be any of the following:

- File not found in the expected location.
- Wrong file type.
- Device to which the file is to be extracted is full.

**Table 8-6**      *Troubleshooting the Firmware Package Installation*

| Diagnostic Action                                                                                                   |                |                   |
|---------------------------------------------------------------------------------------------------------------------|----------------|-------------------|
| Enter these CLI commands:                                                                                           |                |                   |
| <ul style="list-style-type: none"> <li>• <b>configure</b></li> <li>• <b>boot system &lt;filename&gt;</b></li> </ul> |                |                   |
| Symptom                                                                                                             | Possible Cause | Possible Solution |

**Table 8-6**      *Troubleshooting the Firmware Package Installation (continued)*

| Diagnostic Action                                                                    |                                                                |                                                                                  |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------|
| The following error message is returned:<br><br>Error-File <filename> does not exist | The package file does not exist in the specified location.     | Verify the package file location and try again.                                  |
| The package file is not the correct one for the Cisco SCE 8000.                      | There is a mismatch between the package file and the platform. | Verify that you have the package file that is appropriate to your platform type. |

## Troubleshooting the Management Subsystem

See [Table 8-7](#) to help isolate a problem in the management subsystem.

Problems in the management subsystem could be any of the following:

- Management link is down. (Mng LINK LED not lit--also Status is WARNING)
- Management link is up (Mng LINK LED lit) but does not answer ping
- Telnet connection cannot be established because of link problems (Mng LINK LED not lit)
- Management link is up (Mng LINK LED lit) but Telnet connection cannot be established
- Telnet connection established, but terminates automatically



### Note

When the management link is down or a Telnet connection cannot be established, you must open a CLI session on a local terminal connected to the CON port. This enables you to solve the problem and then reconnect through the management port

**Table 8-7**      *Troubleshooting the Management Subsystem*

| Symptom                                                                                                                                      | Diagnostic Action                                                                                                                                       | Possible Cause                                                                                                                                               | Possible Solution                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management link down:<br>Mng LINK LED not lit                                                                                                | <ul style="list-style-type: none"> <li>• CLI command <b>show interface GigabitEthernet 1/1</b></li> <li>• ping to management interface fails</li> </ul> | RJ 45 connector is not connected to the platform or to the network.                                                                                          | Reconnect the cable to the GBE port and to network.                                                                                                                                                                        |
| —                                                                                                                                            | —                                                                                                                                                       | Cable is broken.                                                                                                                                             | Check or replace the cable.                                                                                                                                                                                                |
| Management link up:<br><ul style="list-style-type: none"> <li>• Mng LINK LED is lit</li> <li>• ping to management interface fails</li> </ul> | CLI commands <ul style="list-style-type: none"> <li>• <b>show ip route</b></li> <li>• <b>show ip default-gateway</b></li> </ul>                         | One of the following configurations may be wrong: <ul style="list-style-type: none"> <li>• IP address / subnet mask</li> <li>• IP default gateway</li> </ul> | See <a href="#">Initial Setup Parameters, page 5-3</a> .<br>See the “Setting the IP Address and Subnet Mask of the Management Interface” section in the <a href="#">Cisco SCE8000 10GBE Software Configuration Guide</a> . |

**Table 8-7**      **Troubleshooting the Management Subsystem (continued)**

| Symptom                                                                                                                                   | Diagnostic Action                                            | Possible Cause                                                                                                                                                                           | Possible Solution                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —                                                                                                                                         | CLI command:<br><b>show access-lists</b>                     | An ACL that denies entry may be assigned.                                                                                                                                                | See <a href="#">Initial Setup Parameters, page 5-3</a> .<br><br>See the “Configuring Access Control Lists (ACLs)” section in the <a href="#">Cisco SCE8000 10GBE Software Configuration Guide</a> .                                                                  |
| <ul style="list-style-type: none"> <li>Telnet connection cannot be established</li> <li>Mng LINK LED is not lit (link is down)</li> </ul> | CLI command:<br><b>show interface GigabitEthernet 1/1</b>    | Management interface IP address or subnet mask is incorrect.                                                                                                                             | Check or reconfigure management port IP address and subnet mask.                                                                                                                                                                                                     |
| <ul style="list-style-type: none"> <li>Telnet connection cannot be established</li> <li>Mng LINK LED is lit (link is up)</li> </ul>       | CLI command:<br><b>show telnet status</b>                    | Telnet server is disabled.                                                                                                                                                               | Enable Telnet server: <b>service telnetd</b> .                                                                                                                                                                                                                       |
| —                                                                                                                                         | CLI command:<br><b>show telnet sessions</b>                  | Too many Telnet connections (up to five concurrent sessions are supported via Telnet ).                                                                                                  | Close one or more of the open Telnet sessions.                                                                                                                                                                                                                       |
| —                                                                                                                                         | CLI command:<br><b>show ip default-gateway</b>               | Default gateway is incorrect (when the host used as client is not in the same network as the SCE Platform).                                                                              | Check or reconfigure default gateway. See <a href="#">Initial Setup Parameters, page 5-3</a> .<br><br>See the “Setting the IP Address and Subnet Mask of the Management Interface” section in the <a href="#">Cisco SCE8000 10GBE Software Configuration Guide</a> . |
| —                                                                                                                                         | CLI command:<br><b>show ip route &lt;host-ip-address&gt;</b> | Routing tables are incorrectly configured (when the host used as client is not in the same network as the SCE Platform, and there is more than one gateway on the SCE Platform network). | Check or reconfigure routing tables. See <a href="#">Initial Setup Parameters, page 5-3</a> .<br><br>See the “Setting the IP Address and Subnet Mask of the Management Interface” section in the <a href="#">Cisco SCE8000 10GBE Software Configuration Guide</a> .  |

**Table 8-7**      *Troubleshooting the Management Subsystem (continued)*

| Symptom                                     | Diagnostic Action                                                                                                                 | Possible Cause                               | Possible Solution                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —                                           | CLI commands: <ul style="list-style-type: none"> <li>• <b>show access-lists</b></li> <li>• <b>show ip access-class</b></li> </ul> | Host is not a member of a valid access list. | See <a href="#">Initial Setup Parameters, page 5-3</a> .<br><br>See the “Configuring Access Control Lists (ACLs)” section in <a href="#">Cisco SCE8000 10GBE Software Configuration Guide</a> . |
| Telnet connection terminates automatically. | CLI commands: <ul style="list-style-type: none"> <li>• <b>show line</b></li> <li>• <b>show line vty timeout</b></li> </ul>        | Telnet connection may be timing out.         | Reconfigure line timeout.<br><b>timeout &lt;time in seconds&gt;</b>                                                                                                                             |

## Troubleshooting the Link Interface Subsystem

See [Table 8-8](#) to help isolate a problem in the link interface subsystem.

In general, the case where no traffic is coming out of the Cisco SCE 8000 is often caused by link problems or the 10 GBE interface configuration. In some cases, the problem which seems as a transmit problem could be in the Rx (no traffic is being received by the Cisco SCE 8000 or there is actually no traffic on the line, which could be a normal situation).



### Note

In CLI commands for TenGigabitEthernet interfaces, # stands for the number of the SPA module (Cisco SCE 8000-SIP subslot). This can be 0 through 3.

Problems in the link interface subsystem could be any of the following:

- Link is down. (LINK LED not lit and system status is WARNING)
- Peer does not receive traffic from Cisco SCE 8000. (LINK LED is lit and Tx LED is flashing)
- 10 GBE link is up but not receiving from peer. (LINK LED is lit, but Rx LED is not flashing)

**Table 8-8**      *Troubleshooting the Link Interface Subsystem*

| Symptom                                                                                                                           | Diagnostic Action                                                                                                        | Possible Cause                                                        | Possible Solution                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Link is down. (LINK LED not lit)</li> <li>• Output counters not incrementing.</li> </ul> | CLI command: <ul style="list-style-type: none"> <li>• <b>show interface TenGigabitEthernet 3/#/0 counters</b></li> </ul> | Connector is not connected to the platform or to the network.         | Reconnect the fiber to the 10 GBE port and to network.                              |
| —                                                                                                                                 | —                                                                                                                        | Fiber is broken or damaged.                                           | Reconnect or replace the fiber to the 10 GBE port.                                  |
| —                                                                                                                                 | —                                                                                                                        | Connectivity using external optic bypass is incorrect or problematic. | Reconnect or replace the fiber between the 10 GBE port and the optic bypass module. |

**Table 8-8**      *Troubleshooting the Link Interface Subsystem (continued)*

| Symptom                                                                                                                                                                     | Diagnostic Action                                                                                                                                         | Possible Cause                                                        | Possible Solution                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------|
| —                                                                                                                                                                           | Temporarily disconnect optic bypass module and check operation. See the “ <a href="#">Cabling the 10 GBE Line Interface Ports</a> ” section on page 6-11. | Problem with external optic bypass module.                            | Replace the optic bypass module.  |
| <ul style="list-style-type: none"> <li>10 GBE link is up. (LINK LED is continuous green)</li> <li>No traffic received. (10 GBE interface Rx LED is not flashing)</li> </ul> | —                                                                                                                                                         | No traffic is being transmitted to the Cisco SCE 8000 from its peers. | Check traffic connection at peer. |

## Downgrading Cisco SCOS Release 5.1.x

While downgrading Cisco SCOS Release 5.1.x to an earlier version, an error message similar to the following is displayed:

"Could not allocate 7383087 bytes for Control Application XML data partition"

To downgrade Cisco SCOS Release 5.1.x to an earlier version, follow these steps:

- 
- Step 1**      Copy the Cisco SCOS Release 5.1.x PQI file to the /apps/data/scos/app/ folder:
- ```
SCE8000#> copy ftp://ftpdefaultdirectory/5.1.x/<filename.pqi> /apps/data/scos/app/
```
- Step 2**      Uninstall the Cisco SCOS Release 5.1.x PQI file:
- ```
SCE8000(config if)#> pqi uninstall file <filename.pqi>
```
- Step 3**      Copy the running configuration to the startup configuration:
- ```
SCE8000#> copy running-config startup-config
```
- Step 4**      Install the desired version of Cisco SCOS PKG file from the Cisco SCA BB application.
- Step 5**      Install the desired version of Cisco SCOS PQI file from the Cisco SCA BB application.
-

# Troubleshooting with the 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.

This section describes the following topics:

- [The Logging System, page 8-13](#)
- [Generating a File for Technical Support, page 8-14](#)

## The 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:

- [How to Copy the User Log to an External Source, page 8-13](#)
- [How to Copy the User Log to an Internal Location, page 8-13](#)
- [How to View the User Log, page 8-13](#)
- [How to Clear the User Log, page 8-14](#)
- [How to View the User Log Counters, page 8-14](#)
- [How to View the Nonvolatile Counter for the User-file-log, page 8-14](#)

### How to Copy the User Log to an External Source

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

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

### How to Copy the User Log to an Internal Location

You can view the log file by copying it to disk. This command copies both log files to the local SCE platform disk.

From the **SCE>** prompt, enter **logger get user-log file-name** *target-filename* and press **Enter**.

### How to View the 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 [How to Copy the User Log to an External Source, page 8-13](#))

From the **SCE>** prompt, enter **more user-log** and press **Enter**.

## How to Clear the User Log

You can clear the contents of the user log at any time. The user log contains important information about the functioning of the system. It is recommended that a copy be made before the log is cleared.

- 
- |               |                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the <b>SCE#</b> prompt, enter <b>clear logger device user-file-log</b> and press <b>Enter</b> . |
| <b>Step 2</b> | The system asks <i>Are you sure?</i>                                                                 |
| <b>Step 3</b> | Enter <b>y</b> and press <b>Enter</b> .                                                              |
- 

## How to View the User Log Counters

There are two types of log counters:

- User log counters—Count the number of system events logged from the SCE platform last reboot.
- Nonvolatile counters—These are not cleared during boot time.

From the **SCE>** prompt, enter **show logger device user-file-log counters** and press **Enter**.

## How to View the Nonvolatile Counter for the User-file-log

From the **SCE>** prompt, enter **show logger device user-file-log nv-counters** 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 for the use of Cisco technical support staff.

- 
- |               |                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the <b>SCE#</b> prompt, enter <b>logger get support-file filename</b> and press <b>Enter</b> .<br>The support information file is created using the specified filename. This operation may take some time. |
| <b>Step 2</b> | To copy the support file to an external source, from the <b>SCE#</b> prompt, enter <b>copy filename ftp://username:password@ipaddress/path</b> and press <b>Enter</b> .                                         |
-



# Removal and Replacement Procedures

---

Revised: February 18, 2014

## Introduction

This chapter describes how to perform removal and replacement procedures for Cisco SCE 8000 platform field-replaceable units (FRUs).



### Note

Before you install, operate, or service the system, read [Regulatory Compliance and Safety Information for the Cisco SCE8000](#). This guide contains important safety information you should know before working with the system.

---

This chapter contains the following sections:

- [Safety, page 9-2](#)
- [Preventing Electrostatic Discharge Damage, page 9-3](#)
- [Supported Hardware, page 9-3](#)
- [Removing and Replacing the Power Supply, page 9-4](#)
- [Removing and Replacing the Fan Assembly, page 9-13](#)
- [Removing and Replacing Modules, page 9-15](#)
- [Removing and Replacing Shared Port Adapters, page 9-29](#)
- [Removing and Replacing the Optical Bypass Module, page 9-33](#)

# Safety

**Warning**

**Class 1 laser product.**

Statement 1008

**Warning**

**Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.**

Statement 1056

**Warning**

**This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Statement 1024

**Warning**

**Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.**

Statement 1034

**Caution**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

**Note**

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

# Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Port adapters and processing modules consist of printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Following are guidelines for preventing ESD damage:

- Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to an unfinished chassis surface.
- When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.
- When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.
- Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.
- Place a removed component board-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Never attempt to remove the printed circuit board from the metal carrier.

**Caution**

For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohm (Mohm).

## Supported Hardware

The Cisco SCE 8000 platform supports the following hardware:

- One Service Control Module (Cisco SCE 8000-SCM-E), with an optional redundant Service Control Module (FRU).
- One SPA jacket module (Cisco SCE 8000-SIP), with either two or four SPA 10 GBE interface modules (all FRU).
- Up to two optical bypass modules installed in the bottom slot of the chassis.
- Hot-swappable fan assembly, redundant AC-input or DC-input power supplies.

# Removing and Replacing the Power Supply

This section describes how to remove and install power supplies for the Cisco SCE 8000.



**Note**

In systems with redundant power supplies, you can replace the faulty supply while the system is operating.

This section contains the following information:

- [Required Tools, page 9-4](#)
- [Removing an AC-Input Power Supply, page 9-4](#)
- [Installing an AC-Input Power Supply, page 9-6](#)
- [Removing a DC-Input Power Supply, page 9-6](#)
- [Installing a DC-Input Power Supply, page 9-8](#)

## Required Tools

A flat-blade or number 2 Phillips-head screwdriver is required to perform these procedures. Additionally, a wire cutter or scissors may be necessary for cutting cable tie-wraps.

## Removing an AC-Input Power Supply



**Warning**

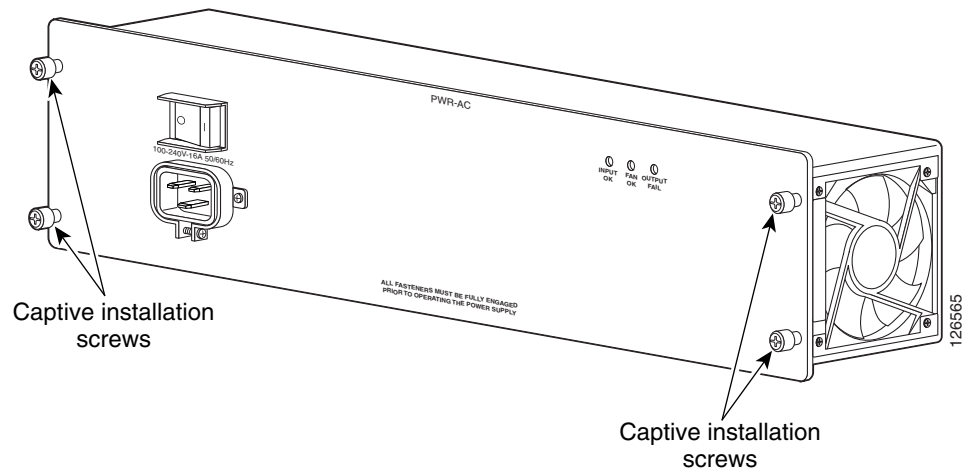
**Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.**

Statement 1034

- Step 1** Turn the power switch to the Off (0) position on the power supply you are removing.
- Step 2** Disconnect the power cord from the power source. Do not touch the metal prongs on the power cord when it is still connected to the power supply.
- Step 3** Remove the power cord from the power connection on the power supply module. Do not touch the metal prongs embedded in the power supply.

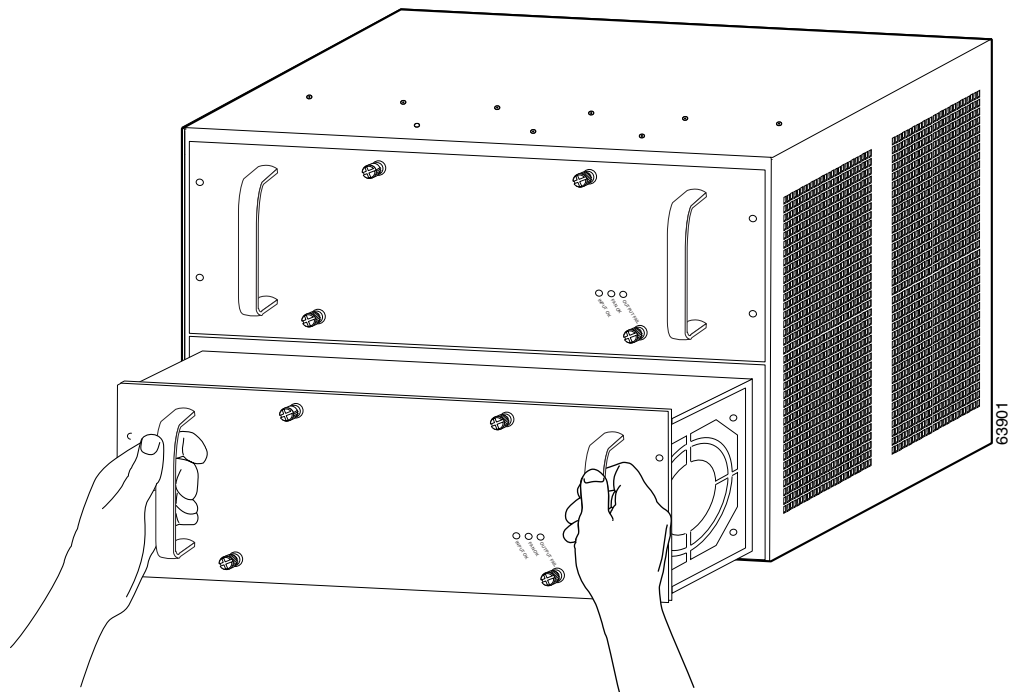
- Step 4** Loosen the captive installation screws on the power supply ([Figure 9-1](#)).

**Figure 9-1** AC Power Supply Captive Installation Screws



- Step 5** Grasp both power supply handles, as shown in [Figure 9-2](#), and slide the power supply completely out of the chassis.

**Figure 9-2** Handling the AC Power Supply



## Installing an AC-Input Power Supply

**Note**

This product requires short-circuit (over current) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

- 
- Step 1** Ensure that the system (earth) ground connection has been made. For ground connection instructions, see [Connecting the System Ground, page 4-20](#)
- Step 2** Verify that the power switch is in the Off (0) position.
- Step 3** Grasp both power supply handles, as shown in [Figure 9-2](#). Slide the power supply into the power supply bay. Make sure that the power supply is fully seated in the bay.
- Step 4** Securely tighten the power supply captive installation screws. (See [Figure 9-1](#).)

**Warning**

**Power supply captive installation screws must be tight to ensure protective grounding continuity.**  
Statement 289

- 
- Step 5** Plug the power cord into the power supply.
- Step 6** Connect the other end of the power cord to an AC-input power source.

**Caution**

In a system with dual power supplies, connect each power supply to a separate input source. In case of a power source failure, the second source will most likely still be available.

- 
- Step 7** Turn the switch on the power supply to the On (I) position.
- Step 8** Verify power supply operation by checking the power supply LEDs.

The power supply LEDs should be in the following states:

- INPUT OK LED is green
- FAN OK LED is green
- OUTPUT FAIL LED is not lit

If the LEDs indicate a power problem, see [Identifying Startup Problems, page 8-7](#) for troubleshooting information.

## Removing a DC-Input Power Supply

**Warning**

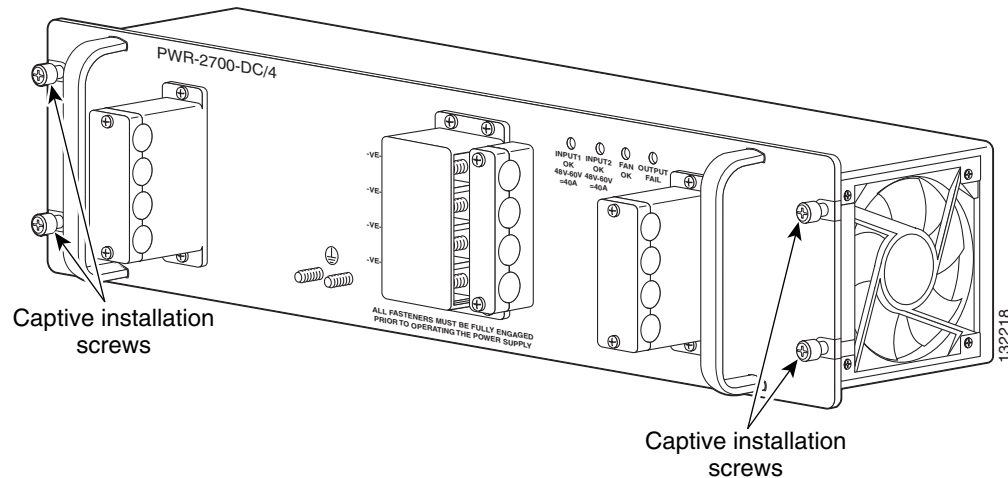
**Before performing any of the following procedures, ensure that power is removed from the DC circuit.**  
Statement 1033

**Warning**

**Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.**  
Statement 166

- Step 1** Verify that power is off to the DC circuit connected to the DC-input power supply you are removing.
- Step 2** Remove the four screws securing the terminal block cover, and slide the cover off the terminal block.

**Figure 9-3** DC-Input Front Panel for 2700-W DC-Input Power Supply



- Step 3** Remove the two screws securing each of the cable holder covers, and remove the cable holder covers off the cable holders.
- Step 4** Disconnect the DC-input wires from the terminal block.
- Always disconnect the DC-input wires in this order:
- Positive (+)
  - Negative (—)
  - Ground



**Warning**

**When installing the unit, the ground connection must always be made first and disconnected last.**  
Statement 42

- Step 5** Remove the two tie-wraps from the ground cable. If there is a long cable tie securing the cable holders, remove that as well.
- Step 6** Loosen the captive installation screws on the power supply. (See [Figure 9-3](#).)

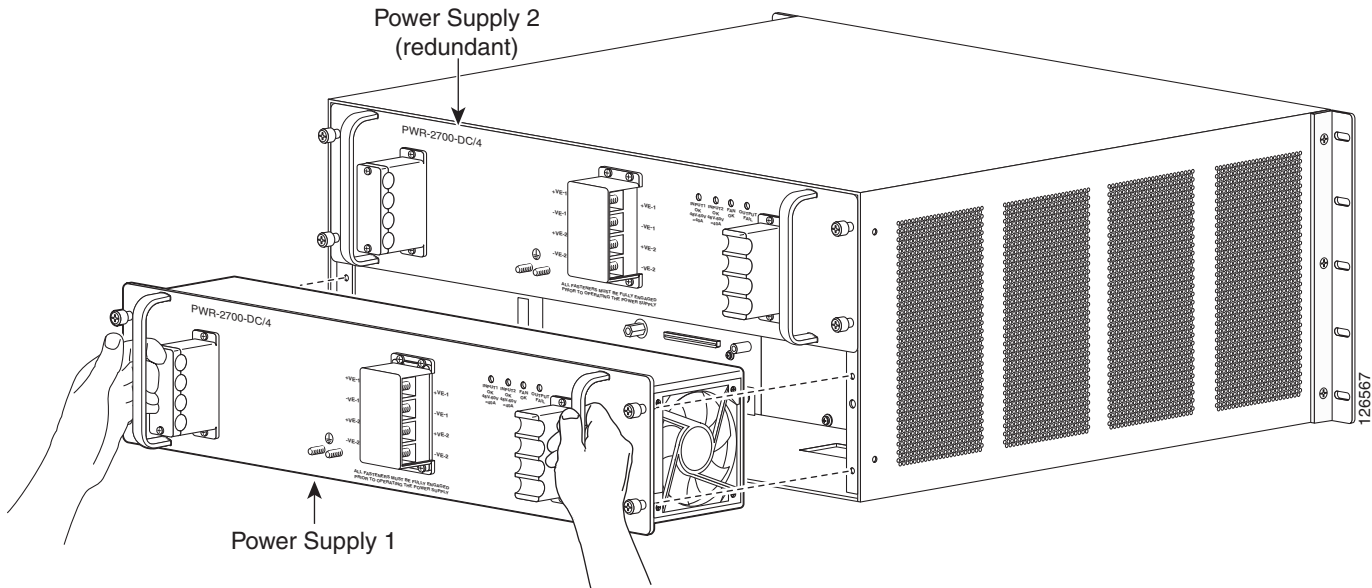


**Caution**

Use both hands to install and remove power supplies. Each PWR-2700-DC DC/4-input power supply weighs 19.8 pounds (9.0 kg).

- Step 7** Grasp both power supply handles, as shown in [Figure 9-4](#), and slide the power supply completely out of the chassis.

**Figure 9-4** Handling a DC-Input Power Supply



## Installing a DC-Input Power Supply

This section covers the DC-input power supply installation procedure for the Cisco SCE 8000 chassis.



### Note

The DC return is to remain isolated from the system frame and chassis (DC-I).



### Warning

**Before performing any of the following procedures, ensure that power is removed from the DC circuit.**  
Statement 1033

### Step 1

Power supply ground is required. Install the PWR-2700-DC/4 power supply ground as described in this procedure.



### Note

The system ground connection with the PWR-2700-DC/4 power supply in a Cisco SCE 8000 is provided by the PWR-2700-DC/4 power supply ground. Additionally, you can connect a system (earth) ground.



### Caution

You must always connect the PWR-2700-DC/4 power supply ground.

**Caution**

You must connect the PWR-2700-DC/4 power supply ground for both power supplies.

**Note**

If you intend to use an additional system (earth ground), ensure that the system ground connection has been made. For ground connection installation instructions, see [Connecting the System Ground](#), page 4-20.

**Step 2**

Remove the plastic bag attached to the front panel and put aside. This bag contains two plastic terminal block barriers, two cable ties, and two cable holder covers.

**Step 3**

Verify that power is off to the DC circuit connected to the power supply you are installing. Grasp both power supply handles, as shown in [Figure 9-4](#). Slide the power supply into the power supply bay. Make sure that the power supply is fully seated in the bay.

**Step 4**

Tighten the power supply captive installation screws.

**Warning**

**Power supply captive installation screws must be tight to ensure protective grounding continuity.**

Statement 289

**Note**

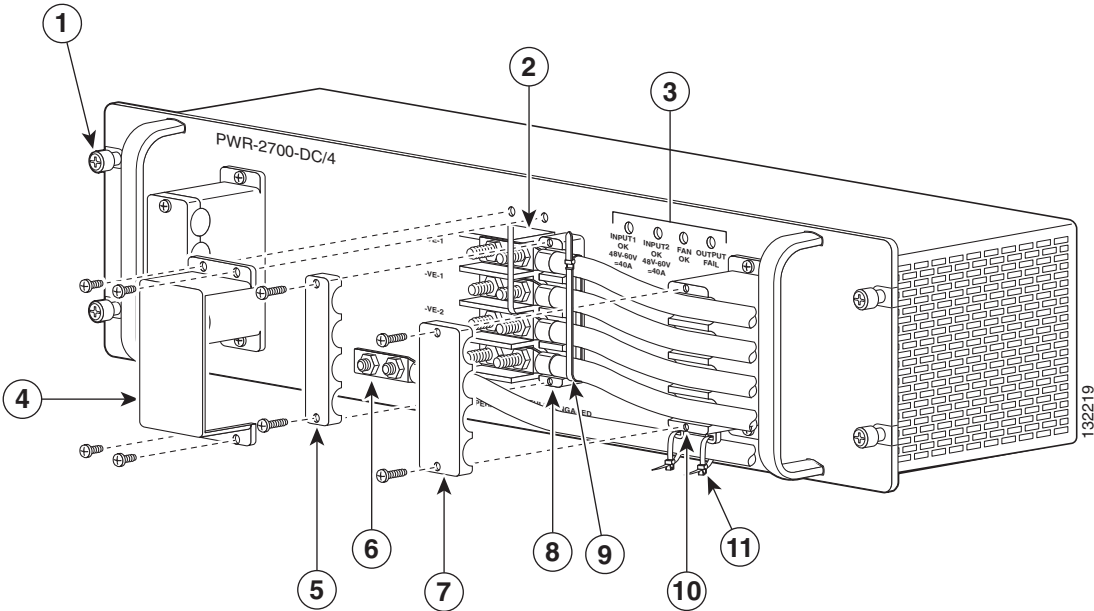
Because the power requirement of the Cisco SCE 8000 does not exceed 1350 W, it is not necessary to connect two pairs of input wires to each power supply. Should it be desired to connect two pairs of input wires, both pairs of input wires for one 2700W DC-input power supply must come from the same battery system (A feed); and both pairs of input wires for the other power supply must come from another battery system (B feed).

**Note**

For multiple DC input power supplies, each DC input must be protected by a dedicated circuit breaker or fuse. The circuit breaker or fuse should be sized according to the power supply input rating and local or national electrical code requirements.

- Step 5** Remove the four screws securing the terminal block cover, and slide the cover off of the terminal block. (See [Figure 9-5](#).)

**Figure 9-5** DC-Input Front Panel for 2700-W DC-Input Power Supply



|   |                                     |    |                    |
|---|-------------------------------------|----|--------------------|
| 1 | Captive installation screw          | 7  | Cable holder cover |
| 2 | DC power cable terminal block       | 8  | Cable holder       |
| 3 | Status LEDs                         | 9  | Tie-wrap           |
| 4 | DC power cable terminal block cover | 10 | Cable holder       |
| 5 | Cable holder cover                  | 11 | Tie-wrap           |
| 6 | Ground                              |    |                    |

- Step 6** Attach the appropriate lugs to the DC-input wires and ground wire. The wires should be sized according to local and national installation requirements. Use only copper wire. The maximum width of a lug is 0.600 inch (15.2 mm).



**Note**

Use fine-stranded copper conductors rated for 90°C (194°F) for North American installations.



**Note**

The power supply terminal block lug opening width is 0.62 inch (15.8 mm). The terminal posts are centered 0.625 inches (15.88 mm) apart and are 1/4-20 threaded. We recommend that you use an appropriately sized industry standard 2-hole, standard barrel compression lug. The power supply ground studs, located below the terminal block, are also threaded 1/4-20 and require two 1/4-inch split-ring washers and two 1/4-20 hex nuts.

**Step 7** Connect the DC-input wires to the 2700 W power supply terminal block. Depending on which side you are connecting the DC-input wires, be sure that the DC-input wires rest in the appropriate cable holder. [Figure 9-6](#) shows DC-input wires coming in from the left side.

Connect the DC-input wires to the 2700 W power supply terminal block in this order:

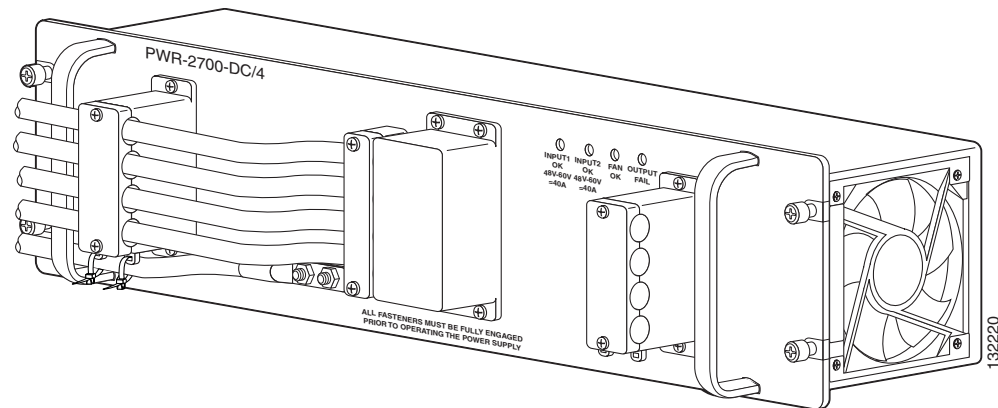
- Ground
- Negative (—)
- Positive (+)



**Note**

When you tighten the terminal nuts, make sure they are snug. Do not over tighten them. The recommended torque strength is 20 inch-pounds. Over tightening the terminal nuts can break the terminal block (Maximum torque: 36 inch-pounds).

**Figure 9-6 DC-Input Wires on Left Side**



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

**Step 8** Secure the ground cable to the cable holder with the two cable-ties.

**Step 9** Retrieve the cable holder covers from the plastic bag and attach them to the front panel at the locations shown in [Figure 9-3](#).



**Note**

If the cable holder illustrated as number 5 and 8 in [Figure 9-3](#) does not hold the DC input cables snugly, use a long cable tie to secure the cable holders as illustrated in number 9.

**Step 10** Secure the terminal block cover using four screws and the terminal block barriers with two screws each.

- Step 11** Turn on the DC inputs and verify power supply operation by checking the power supply front panel LEDs.

The power supply rear panel LEDs should be in the following states:

- INPUT OK LED is green
- FAN OK LED is green
- OUTPUT FAIL LED is not lit

If the LEDs indicate a power problem, see [Identifying Startup Problems, page 8-7](#)

---

# Removing and Replacing the Fan Assembly

This section describes how to remove and replace fan assemblies for the Cisco SCE 8000 chassis:

- [Required Tools, page 9-13](#)
- [Removing the Fan Assembly, page 9-13](#)
- [Installing the Fan Assembly, page 9-14](#)

## Required Tools

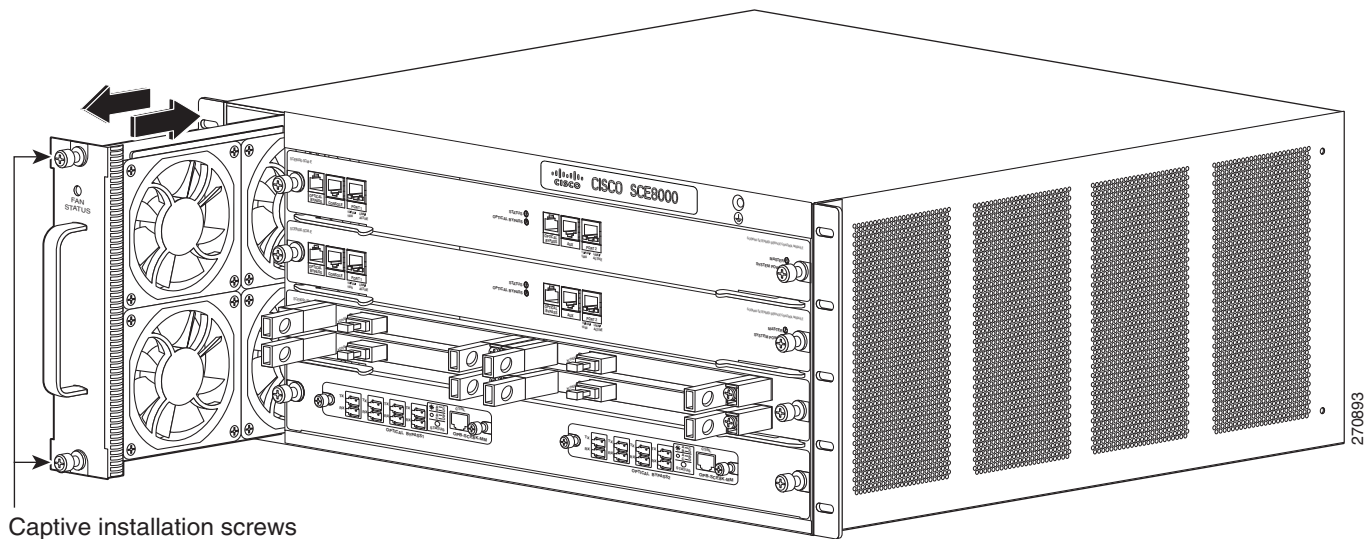
A flat-blade or number 2 Phillips-head screwdriver is required to perform this procedure.

## Removing the Fan Assembly

The fan assembly is designed to be removed and replaced while the system is operating without presenting an electrical hazard or damage to the system.

- 
- Step 1** Loosen the two captive installation screws by turning them counterclockwise.

**Figure 9-7** Fan Assembly



When removing the fan tray, keep your hands and fingers away from the spinning fan blades. Let the fan blades completely stop before you remove the fan tray.

- Step 2** Grasp the fan assembly with both hands and pull it outward; rock it gently if necessary to unseat the power connector from the backplane. (See [Figure 9-7](#).)
- Step 3** Pull the fan assembly clear of the chassis, and put it in a safe place.
-

## Installing the Fan Assembly

- 
- Step 1** Hold the fan assembly with the fans facing to the right and the FAN STATUS LED at the bottom. (See [Figure 9-7](#).)
- Step 2** Place the fan assembly into the front chassis cavity so that it rests on the chassis, and then lift the fan assembly up slightly, aligning the top and bottom chassis guides.
- Step 3** Push the fan assembly into the chassis until the power connector seats in the backplane and the captive installation screws make contact with the chassis.
- Step 4** Tighten the captive installation screws.
- Step 5** Verify that fans are operational:
- Listen for the fans; you should immediately hear them operating. If you do not hear them, ensure that the fan assembly is inserted completely in the chassis and the faceplate is flush with the switch back panel.
  - Verify that the FAN STATUS LED is green. If the LED is red, one or more fans is faulty.
-

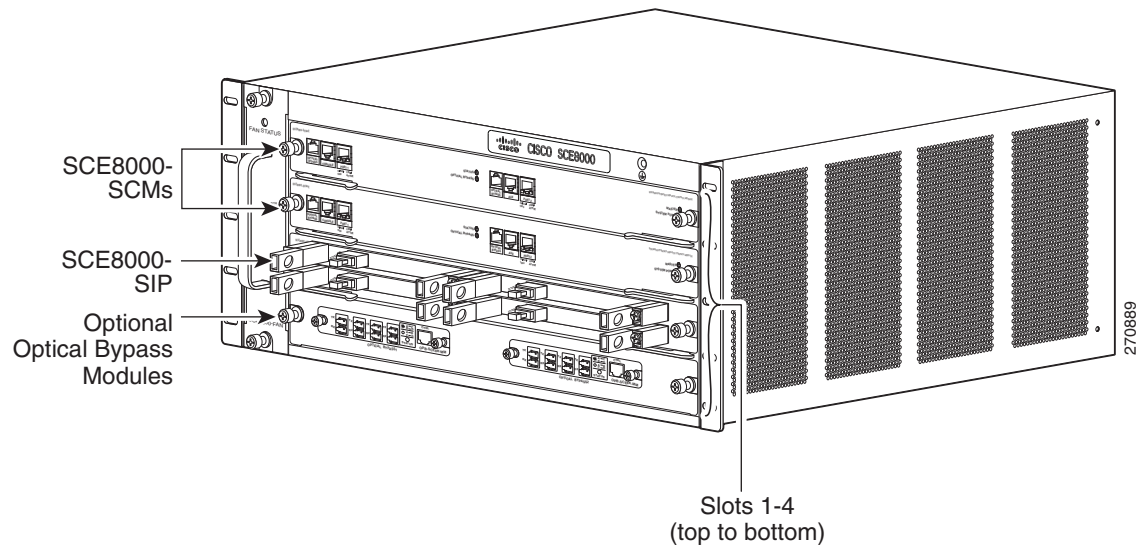
# Removing and Replacing Modules

The Cisco SCE 8000 platform supports two types of modules:

- Service Control Module (Cisco SCE 8000-SCM-E)
- SPA Interface Processor (Cisco SCE 8000-SIP)

Figure 9-8 shows the position of these modules in the Cisco SCE 8000 chassis.

**Figure 9-8** Slot Numbers on Cisco SCE 8000 Chassis



## Required Tools

These tools are required to remove or install modules in the Cisco SCE 8000 chassis:

- 3/16-inch flat-blade screwdriver
- Number 2 Phillips-head screwdriver
- Wrist strap or other grounding device
- Antistatic container that the module was shipped in

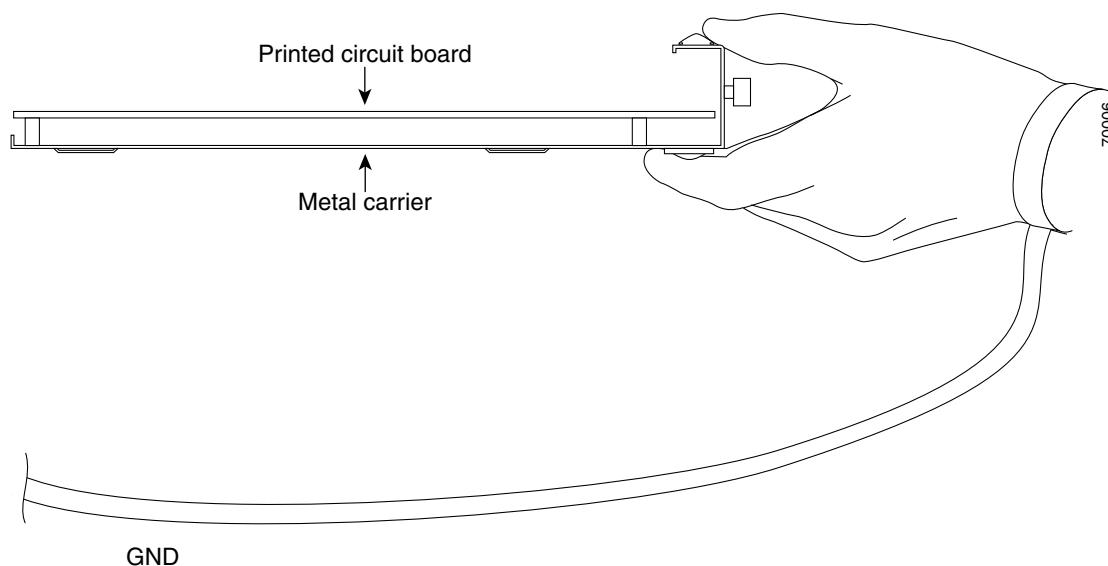
## Handling SIPs

Each SIP circuit board is mounted to a metal carrier and is sensitive to electrostatic discharge (ESD) damage.

Always handle the SIP by the carrier edges and handle; never touch the SIP components or connector pins. (See [Figure 9-9](#).)

When a slot is not in use, a blank filler plate must be installed in the empty slot to allow the SCE platform to conform to electromagnetic interference (EMI) emissions requirements and to allow proper airflow across the installed modules. If you plan to install a SIP in a slot that is not in use, you must first remove the blank filler plate.

**Figure 9-9** Handling a SIP



## Installing a Module

Perform the following procedure to install a module:

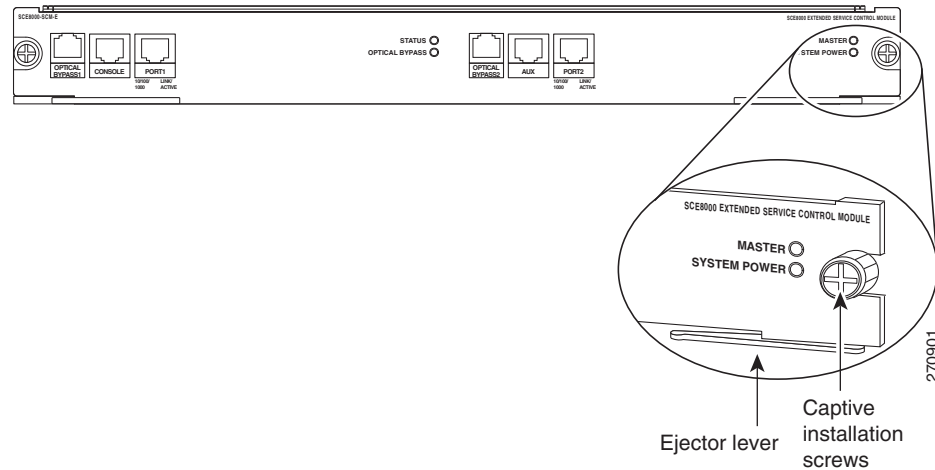
- 
- Step 1** Choose a slot for the module.
- Modules must be installed in the proper slots, as follows:
- A single Cisco SCE 8000-SCM-E module must be installed in slot 1.
  - If a second Cisco SCE 8000-SCM-E module is used, it must be installed in slot 2.
  - The Cisco SCE 8000-SIP module must be installed in slot 3.
- Step 2** At the **SCE#** prompt, enter **reload shutdown** and press **Enter** to power down the Cisco SCE 8000 platform before installing or removing any module.
- Step 3** Make sure that there is enough clearance to accommodate any interface equipment that you connect directly to the module ports.
- Step 4** Verify that the captive installation screws are tightened on all modules already installed in the chassis. This ensures that the EMI gaskets on all modules are fully compressed to maximize the opening space for the new or replacement module.

**Note**

If the captive installation screws are loose, the EMI gaskets on the installed modules will push adjacent modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

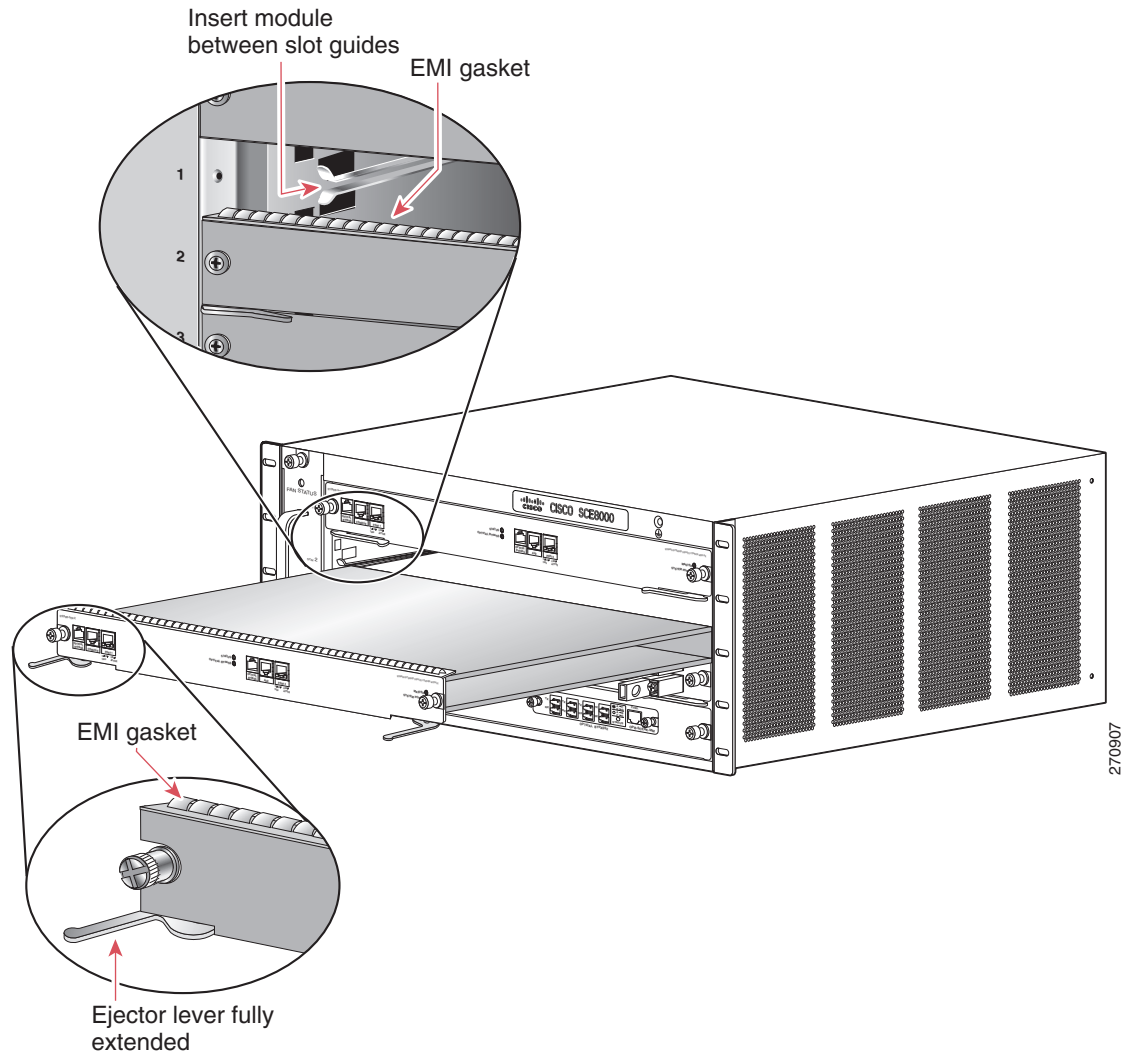
- Step 5** Remove the module filler plate by removing the two Phillips pan-head screws from the filler plate. To remove a module, follow the procedure in the [“Removing a Module”](#) section on page 9-20.
- Step 6** Fully open both ejector levers on the new module. (See [Figure 9-10](#).)

**Figure 9-10** *Ejector Levers and Captive Installation Screws*



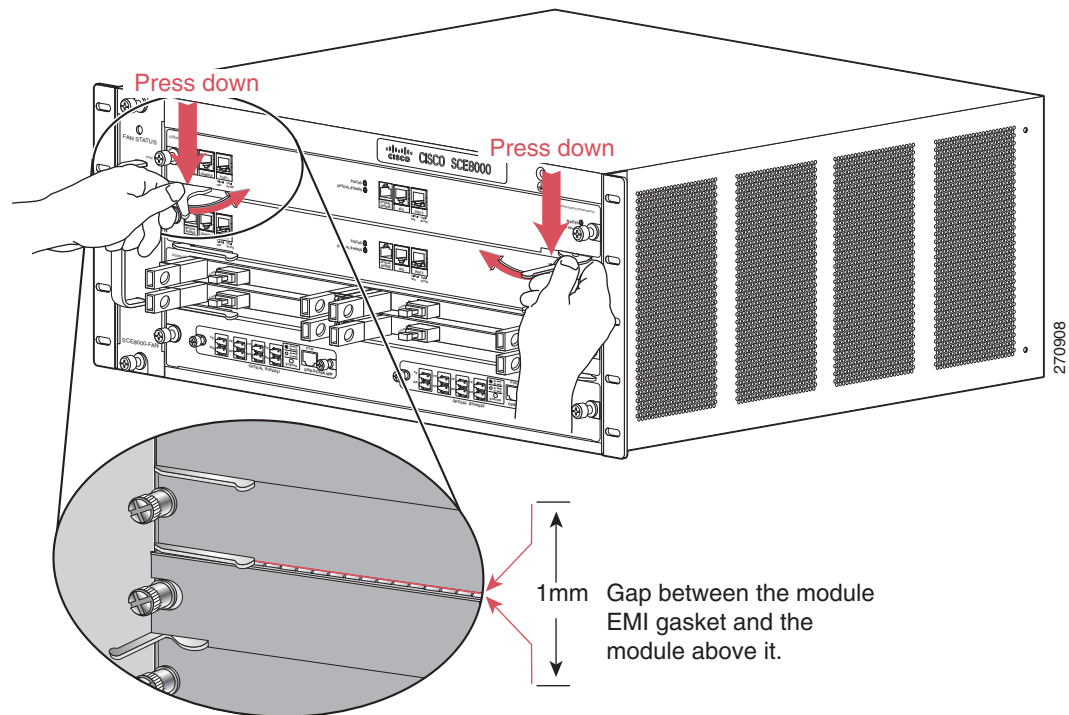
- Step 7** Position the module in the slot. (See [Figure 9-11](#).) Make sure that you align the sides of the module carrier with the slot guides on each side of the slot.

**Figure 9-11** Positioning the Module in the Slot



- Step 8** Carefully slide the module into the slot until the EMI gasket along the top edge of the module makes contact with the module in the slot above it and both ejector levers have closed to approximately 45 degrees in relation to the module faceplate. (See [Figure 9-12](#).)

**Figure 9-12** Clearing the EMI Gasket



- Step 9** Using the thumb and forefinger of each hand, grasp the two ejector levers and press down to create a small (0.040 inch [1 mm]) gap between the module EMI gasket and the module above it. (See [Figure 9-12](#).)



**Caution**

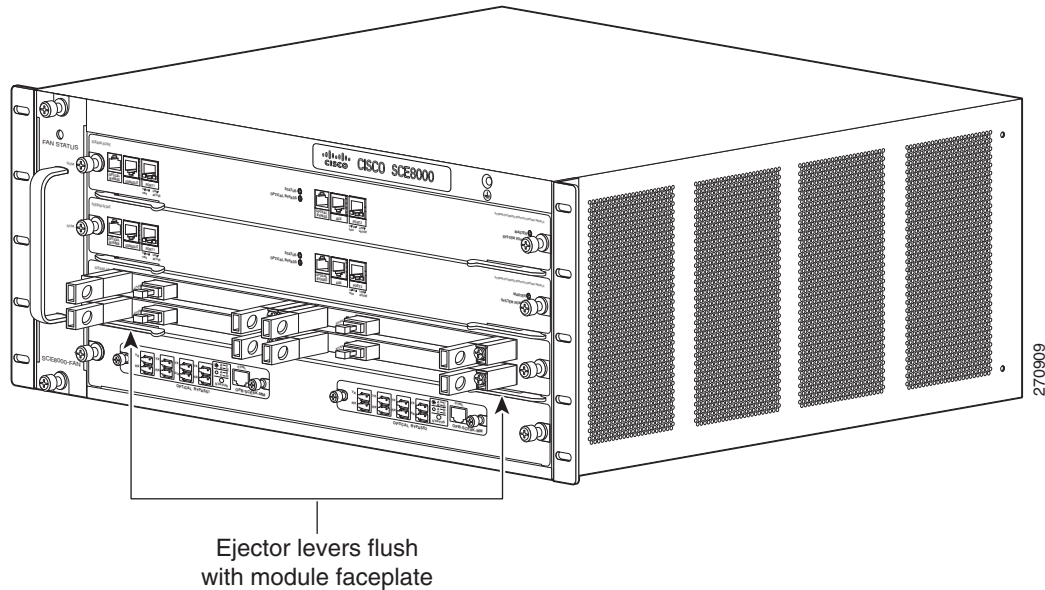
Do not press down too forcefully on the ejector levers. They can bend and be damaged.

- Step 10** While pressing down, simultaneously close the left and right ejector levers to fully seat the module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See [Figure 9-13](#))

**Note**

Failure to fully seat the module in the backplane connector can result in incorrect operation or error messages.

**Figure 9-13** Ejector Lever Closure



- Step 11** Tighten the two captive installation screws on the module.

**Note**

Make sure the ejector levers are fully closed before tightening the captive installation screws.

## Removing a Module

Before you remove a Cisco SCE 8000-SCM, you should first save the current configuration, if the current configuration should be preserved and duplicated on the new Cisco SCE 8000-SCM-E. (Use the **copy running-config startup-config** command.) This step saves time when bringing the module back online. You can recover the configuration by downloading it from the server to the nonvolatile memory of the Cisco SCE 8000-SCM-E.

**Tip**

When you install a new Cisco SCE 8000-SCM-E, check the factory default configuration. You might need to reconfigure the system to your requirements. You can reconfigure the Cisco SCE 8000-SCM-E manually, or if you previously uploaded the original configuration to a server, you can download it to the new Cisco SCE 8000-SCM-E.

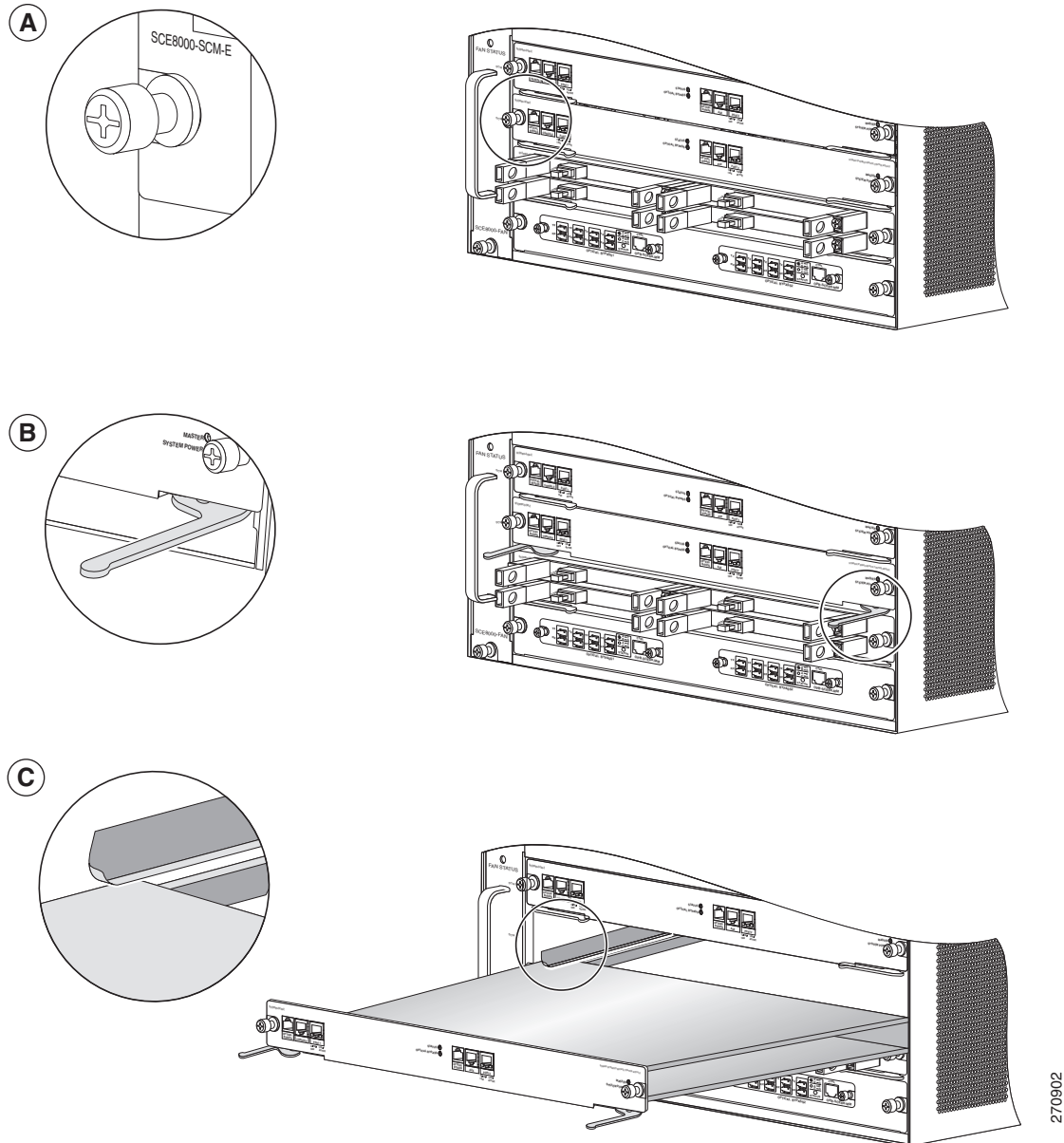
- 
- Step 1** At the **SCE#** prompt, enter **reload shutdown** and press **Enter** to power down the Cisco SCE 8000 platform before installing or removing any module.
- Step 2** Verify that the captive installation screws on all of the modules in the chassis are tight. This step assures that the space created by the removed module is maintained.
-  **Note** If the captive installation screws are loose, the EMI gaskets on the installed modules will push the modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.
- 
- Step 3** Disconnect all cables.
- Step 4** Loosen the two captive screws on the module.
- Step 5** Place your thumbs on the left and right ejector levers and simultaneously rotate the levers outward to unseat the module from the backplane connector.
- Step 6** Grasp the front edge of the module and slide the module part of the way out of the slot.
- Step 7** Pull the module out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.
- Step 8** Place the module on antistatic foam, or immediately reinstall it in another slot.
- Step 9** If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis.
-

## Inserting and Removing a Module: Detail

See [Figure 9-14](#) for detailed views of:

- Captive screw (A)
- Ejector lever (B)
- Slot guide (C)

**Figure 9-14**     *Module Installation and Removal*



270902

## Verifying the Installation

Use the **show version** command to verify that the system software and firmware are installed properly.

**Step 1** From the **SCE>** prompt, enter **show version** and press **Enter**.

This example shows the output of the **show version** command:

```
System version: Version 3.1.6S Build 279
Build time: Jun 10 2008, 19:27:47 (Change-list 335658)
Software version is: Version 3.1.6S Build 279
Hardware information is:
-----
Firmware
-----
kernel : [kernel] 1.0.0/5 (inactive: [kernel] 1.0.0/5)
u-boot : [uboot] 1.0.0/6 (field: [uboot] 0.8.1/13)
select : [ubs-cf1] 1.0.0/5 (secondary: [ubs-cf1] 1.0.0/5)
-----
Slot 1: SCM-8000
-----
serial-num : CAT1202G07D
part-num : 73-10598-01 38
cpld : 0x8162
vtpld : 0xc001
summit-0 : 0x10008
summit-1 : 0x10008
dpt/tx : 0x4837
cls/ff : 0x2047
cls flow cap: 33554432

-----
TVR
-----
#cpus : 1
cpu SVR : 0x80900120
cpu PVR : 0x80040202
cpu freq : 1000MHz
cpu (eeprom): 2.1, 1000MHz
cpld : 0xa1b7
cpld-ufm : 0xa803
summit : 0x10007
cf : Model=SMART CF, FwRev=0x20060811, Size=4062240KB
-----
CFC-0
-----
board type : P2
#cpus : 3
cpu-0 SVR : 0x80900121
cpu-0 PVR : 0x80040202
cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb20e
cpld-1 : 0xb20e
cpld-2 : 0xb20e
cpld-0-ufm : 0xb803
```

```

cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1044
-----
CFC-1
-----
board type : P2
#cpus : 3
cpu-0 SVR : 0x80900121
cpu-0 PVR : 0x80040202
cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb20e
cpld-1 : 0xb20e
cpld-2 : 0xb20e
cpld-0-ufm : 0xb803
cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1044
-----
Slot 3: SIP-8000
-----
serial-num : CAT1204G01H
part-num : 73-10947-01
cpld : 0x9162
summit-0 : 0x10006
summit-1 : 0x10006
dpt-0 : 0x3033
dpt-1 : 0x3033
spa[0] : SPA-1X10GE-L-V2
spa[1] : SPA-1XTENGE-XFP
spa[2] : SPA-1X10GE-L-V2
spa[3] : SPA-1XTENGE-XFP
-----
SCE8000 Chassis
-----
product-num : CISCO7604
serial-num : FOX10420BKZ
part-num : 73-9789-02
part-rev : A0
vid : V01

```

Part number: 73-10598-01 38  
Revision:  
Software revision:  
LineCard S/N : CAT1202G07D  
Power Supply type: AC  
SML Application information is:  
No application is configured.  
Logger status: Enabled

Platform: SCE8000 - 4x10GBE  
Management agent interface version: SCE Agent 3.1.6 Build 134  
Software package file: ftp://ftpserver/simba.pkg  
SCE8000 uptime is 9 minutes, 54 seconds

After you verify installation of a Cisco SCE 8000 module and check connectivity, you must configure the module. For complete information on configuring the Cisco SCE 8000 platform, see the [Cisco SCE8000 10GBE Software Configuration Guide](#). For information on all Cisco SCE 8000 platform commands, see the [Cisco SCE8000 CLI Command Reference](#) document.

---

# Installing and Replacing the Cisco SCE 8000-SCM Module

In general, the Cisco SCE 8000 chassis is shipped fully configured. However, in some cases a second Cisco SCE 8000-SCM module may be installed or removed. In such cases, make sure to see the following guidelines:

**Note**

Dual Cisco SCE 8000-SCM modules are supported only on systems running Cisco SCOS Release 3.6.0 or later.

- When two Cisco SCE 8000-SCM modules are installed, the module in slot 1 functions as the master, and the one in slot 2 serves as the slave.
- If there is only one Cisco SCE 8000-SCM module installed, it must be installed in slot 1.

If the Cisco SCE 8000-SCM module in slot 2 is to become the master Cisco SCE 8000-SCM module, the Cisco SCE 8000-SCM in slot 1 must be removed and the module on slot 2 must be moved and reinstalled in slot 1.

No user data is saved on the slave Cisco SCE 8000-SCM, which means that no previous configurations of any sort, including PQI and SLI, are carried with this Cisco SCE 8000-SCM.

- The system must be turned off before replacing either Cisco SCE 8000-SCM module.
- When a new package or application is installed, it is automatically installed on both Cisco SCE 8000-SCM modules. No special software installation procedures are required.
- If the second Cisco SCE 8000-SCM module (slave) is running a version or build different from the one running on the master Cisco SCE 8000-SCM module, then, and if both versions are 3.6.0 or later, the system syncs the package on the second module to the one on the master module at the time of the next boot.

**Note**

This situation can occur only when a master Cisco SCE 8000-SCM module is removed and then inserted as a slave Cisco SCE 8000-SCM module, either in the same Cisco SCE 8000 chassis or a different one.

## Installation and Upgrade Procedures for Dual Cisco SCE 8000-SCM Modules

### First-Time Installation

- 
- |               |                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Make sure that Cisco SCOS Release 3.6.0 or later has been installed on both Cisco SCE 8000-SCM modules.                                |
| <b>Step 2</b> | At the <b>SCE#</b> prompt, enter <b>reload shutdown</b> and press <b>Enter</b> , and then turn off the Cisco SCE 8000 10 GBE platform. |
| <b>Step 3</b> | Insert one Cisco SCE 8000-SCM module in slot 1 and the second in slot 2.                                                               |
| <b>Step 4</b> | Turn on the Cisco SCE 8000 power.                                                                                                      |
-

## Installing a Cisco SCE 8000-SCM Module that was a Slave Module as a Master Module

When redeploying a Cisco SCE 8000-SCM module that had been installed as a slave module, and installing it as a master Cisco SCE 8000-SCM module, it will run the latest package that had been installed on it as a slave module.

No user data is saved on the slave Cisco SCE 8000-SCM, which means no previous configurations, including PQI and SLI, are carried with this Cisco SCE 8000-SCM.

## Removing a Cisco SCE 8000-SCM Module

OIR is not supported. Always use the **reload shutdown** command and then turn off the power before removing any Cisco SCE 8000-SCM module. Failure to turn off the power before removing a Cisco SCE 8000-SCM module results in a system reset, as follows:

### Removing the Master Cisco SCE 8000-SCM Module

Removing the Cisco SCE 8000-SCM module in slot 1 from a running system results in immediate reset. The system cannot recover from reset. To recover from reset, turn off the system, insert a Cisco SCE 8000-SCM module in slot 1, and then turn on the system.

### Removing the Slave Cisco SCE 8000-SCM Module

Removing the Cisco SCE 8000-SCM module in slot 2 from a running system results in a software watchdog timeout and a reset. After a reboot, the system functions like any other system with a single Cisco SCE 8000-SCM module.

## Adding a Cisco SCE 8000-SCM Module in Slot 2

Turn off the power before installing a Cisco SCE 8000-SCM module in slot 2. If you add a second Cisco SCE 8000-SCM module while the system is running with a single Cisco SCE 8000-SCM module, the new module is held at reset until next system boot.



### Note

---

Always use the **reload shutdown** command before turning off the Cisco SCE 8000.

---

Following the reboot, if the software version installed on the new Cisco SCE 8000-SCM module does not match the version installed in the Cisco SCE 8000-SCM module found in slot 1, the system automatically syncs the software on the new module, and reboots again. Because no external ports are open at this stage, this process appears as a normal boot sequence that takes longer than usual.

## Downgrading Dual Cisco SCE 8000-SCM Modules

Downgrading the system to a version earlier than 3.6.0 is not permitted on a system with dual Cisco SCE 8000-SCM modules.

Perform the following steps to downgrade:

- 
- |               |                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | At the <b>SCE#</b> prompt, enter <b>reload shutdown</b> and press <b>Enter</b> and then turn off the Cisco SCE 8000 10 GBE platform. |
| <b>Step 2</b> | Remove the Cisco SCE 8000-SCM module in slot 2.                                                                                      |
| <b>Step 3</b> | Turn on the Cisco SCE 8000 power.                                                                                                    |
| <b>Step 4</b> | Perform the downgrade.                                                                                                               |
- 

## Upgrading Dual Cisco SCE 8000-SCM Modules

Use the Upgrade wizard in the Cisco SCA BB console to upgrade a system with dual Cisco SCE 8000-SCM modules the same as for a single Cisco SCE 8000-SCM module system. See the [How to Upgrade the SCE Using the SCE Software Upgrade Wizard](#) section in the *Cisco Service Control Application for Broadband User Guide*.

# Removing and Replacing Shared Port Adapters

This section provides information about the following tasks:

When removing and replacing the 1-port 10 GBE SPAs, follow these guidelines:

- SPAs must be installed in pairs. The Cisco SCE 8000 supports the following SPA configurations:
  - Two SPAs inserted in subslots 0 and 1
  - Four SPAs
- If only two SPAs are installed, sublots 2 and 3 must be covered by blank filler panels.
- [Required Tools and Equipment, page 9-29](#)
- [Laser/LED Safety, page 9-29](#)
- [Handling SPAs, page 9-30](#)
- [SPA Installation and Removal, page 9-31](#)
- [Installing a SPA in a SIP, page 9-32](#)
- [Removing a SPA from a SIP, page 9-32](#)

## Required Tools and Equipment

You need the following tools and parts to install SPAs. If you need additional equipment, contact a service representative for ordering information.

- Shared port adapter (SPA)
- Number 1 Phillips-head and a 3/16-inch flat-blade screwdriver
- Number 2 Phillips-head screwdriver
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap supplied with the SPA
- Antistatic container in which the SPA was shipped

## Laser/LED Safety

An optical single-mode transmitter uses a small laser to transmit the light signal to the network ring. Keep the transmit port covered whenever a cable is not connected to it. Although multi-mode transceivers typically use LEDs for transmission, it is good practice to keep open ports covered and to avoid staring into open ports or apertures. The transceivers aperture port contains a laser warning label, as shown in [Figure 9-15](#). These warnings apply to SPAs and XFP modules that transmit signals via an optical carrier signal.

**Figure 9-15 Class 1 Laser Warning Labels for SPA Ports**

|                                                                                                                                                                                                                                                                                                                              |       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <div>CLASS 1 LASER PRODUCT<br/>LASERPRODUKT DER KLASSE 1</div>                                                                                                                                                                                                                                                               |       |
| <div>PRODUIT LASER DE CLASSE 1<br/>クラス 1 レーザ製品<br/>PRODUCTO LASER CLASE 1</div>                                                                                                                                                                                                                                              | H6655 |
| <div><div></div><div>Warning</div></div> <div><div>Class 1 laser product.</div><div>Statement 1008</div></div>                                                                                                                              |       |
| <div><div></div><div>Warning</div></div> <div><div>Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.</div><div>Statement 1051</div></div> |       |
| <div><div></div><div>Warning</div></div> <div><div>Class 1 LED product.</div><div>Statement 1027</div></div>                                                                                                                                |       |

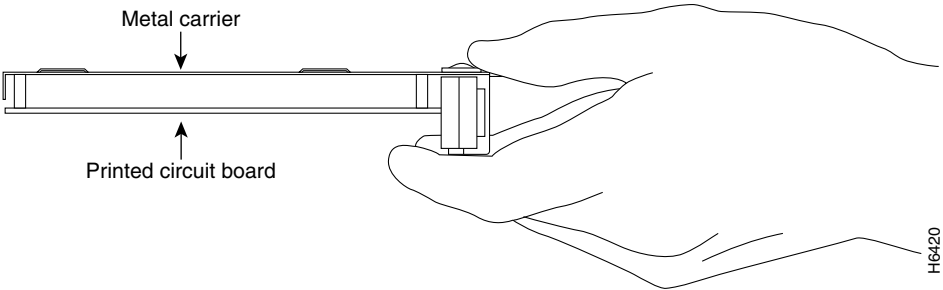
# Handling SPAs

Each SPA circuit board is mounted to a metal carrier and is sensitive to electrostatic discharge (ESD) damage.

Always handle the SPA by the carrier edges and handle; never touch the SPA components or connector pins. (See [Figure 9-16](#).)

When a subslot is not in use, a SPA blank filler plate must fill the empty subslot to allow the chassis to conform to electromagnetic interference (EMI) emissions requirements and to allow proper airflow across the installed modules. If you plan to install a SPA in a subslot that is not in use, you must first remove the SPA blank filler plate.

**Figure 9-16 Handling a SPA**



## SPA Installation and Removal


**Warning**

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Statement 94

SPAs can be inserted or removed independently from the SIP. Removal of a SIP with installed SPAs is also supported.

Figure 9-17 illustrates how to install and remove a SPA in the Cisco SCE 8000-SIP.

**Figure 9-17** SPA Installation and Removal

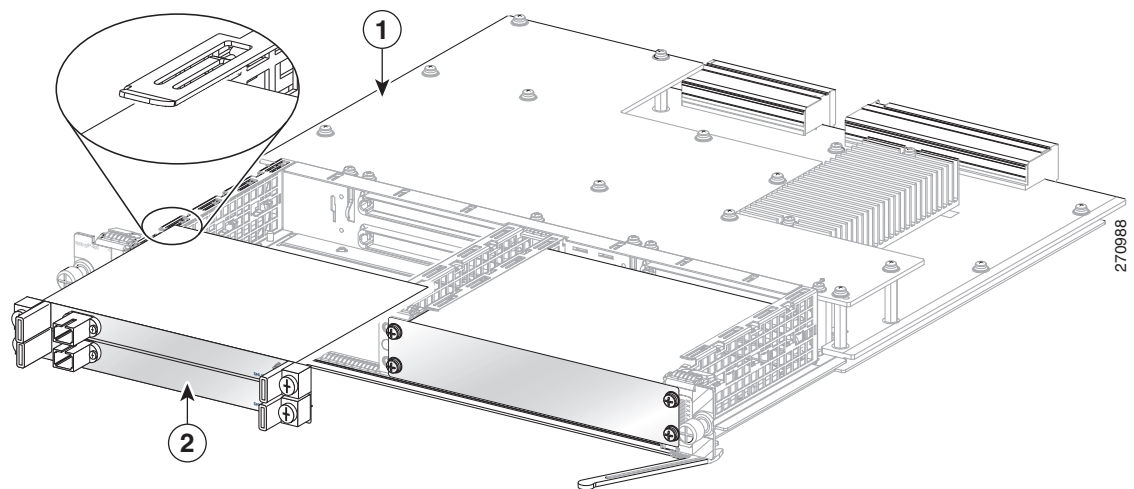


**Table 9-1** Component Indications

| This number | Indicates this component |
|-------------|--------------------------|
| 1           | Cisco SCE 8000-SIP       |
| 2           | 1X10 GBE SPA module      |

## Installing a SPA in a SIP

To install a SPA in a SIP, see [Figure 9-17](#) and do the following:

- 
- Step 1** At the **SCE#** prompt, enter **reload shutdown** and press **Enter** to power down the Cisco SCE 8000 platform before installing or removing any module.
  - Step 2** To insert the SPA in the SIP, locate the guide rails inside the SIP that hold the SPA in place. They are at the top left and top right of the SPA slot and are recessed about an inch, as shown in [Figure 9-17](#).
  - Step 3** Carefully slide the SPA into the SIP until the SPA is firmly seated in the SPA interface connector. When fully seated, the SPA might be slightly behind the SIP faceplate.
  - Step 4** After the SPA is properly seated, fasten the SPA in place with the captive installation screws.
- 

## Removing a SPA from a SIP

To remove a SPA from a SIP, see [Figure 9-17](#) and do the following:

- 
- Step 1** At the **SCE#** prompt, enter **reload shutdown** and press **Enter** to power down the Cisco SCE 8000 platform before installing or removing any module.
  - Step 2** If attached, remove any cables from the SPA.
  - Step 3** To remove the SPA from the SIP, unfasten the captive installation screws on the SPA.
  - Step 4** Grasp the handles of the SPA and pull the SPA from the SIP.
-

# Removing and Replacing the Optical Bypass Module

- [Removing the Optical Bypass Module, page 9-33](#)
- [Installing the Optical Bypass Module, page 9-33](#)
- [Replacing the Optical Bypass Module Without Disrupting Traffic on the Link, page 9-33](#)

## Removing the Optical Bypass Module

- 
- |               |                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Disconnect all cables.                                                                                                                            |
| <b>Step 2</b> | Loosen the two captive screws on the module.                                                                                                      |
| <b>Step 3</b> | Pull the module out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.   |
| <b>Step 4</b> | Place the module on antistatic foam, or immediately reinstall it in another slot.                                                                 |
| <b>Step 5</b> | If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis. |
- 

## Installing the Optical Bypass Module

- 
- |               |                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Remove the module filler plate by loosening the two screws.                                                                                                      |
| <b>Step 2</b> | Insert the module into the opening in the panel. There are no guide rails. Do not touch the module circuitry.                                                    |
| <b>Step 3</b> | Tighten the two captive screws on the module.                                                                                                                    |
| <b>Step 4</b> | Connect the cables as described in the <a href="#">“Cabling the 10 GBE Line Interface Ports: Using the External Optical Bypass Module”</a> section on page 6-14. |
- 

## Replacing the Optical Bypass Module Without Disrupting Traffic on the Link

You can replace a malfunctioning Cisco SCE 8000 platform without disrupting traffic on the link by removing the optical bypass modules while still connected to the network and installing them into the new Cisco SCE 8000.

- 
- |               |                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Install the new Cisco SCE 8000 platform in the rack. Power up the platform and perform necessary initial configuration.                                                                                            |
| <b>Step 2</b> | Disconnect the cables connecting the optical bypass module to the old Cisco SCE 8000 platform. Do not disconnect the cables connecting the optical bypass to the subscriber side or network side network elements. |

- Step 3** Remove the optical bypass module from the Cisco SCE 8000 chassis and immediately install it in the new Cisco SCE 8000 platform. Alternatively, it can be installed in an external mounting panel elsewhere in the rack.
- Step 4** Connect the cables from the optical bypass module to the line interfaces of the new Cisco SCE 8000 platform. See the [“Optical Bypass Module Connectivity” section on page 6-9](#).
-



# Using Optical Splitters with 10 GBE Links

---

Revised: February 18, 2015

## Introduction

When designing a deployment with the Cisco SCE 8000, it is important to keep in mind certain characteristics of the 10 GBE link that affect the configuration of optical splitters and SPAN ports:

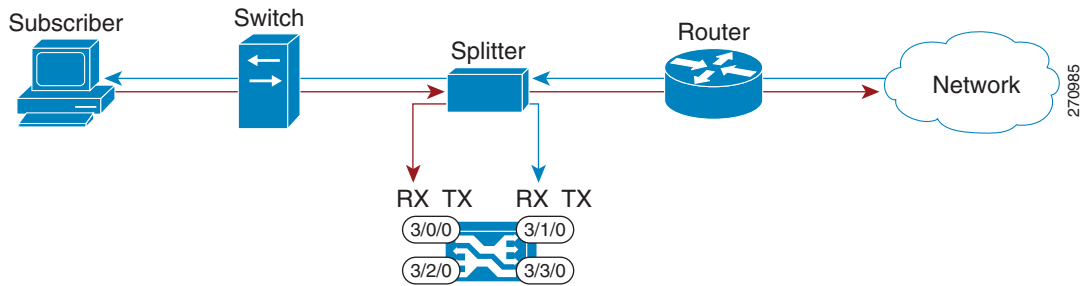
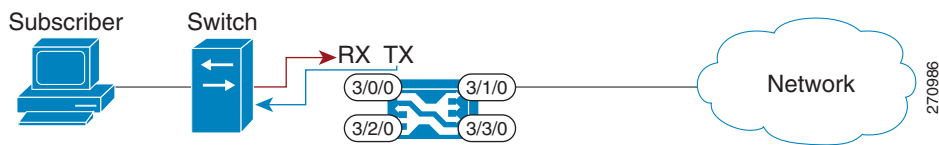
- 10 GBE does not support autonegotiation (unlike regular GBE). The fixed 10 GBE configuration is as follows:
  - duplex = full
  - speed = 10 GBE
- The 10 GBE port is UP once it detects light (and correct sync pattern) in the RX input.
- A Switch or Router port will not transmit data unless it is UP (that is, it detects a good signal on the RX input).

This chapter contains the following sections:

- [Supported Configurations, page A-1](#)
- [Unsupported Configuration, page A-2](#)

## Supported Configurations

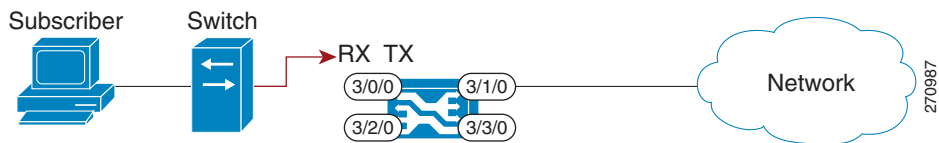
With regard to the 10 GBE characteristics described in the introduction, the following configurations are supported in the 10 GBE environment as shown in [Figure A-1](#) and [Figure A-2](#).

**Figure A-1 Supported Optical Splitter Configuration****Figure A-2 Supported SPAN Port Configuration****Note**

In the preceding configuration, it is essential that the Cisco SCE 8000 be operating in receive-only mode. Other configurations may cause SPAN port traffic to be returned to the switch, causing unpredictable behavior.

## Unsupported Configuration

With regard to the preceding 10 GBE characteristics, the following configuration is not supported in the 10 GBE environment as shown in [Figure A-3](#). In this configuration, the switch port remains in the DOWN state and therefore does not transmit.

**Figure A-3 Unsupported SPAN Port Configuration**



# CLI Commands to Verify a Successful Installation

---

Revised: February 18, 2015

## Introduction

When you have completed the installation of your Cisco SCE 8000 10 GBE platform, we recommend that you run several CLI commands to verify that the proper components have been successfully installed and are operational.

# Basic Post-Installation Checklist

The following table provides a basic post-installation checklist with the related CLI commands. Further verification of the system configuration would depend on the specific topology and configuration of the installation, but this list will verify that the basic installation is operational.

See the descriptions of the individual commands for samples of the command output. Relevant information in the output is in **bold**.

| To check this                 | Use this command                               | Comments                                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version                       | <b>show version</b>                            | Check the following: <ul style="list-style-type: none"> <li>• Firmware version</li> <li>• Application version</li> <li>• Management agent status</li> <li>• Management agent version</li> </ul>                                                 |
| Optics                        | <b>show inventory</b>                          | In the physical inventory of the SCE platform, verify that the installed optics are supported by the interfaces.                                                                                                                                |
| Port configuration            | <b>show interface</b>                          | Run this command for each port to get a listing of the status and configuration of all ports.                                                                                                                                                   |
| Operational status            | <b>show system operational status</b>          | Status should be <i>operational</i> .<br>This command will give you an indication of problems such as a power problem or external bypass not configured properly.                                                                               |
| Linecard status               | <b>show interface linecard</b>                 | It should not be <i>shutdown</i> or <i>silent</i> .                                                                                                                                                                                             |
| Connection mode               | <b>show interface linecard connection-mode</b> | Make sure that both the connection mode and the failure mode are configured correctly.                                                                                                                                                          |
| Link mode                     | <b>show interface linecard link mode</b>       | When connection-mode is inline, link mode should be configured to <i>forwarding</i> .                                                                                                                                                           |
| External bypass configuration | <b>show interface linecard external-bypass</b> | Only if external bypass modules are installed. Check the following: <ul style="list-style-type: none"> <li>• Configuration should be <i>activated</i> on failure.</li> <li>• The number of devices should match the number of links.</li> </ul> |

| To check this                    | Use this command                                                | Comments                                                                                                                                                                                                                                      |
|----------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RDR formatter                    | <b>show RDR-formatter</b>                                       | Verify the following: <ul style="list-style-type: none"> <li>RDR formatter has established a connection with the configured destinations.</li> <li>Redundancy status is configured correctly in case of more than one destination.</li> </ul> |
| Connection to Subscriber Manager | <b>show interface linecard subscriber sm-connection-failure</b> | If using SM, verify that the connection with the SM is established.                                                                                                                                                                           |
| Connection to Quota Manager      | <b>show ip rpc-adapter sessions</b>                             | If using QM, verify that the connection with the QM is established.                                                                                                                                                                           |

#### Complete command sequence for a fully-populated Cisco SCE 8000 10 GBE platform using both the SM and the QM

```

SCE> enable 5
Password:<cisco>
SCE> show version
SCE> show inventory
SCE> show interface TenGigabitEthernet 3/0/0
SCE> show interface TenGigabitEthernet 3/1/0
SCE> show interface TenGigabitEthernet 3/2/0
SCE> show interface TenGigabitEthernet 3/3/0
SCE> show system operation-status
SCE> show interface linecard 0
SCE> show interface linecard 0 connection-mode
SCE> show interface linecard 0 link mode
SCE> show interface linecard 0 external-bypass
SCE> show rdr-formatter
SCE> show interface linecard 0 subscriber sm-connection-failure
SCE> show ip rpc-adapter sessions

```

## CLI Command Output Samples

The text in **bold** in the following output samples indicates the lines you should check when doing a post-installation check. For some commands, the output is short and the entire output is relevant. In these cases, nothing is in bold.

## show version

Look for the following lines:

- System version
- Application file
- Management agent interface version

SCE> **show version**

**System version: Version 3.5.5 Build 252**

Build time: May 31 2009, 15:50:44 (Change-list 483168)

Software version is: Version 3.5.5 Build 252

Cryptography class: K9

Hardware information is:

-----  
Firmware

-----  
kernel : [kernel] 2.3.0/1 (inactive: [kernel] 2.3.0/1)  
u-boot : [uboot] 2.1.0/1 (field: [uboot] 0.8.0/3)  
select : [ubs-cf0] 2.3.0/1 (secondary: [ubs-cf0] 2.3.0/1)

-----  
Slot 1: SCE8000-SCM-E

-----  
serial-num : CAT1151G01D  
part-num : 73-10598-01 36  
cpld : 0x816c  
vtpld : 0xc004  
summit-0 : 0x10008  
summit-1 : 0x10008  
dpt/tx : 0x4913  
cls/ff : 0x2112  
cls cam : 0x454120  
cls flow cap: 33554432  
ssa : 0x90

-----  
TVR

-----  
#cpus : 1  
cpu SVR : 0x80900121  
cpu PVR : 0x80040202  
cpu freq : 1000MHz  
cpu (eeprom): 2.1, 800MHz  
cpld : 0xa1bc  
cpld-ufm : 0xa803  
summit : 0x10007  
cf : Model=SILICONSYSTEMS INC 4GB-3213, S/N=357TTR79SY716QC00005,  
FwRev=0x242-0230, Size=4125744KB  
phy-0 : 0xcc2  
phy-1 : 0xcc2  
phy-2 : 0xcc2

-----  
CFC-0

-----  
board type : P2  
#cpus : 3  
cpu-0 SVR : 0x80900121  
cpu-0 PVR : 0x80040202

```

cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb219
cpld-1 : 0xb219
cpld-2 : 0xb219
cpld-0-ufm : 0xb803
cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1100

```

```

-----
CFC-1
-----

```

```

board type : P2
#cpus : 3
cpu-0 SVR : 0x80900121
cpu-0 PVR : 0x80040202
cpu-0 freq : 1500MHz
cpu-1 SVR : 0x80900121
cpu-1 PVR : 0x80040202
cpu-1 freq : 1500MHz
cpu-2 SVR : 0x80900121
cpu-2 PVR : 0x80040202
cpu-2 freq : 1500MHz
cpu (eeprom): 2.1, 1500MHz
cpld-0 : 0xb219
cpld-1 : 0xb219
cpld-2 : 0xb219
cpld-0-ufm : 0xb803
cpld-1-ufm : 0xb803
cpld-2-ufm : 0xb803
summit-0 : 0x1000a
summit-1 : 0x1000a
fc : 0x1100

```

```

-----
Slot 3: SCE8000-SIP
-----

```

```

serial-num : CAT1105501R
part-num : 73-10947-01 11
cpld : 0x916c
summit-0 : 0xf2c1501
summit-1 : 0xf2c1601
dpt-0 : 0x3110
dpt-1 : 0x3110
ssa-0 : 0x90
ssa-1 : 0x90
spa[0] : SPA-1X10GE-L-V2
spa[1] : SPA-1X10GE-L-V2
spa[2] : SPA-1X10GE-L-V2
spa[3] : SPA-1X10GE-L-V2

```

```

-----
SCE8000 Chassis
-----

```

```

product-num : SCE8000

```

```
serial-num   : FOX1208G450
part-num     : 73-11293-01
part-rev     : A0
vid          : V01
```

```
Part number      : 73-10598-01 36
Revision         : 1
Software revision : 1
LineCard S/N     : CAT1151G01D
Power Supply type : AC
```

SML Application information is:

**Application file: /apps/data/scos/app/en355262.sli**

Application name: Engage SML Version 3.5.5 build 74

Using Lib - PL\_3.5.5\_b74

Using Lib - Classifier\_3.5.5\_b74

Application help: Entry point of Engage

Original source file:

/auto/srbu-proj1/apps/users/atukh/autoBuild/App/SML/Engage/dev/src/com/pcube/AppTemplate/Main/template\_app\_main.san

Compilation date: Tue, May 19, 2009 at 19:51:58

Compiler version: SANC v3.20 Build 12 built on: Tue 02/01/2009 11:11:05.;SME plugin v1.1

Capacity option used: 'EngageDefaultSCE8000'.

Logger status: Enabled

Platform: SCE8000

**Management agent interface version: SCE Agent 3.5.5 Build 121**

Software package file: ftp://ftpserver/D:\pcube\Os\3.5.5\252\simba\_03550252\_K9.pkg

SCE8000 uptime is 5 days, 23 hours, 52 minutes, 40 seconds

## show inventory

Look for the following lines:

- All lines containing the text 'NAME: "SCE8000 optic'. There should be one line for each installed optic.

```
SCE> show inventory
NAME: "SCE8000 Chassis", DESCR: "SCE8000"
PID: SCE8000          , VID: V01, SN: FOX1232G00V

NAME: "SCE8000 Service Control Module (SCM) in slot 1", DESCR: "SCE8000-SCM-E"
PID: SCE8000-SCM-E    , VID: V01, SN: CAT1231G040

NAME: "SCE8000 SPA Interface Processor (SIP) in slot 3", DESCR: "SCE8000-SIP"
PID: SCE8000-SIP      , VID: V01, SN: CAT1229G03H

NAME: "SCE8000 SPA module 3/0", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2  , VID: V02, SN: JAE1229PFVA

NAME: "SCE8000 SPA module 3/1", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2  , VID: V02, SN: JAE1229PFR4

NAME: "SCE8000 SPA module 3/2", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2  , VID: V02, SN: JAE1229PFR6

NAME: "SCE8000 SPA module 3/3", DESCR: "SPA-1X10GE-L-V2"
PID: SPA-1X10GE-L-V2  , VID: V02, SN: JAE1229PFR2

NAME: "SCE8000 FAN 1", DESCR: "SCE8000-FAN"
PID: SCE8000-FAN      , VID: V01, SN: DCH12281410

NAME: "SCE8000 AC power supply 0", DESCR: "PWR-2700-AC/4"
PID: PWR-2700-AC/4    , VID: V02, SN: APS12160003

NAME: "SCE8000 AC power supply 1", DESCR: "PWR-2700-AC/4"
PID: PWR-2700-AC/4    , VID: V02, SN: APS1216002N

NAME: "SCE8000 optic 3/0/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: ONT121110LJ

NAME: "SCE8000 optic 3/1/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: ECL122201CD

NAME: "SCE8000 optic 3/2/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: ECL122201CJ

NAME: "SCE8000 optic 3/3/0", DESCR: "XFP-10GLR-OC192SR "
PID: XFP-10GLR-OC192SR , VID: V02, SN: ECL122103BA
```

## show interface

Run this command for each interface. The command syntax is:

```
show interface TenGigabitEthernet 3/bay-number/0
sce> show interface TenGigabitEthernet 3/0/0
Auto negotiation configured: Disabled
Actual status:
    Link is: ON
    Auto negotiation: Disabled
Bandwidth (L1): 10000000 Kbps, Burst-size: 50000 bytes
Pseudo IP Address: Not Configured
```

## show system operational status

```
sce> show system operation-status
System Operation status is Operational
```

## show interface linecard

```
sce> show interface LineCard 0
The application assigned to slot 0 is /apps/data/scos/app/en35156.sli
Silent is off
Configured shutdown is off
Shutdown due to sm-connection-failure is off
Resulting current shutdown state is off
WAP handling is disabled
```

## show interface linecard connection-mode

```
sce> show interface linecard 0 connection-mode
slot 0 connection mode
Connection mode is inline
slot failure mode is external-bypass
Redundancy status is standalone
```

## show interface linecard link mode

```
sce> show interface LineCard 0 link mode
Link mode on all links
Current link mode is : forwarding
Actual link mode on active is : forwarding
Actual link mode on failure is: monopath-bypass
```

## show interface linecard external-bypass

```
sce1> show interface LineCard 0 external-bypass
External bypass current state is 'not activated'.
External bypass failure state is 'activated'.
Amount of expected external bypass devices: 2 (automatically configured).
Amount of detected external bypass devices: 2
```

## show RDR-formatter

Look for:

- Forwarding mode
- Status (in Status column in the Connection Table)

```
sce> show RDR-formatter
Status: enabled
Connection is: up
Forwarding mode: redundancy
Connection Table:
```

| Collector              | Port  | Status | Priority per Category: |             |           |           |
|------------------------|-------|--------|------------------------|-------------|-----------|-----------|
| IP-Address / Host-Name |       |        | Category1              | Category2   | Category3 | Category4 |
| 10.240.59.39           | 33000 | up     | 100 primary            | ---         | ---       | ---       |
| 10.240.59.44           | 33000 | up     | ---                    | 100 primary | ---       | ---       |

```
RDR:   queued:    0 ,sent:60108106, thrown:    0, format-mismatch:    0
UM:    queued:    0 ,sent:    0, thrown:    0
Logger: queued:    0 ,sent:    0, thrown:    0
Errors: thrown:    0
Last time these counters were cleared: 07:36:52 EDT TUE April 28 2009
```

## show interface linecard subscriber sm-connection-failure

If working with the Subscriber Manager, use this command to make sure the connection with the SM is established:

```
SCE> show interface linecard 0 subscriber sm-connection-failure
Current SM link state: up.
Configured action to take when SM link is down: No action.
Changing of system operational-status to 'warning' when SM link is down: enabled.
```

## show ip rpc-adapter sessions

If working with the Quota Manager, use this command to make sure the connection with the QM is established:

```
sce> show ip rpc-adapter sessions
```

```
client-name=usr.SM  
client-address=/10.240.59.36  
started=Mon Apr 06 12:43:01 GMT-04:00 2009  
received-message-num=408790  
sent-message-num=237292  
sent-notifications-num=0  
dropped-notifications-num=0  
client-username=null
```

```
client-name=mcn.SM  
client-address=/10.240.59.36  
started=Mon Apr 06 12:43:02 GMT-04:00 2009  
received-message-num=5715112  
sent-message-num=6101181  
sent-notifications-num=386768  
dropped-notifications-num=0  
client-username=null
```

```
client-name=mcn.QuotaManager-10.248.64.119_10.240.59.36_SCE.J.API.PRPC  
client-address=/10.240.59.36  
started=Mon Apr 06 12:43:03 GMT-04:00 2009  
received-message-num=404194  
sent-message-num=232248  
sent-notifications-num=0  
dropped-notifications-num=0  
client-username=null
```



# Cisco Service Control Engine System Log Messages

---

**Revised: February 18, 2015**

The Cisco Service Control Engine (SCE) 8000 generates system, error, and other informational messages to inform Cisco SCE 8000 users of significant events. This appendix describes the system log messages generated by the Cisco SCE 10 8000 GBE platform.

The system messages in the Cisco SCE 8000 platform have the following structure:

`%FACILITY-SEVERITY-MNEMONIC: Description`

The following list describes the various components of the message structure:

- **FACILITY** indicates the platform that is generating the message. The FACILITY value in the Cisco SCE 8000 platform indicates LOCAL7, which represents the default facility type of the Cisco SCE 8000 platform.
- **SEVERITY** is a numeral that reflects the severity of the corresponding error condition. The messages have a severity level ranging from 0 to 6, with 0 indicating the highest severity level and 6 the lowest.
- **MNEMONIC** uniquely identifies the message. All mnemonics are uppercase character strings.
- **Description** describes the corresponding error condition and contains variable fields that change from message to message. The variable fields can represent IP addresses, character strings, filename, and so on.

This document lists the following system message categories by severity level. Each message is followed by an explanation and a recommended action.

- [Fatal Messages, Severity Level 2, page C-2](#)
- [Error Messages, Severity Level 3, page C-4](#)
  - [Common Error Messages, page C-4](#)
  - [Control Card Error Messages, page C-5](#)
  - [Line Card Error Messages, page C-6](#)
- [Informational Messages, Severity Level 6, page C-7](#)
- [Warning Messages, Severity Level 4, page C-41](#)
- Emergency Messages, Severity Level 0
- Alert Messages, Severity Level 1
- Critical Messages, Severity Level 2

- Warning Messages, Severity Level 4
- Notice Messages, Severity Level 5

## Fatal Messages, Severity Level 2

**Fatal Message** %LOCAL7-2-SE\_USER\_FATAL "SE <%s> Module: A Fatal Error occurred. Please report to Cisco's customer support"

**Explanation** This message is generated to inform that a fatal error has occurred.

**Recommended Action** Report this to Cisco Customer Support.

**Fatal Message** %LOCAL7-2-LOGGER\_USER\_FATAL\_MSG "<%s>"

**Explanation** This message is generated while you add your own fatal messages to the user log file using the **logger add-user-message** command in the CLI.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-DP\_CLS\_SEQ\_ERR "HW internal error

**Explanation** This is an internal hardware error. This fatal hardware interrupt is generated when there is a mismatch in the sequence of messages to the classifier.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-CLS\_FF\_SEQ\_ERR "HW internal error

**Explanation** This is an internal hardware error. This fatal hardware interrupt is generated when there is a mismatch in the sequence of messages to the flow filter.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-DP\_IN\_SEQ\_ERR "HW internal error

**Explanation** This is an internal hardware error. This fatal hardware interrupt is generated when there is a mismatch in the sequence of the dispatcher input messages.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-DP\_OUT\_SEQ\_ERR "HW internal error

**Explanation** This is an internal hardware error. This fatal hardware interrupt is generated when there is a mismatch in the sequence of the dispatcher output messages.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-LIC\_CRASH\_FATAL "HW internal error: LIC Interrupt - bypass wd not working in crash mode."

**Explanation** This is an internal hardware error that occurs when bypass does not work in the crash mode, and a linecard interrupt occurs.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-GENERIC\_FATAL "A problem occurred in the <%s> ,Please report to Cisco's customer support."

**Explanation** This message is displayed in a user's log when a generic fatal error occurs.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-MSG\_HANDLER\_READING\_FROM\_Q\_FAILED "SW internal error: failed reading from message queue"

**Explanation** This fatal message is displayed when the remote procedure call (RPC) message handler fails to receive a message from the corresponding queue.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-READING\_FROM\_Q\_FAILED " SW internal error - Failed to read from receive queue number %d, from ppc: %d, to ppc: %d, queue: %d."

**Explanation** This fatal message is displayed when failure to read a message from a queue number with a traffic processor and queue details occurs.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-TOO\_MANY\_MSGS\_FROM\_SINGLE\_QUEUE "SW internal error - Received %d consecutive messages from queue number %d, from ppc: %d, to ppc: %d, queue: %d."

**Explanation** This fatal message is displayed when more than 400 messages exist in a single queue.

**Recommended Action** None.

**Fatal Message** %LOCAL7-2-READING\_FROM\_Q\_FAILED "A SW error occurred. Please report to P-Cube's Customer Support"

**Explanation** This message is displayed when the line card handler fails to read a message from the corresponding queue.

**Recommended Action** None.

**Fatal Message** SIMBA\_USR\_HW\_MONITOR\_FATAL "<%s>: <%s> hardware monitor status is FATAL"

**Explanation** This message is displayed when a fatal error occurs in any of the corresponding hardware modules.

**Recommended Action** None.

## Error Messages, Severity Level 3

### Common Error Messages

**Common Error Message** %LOCAL7-3-SE\_USER\_ERROR "SE %s Module: An Error occurred. Please report to Cisco's customer support"

**Explanation** This error message is generated when one of the following scenarios occur:

- The hardware monitor sanity check fails.
- When there is an error in a partition, the ControlCard watchdog timeout handler, and so on.

**Recommended Action** Generate the support file and contact Cisco Customer Support.

**Common Error Message** %LOCAL7-3-"NOT\_ENOUGH\_MEMORY "Partition init - not enough memory. Required = %lu + %lu for sys heap, Available = %lu\n Memory will be adjusted"

**Explanation** This message is displayed when there is insufficient memory for allocating a new parent block from the VxWorks heap.

**Recommended Action** None.

**Common Error Message** %LOCAL7-3-FAILED\_TO\_ALLOCATE\_MEMORY "Part init - failed to allocate the parent block. size = %lu"

**Explanation** This message is displayed when there is a failure to allocate memory for the parent block, and the log displays the parent block size.

**Recommended Action** None.

## Control Card Error Messages

**Control Card Error Message** %LOCAL7-3-RESTART\_FAILED\_SHUT\_DOWN "Management agent restart procedure failed"

**Explanation** This message is displayed to indicate that the management agent is going to restart, and the status of the management agent is not down.

**Recommended Action** None.

**Control Card Error Message** %LOCAL7-3-RESTART\_FAILED\_START\_UP "Management agent restart procedure failed"

**Explanation** This message is displayed to indicate that the management agent is down, and hence the service mode configuration is set to true for restarting the management agent.

**Recommended Action** None.

**Control Card Error Message** %LOCAL7-3-SIMBA\_USR\_HW\_MONITOR\_ERROR "<%s>"

**Explanation** This message is displayed to indicate that a hardware error occurred and may cause unusual behavior of the device.

**Recommended Action** Generate the support file and contact Cisco Customer Support.

**Control Card Error Message** %LOCAL7-3-GEN\_CONFIG\_FILES\_BAD "General configuration file executed with %lu errors. Please view the file '<%s>' for details."

**Explanation** This message is displayed when an error occurs when startup configuration is applied. However, if one of the CLIs fails during the configuration, that CLI will not be effective.

**Recommended Action** Generate the support file and contact Cisco Customer Support.

**Control Card Error Message** %LOCAL7-3-APP\_CONFIG\_FILES\_BAD "Application configuration files executed with %lu errors."

**Explanation** This message is displayed when an error occurs when application configuration is applied. If one of the CLIs fails during the configuration, that CLI will not be effective.

**Recommended Action** Generate the support file and contact Cisco Customer Support.

**Control Card Error Message** %LOCAL7-3-LOGGER\_USER\_ERR\_MSG "<%s>"

**Explanation** This message is generated when you add your own error messages to the user log file using the **logger add-user-message** command.

**Recommended Action** None.

**Control Card Error Message** %LOCAL7-3-MESSAGE\_QUEUE\_FAILURE "This is a five string dbg message 1

**Explanation** This message is generated when Cisco SCE fails to read the logger message from the logger queue because the queue is corrupted. This message displays the error details of the queue, queue index, and queue information.

**Recommended Action** None.

**Control Card Error Message** %LOCAL7-3-INIT\_FAILED "Subscriber database initialization failed."

**Explanation** This error message is generated when the task of spawning the party DB manager fails.

**Recommended Action** None.

**Error Message** %LOCAL7-3-RUN\_PARTIES\_FAILD\_NAME\_DEFAULT "subscriber database load - failed to change default subscriber name to <%s>."

**Explanation** This message is generated when an error occurs while changing the default name of the subscriber.

**Recommended Action** None.

**Control Card Error Message** %LOCAL7-3-RUN\_PARTIES\_FAILED\_INSERT\_PARTY "subscriber database load - failed to insert subscriber <%s>."

**Explanation** This message is generated when a problem occurs while inserting a new subscriber into the party database.

**Recommended Action** None.

## Line Card Error Messages

**Line Card Error Message** %LOCAL7-3-DP\_SEARCH\_ENGINE\_FAILURE "A HW failure in the tunneling engine has been detected. Please speak with Cisco customer support"

**Explanation** This message is displayed to indicate that a hardware failure occurred in the tunneling engine, and may cause an unusual behavior of the device.

**Recommended Action** None. Contact Cisco Customer Support.

## Informational Messages, Severity Level 6

**Error Message** %LOCAL7-6-INIT\_SUCCEEDED: Part init - Partitions manager initialization succeeded, total application memory size *size*.

**Explanation** This message is displayed when memory is successfully allocated for the partition manager from the memory block, and initialization is successful.

In this message, *size* refers to the size of the memory block being allocated.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STARTED\_INTERPRETATION: Debug log interpretation started. Output file name *name*.

**Explanation** This message is displayed when debug log interpretation (to a readable format) is started, and the output is being saved to a file name.

In this message, *name* is the name of the output file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-INTERPRETATION\_FINISHED: Debug log interpretation terminated. Output file name *name*.

**Explanation** This message is displayed when debug log interpretation (to readable format) is terminated, and the output is being saved to a file.

In this message, *name* is the name of the output file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STARTED\_STATS\_INTERPRETATION: "Statistics File interpretation started. source file name *file name*

**Explanation** This message is displayed when statistics interpretation is started.

In this message, *file name* is the name of the source file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STATS\_INTERPRETATION\_FINISHED: "Statistics File interpretation terminated. source file name *file name*

**Explanation** This message is displayed when statistics interpretation (to a readable format) is terminated.

In this message, *file name* is the name of the source file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ENABLED\_CONF\_CHANGED: "Attack-filter configuration was <%s> for some (or all) attack types."

**Explanation** This message is displayed to indicate the status of the attack filter configuration.

**Recommended Action** None.

**Error Message** %LOCAL7-6-HOST\_NAME\_CHANGED: "System hostname changed to *hostname*."

**Explanation** This message is displayed to indicate that the system hostname is changed to the configured host name.

In this message, *hostname* is the new host name.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FLASH\_TO\_DEFAULT\_CALLED: CPU#000 'Reset to Default' called."

**Explanation** This message is displayed to indicate that the system has started resetting the Cisco SCE configurations to factory default configurations.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FLASH\_TO\_DEFAULT\_FINISHED: "'Reset to Default' finished."

**Explanation** This message is displayed to indicate that the system has completed resetting the Cisco SCE configurations to factory default configurations.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SOFT\_RESET\_AND\_REFRESH\_OK\_USER: "Linecard in slot *slot-number* was soft-reset and refreshed with all data."

**Explanation** This message is displayed to indicate that the linecard in the slot has been soft reset and refreshed with all the data. (The soft reset refreshes the linecard to the state it was in before the reset).

**Recommended Action** None.

**Error Message** %LOCAL7-6-REBOOTCC\_CALLED: "Rebooting the box per user request."

**Explanation** This message is displayed while rebooting the Cisco SCE 8000 platform on a user's request.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SHUTDOWNCC\_CALLED:"Shutting down the box per user request."

**Explanation** This message is displayed when the Cisco SCE 8000 platform is shut down on a user's request.

**Recommended Action** None.

**Error Message** %LOCAL7-6-START\_SHUT\_NO\_SHUT:"Starting Line Card on slot *slot-number* state change to <%s>"

**Explanation** This message is displayed when the user information for a linecard slot state is changed to shutdown or no-shutdown.

In this message, *number* indicates the slot number, and *state* indicates shutdown or no-shutdown.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINECARD\_SHUTDOWN\_STATE: "Linecard on slot *slot-number* is *state*."

**Explanation** This message is displayed to indicate the state of a linecard: enabled or disabled.

In this message, *slot-number* indicates the slot number, and *state* indicates the linecard state: enabled or disabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_TIME\_ZONE:"Time zone set to *zone num* minutes."

**Explanation** This message is displayed to indicate the time zone set in the system.

In this message, *zone* indicates the time zone, and *num* indicates the minutes.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_CLOCK:"System clock set to *GMT-time*."

**Explanation** This message is displayed to indicate that the system clock is updating the GMT time and the Traffic Processor.

In this message, *GMT-time* indicates the time in GMT format.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_CALENDAR:"Time-of-day clock set to *time*."

**Explanation** This message is displayed to indicate that the time-of-day clock is set to a given time. The command used to set the calendar time is:

*calendar set 09:31:23 26 August 2011*

In this message, *time* indicates the calendar time that is set.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CONFIGURATION\_SAVED:Configuration file *file-name* was saved - files size = *size*.

**Explanation** This message is displayed to indicate that the current configuration file is saved to a file.

In this message, *file-name* indicates the name of the file, and *size* indicates the size of the file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CONFIGURATION\_FILES\_DELETED:"Configuration files were deleted according to user command."

**Explanation** This message is displayed to indicate that all the configuration files corresponding to the Cisco Service Control Operating System (Cisco SCOS) and management agents have been deleted, and the default configuration added to the files.

**Recommended Action** None.

**Error Message** %LOCAL7-6-COPY\_FILE:"File system operation

**Explanation** This message is displayed to indicate that the **copy** command has been executed in the CLI, and that the current file is being copied to the destination file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FINISHED\_COPYING: "Finished copying file of size *num* bytes"

**Explanation** This message is displayed to indicate that the task of copying the current file to the destination file is completed.

In this message, *num* indicates the file size in bytes.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_FILE:"File system operation

**Explanation** This message is displayed to indicate the deletion of a file or a directory using the **delete** command in the CLI.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RENAME\_FILE:File system operation

**Explanation** This message is displayed to indicate the renaming of a source file name to a destination file name using the **rename** command in the CLI.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CREATE\_DIR:"File system operation

**Explanation** This message is displayed to indicate the creation of a directory in Cisco SCE using the **mkdir** command in the CLI.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_DIR:"File system operation

**Explanation** This message is displayed to indicate the deletion of a file or a directory using the **delete** command in the CLI.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_RECURSIVE : "File system operation

**Explanation** This message is displayed to indicate the deletion of a file or a directory using the **delete** command in the CLI, with a recursive option. The recursive option deletes all the subdirectories and files present in the main directory.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_RECURSIVE\_RESULT : "File system operation

**Explanation** This message is displayed to indicate the successful deletion of a file or a directory with a recursive option.

**Recommended Action** None.

**Error Message** %LOCAL7-6-GET\_FTP:"File system operation

**Explanation** This message is displayed to indicate that file transfer to or from Cisco SCE has occurred.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PUT\_FTP:"File system operation

**Explanation** This message is displayed to indicate that data from Cisco SCE is being copied to the system using the **FTP PUT** command.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_ENABLED\_CFG\_USER:"Management agent was <state> by user configuration."

**Explanation** This message is displayed to indicate that the user information management agent in Cisco SCE is enabled or disabled by user configuration.

In this message, *state* indicates whether the management agent is enabled or disabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_ENABLED\_TO\_DEFAULT:"Management agent status was set to its default configuration."

**Explanation** This message is displayed to indicate that the user information management agent status was set to its default configuration.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RESTART\_CALLED : "Management agent restart procedure called."

**Explanation** This message is displayed when the management agent restart procedure is called by Cisco SCE.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RESTART\_FINISHED:"Management agent restart procedure finished successfully."

**Explanation** This message is displayed when the management agent JVM restart procedure is successful.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RESTART\_FROM\_JAVA\_CALLED : "Management agent self restart procedure called."

**Explanation** This message is displayed when the management agent is restarted from JVM.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UM\_AGENT\_IS\_UP:"Management agent is up."

**Explanation** This message is displayed when the user management agent is up and running.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UM\_AGENT\_IS\_DOWN:"Management agent is down."

**Explanation** This message is displayed when the user management agent is down.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_ACTIVATED:"Activating external bypass device due to user request"

**Explanation** This message is displayed when a user manually activates the external optical bypass device.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_DEACTIVATED:"Deactivating external bypass device due to user request"

**Explanation** This message is displayed when a user manually deactivates the external optical bypass device.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_ACTIVATED\_LINK\_CUTOFF:"External bypass device activated and detected on link *num*, taking the link down for *num-sec* milliseconds."

**Explanation** This message is displayed when preparing a link for external bypass. The link is restarted before external bypass is activated. Restarting the link involves deactivating the link for a few milliseconds and then reactivating it.

In this message, *num* indicates the link, and *num-sec* indicates the number of milliseconds.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_ACTIVATED\_TEST\_PACKETS\_ON\_HOLD:"During external bypass device activation procedure, test packets are disabled for *num-sec* milliseconds."

**Explanation** This message is displayed when the test packet mechanism is put on hold during the external bypass device activation period. This is done to prevent packets from being dropped.

In this message, *num* indicates the link.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_WIRE\_TEST\_AUTO\_NEG\_TEMP\_OFF:"External bypass test is on. deactivating auto-negotiation for interface <intf-name>."

**Explanation** This message is displayed while performing the external bypass test. Auto negotiation, if supported, is deactivated for the interface.

In this message, *intf-name* is the name of the interface.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_WIRE\_TEST\_AUTO\_NEG\_BACK\_ON:"Ending external bypass test. Restoring the activation status of auto-negotiation for interface <intf-name>"

**Explanation** This message is displayed after the external bypass test is completed, and autonegotiation is reactivated for the corresponding interface.

In this message, *intf-name* is the name of the interface.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_WIRE\_TEST\_EB\_ON:"External bypass test is on. Manually activating the external bypass units."

**Explanation** This message is displayed to indicate that the external bypass test is on, and that the external bypass units are being manually activated.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXTERNAL\_BYPASS\_WIRE\_TEST\_EB\_BACK:"Ending external bypass test. Restored the external bypass units' activation status"

**Explanation** This message is displayed after the completion of the external bypass test, and during the restoration of the external bypass units' activation status.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_IP:"IP address of slot *slot-num* set to *ip-addr*, subnet mask *subnet-mask*."

**Explanation** This message is displayed while the IP address and subnet mask for the corresponding slot is being set.

In this message, *ip-addr* indicates the IP address of the slot, *subnet-mask* indicates the subnet mask of the slot, and *slot-num* indicates the number of the slot.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_IP\_CHANGED:"IP address of peer box was changed (was *old-ip-addr*, changed to *new-ip-addr*)."

**Explanation** This message is displayed while the existing IP address of the peer box is being changed. The message appears when the existing IP address and the new IP addresses are not matched in the peer Cisco SCE box.

In this message, *old-ip-addr* indicates either the old IP address or the existing IP address of the peer box, and *new-ip-addr* indicates the new IP address.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_IP\_SET:"Peer box IP address is *ip-addr*."

**Explanation** This message is displayed when Cisco SCE sets the IP address of the peer box for the first time. It verifies if the previous IP address is set; if not, the IP address is set to a new IP address.

- In this message, *ip-addr* is the new IP address set for the peer box.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_DEFGW:"IP Default gateway set to *def-gw-ip-addr*."

**Explanation** This message is displayed while a new default gateway for a particular slot is being set.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FINISHED\_VERIFY: "Package verification finished"

**Explanation** This debug-related information message is displayed when the verification of a package is completed successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STARTED\_EXTRACT:"Package extraction started on file '*pkg-filename*'"

**Explanation** This debug-related information message is displayed when package extraction begins. Extraction can occur with or without the verification of a package. This message returns the name of the file on which extraction is initiated.

- In this message, *pkg-filename* indicates the name of the package file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FINISHED\_EXTRACT: "Package extraction finished"

**Explanation** This debug informational message is displayed when the package extraction process is completed (with or without verification). The filename is displayed after the extraction is completed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STARTED\_COMPARE: "Package compare started on file '*pkg-filename*' "

**Explanation** This debug informational message is displayed when the package comparison process begins. The package that is compared is displayed on the screen.

In this message, *pkg-filename* indicates the name of the package file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FINISHED\_COMPARE: "Package compare finished"

**Explanation** This debug informational message is displayed when the package comparison process is completed. The comparison process also includes checking the package creation and package verification tasks. When the comparison is successfully completed, the filename is displayed on the screen.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CLEAR\_DB\_DONE\_USER: "Subscribers database was cleared of all data successfully."

**Explanation** This debug informational message is displayed when subscribers' database is cleared of all data successfully. The database is cleared only when the linecard is in either the shutdown mode or the no-application mode.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_ALL\_ANONYMOUS: "Removing all anonymous subscribers."

**Explanation** This debug informational message is displayed when all the anonymous subscribers' information is removed. This message appears when a call for removing all the current anonymous (internal) subscribers is invoked.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_ALL\_INTRODUCED: "Removing all introduced subscribers."

**Explanation** This debug informational message is displayed when all the introduced subscribers are removed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_ALL\_TUNNELED : "Removing all tunneled subscribers."

**Explanation** This debug informational message is displayed while removing all the tunneled subscribers.

**Recommended Action** None.

**Error Message** %LOCAL7-6-NOTIFY\_ALL\_ANONYMOUS: "Sending notifications for all anonymous subscribers."

**Explanation** This debug informational message is displayed while sending notifications to all the anonymous subscribers. This message is displayed when the notification function for all the anonymous parties is invoked.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PASSWORD\_CHANGED: "A new password was set for level *level*."

**Explanation** This message is displayed when a new password is set for a given privilege level. In this message, *level* indicates the privilege level.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ASSIGNCFG\_START: "Starting application load of application file

**Explanation** This message is displayed when an application is assigned to a line card. This message displays the loaded application name and the line card slot number.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ASSIGNCFG\_OK: "Application assigned to slot *slot-num*. \nApplication file

**Explanation** This message is displayed after an application is assigned to a line card slot. The Cisco SCE 8000 platform displays the application assigned to a particular line card slot number, and the application file name.

In this message, *slot-num* indicates the slot number.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNASSIGNCFG\_START: "Starting application unload to slot *slot-num*."

**Explanation** This message is displayed when Cisco SCE begins unloading an application from a line card slot.

In this message, *slot-num* indicates the slot number.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNASSIGNCFG\_OK: "Current application on slot *slot-num* was successfully un-assigned."

**Explanation** This message is displayed when an application is successfully unassigned from a line card slot.

In this message, *slot-num* indicates the slot number.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REPLACE\_CFG\_START: "Starting application replace of application file

**Explanation** This message is displayed while replacing the existing application with a new application for the corresponding line card slot.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOGGER\_INIT\_SUCCESS: "Logger task Initialized successfully"

**Explanation** This message is displayed when logger task initialization is successful.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXIT\_BY\_REQUEST : "Logger exit request received. Exiting logger ..."

**Explanation** This message is displayed when the logger task exits after receiving an exit request message from an event.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINE\_ATTACK\_FILES\_CLEAR: "Cleared line-attack log files"

**Explanation** This message is displayed when the line-attack log file is cleared. Line-attack messages are stored in a line-attack log file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ACTIVE\_CONNECTION\_OPEN: "Formatter active connection opened

**Explanation** This message is displayed to provide the details of the RDR formatter IP address, port number, and the category of the connection that is in active state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SWITCH\_CONNECTION\_OPEN: "Formatter switched active connection to: address %s, port %d, category %d."

**Explanation** This message is displayed to provide the details of the RDR formatter IP address, port number, and the category of the switched connection that is in active state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CONNECTION\_CLOSED: "Formatter connection closed"

**Explanation** This message is displayed to provide the details of the RDR formatter IP address along with the port number of the connection that is closed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CONNECTION\_OPENED: "Formatter connection opened"

**Explanation** This message is displayed to provide details of the RDR formatter IP address along with the port number for which the connection is opened.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOGGERLINEATTACKLOGFULLTRAP: "<%s>"

**Explanation** This trap is generated when the logger file, LineAttackLog, is full.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINKMODE\_BYPASS\_TRAP: "<%s>"

**Explanation** This trap is generated when the Cisco SCE link mode is set to bypass state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINKMODE\_FORWARDING\_TRAP: "<%s>"

**Explanation** This trap is generated when the Cisco SCE link mode is set to forwarding state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINKMODE\_CUTOFF\_TRAP: "<%s>"

**Explanation** This trap is generated when the Cisco SCE link mode is set to cutoff state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINKMODE\_SNIFFING\_TRAP: "<%s>"

**Explanation** This trap is generated when the Cisco SCE link mode is set to sniffing state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_ALL\_INTRODUCED\_MAPPINGS: "Removing all introduced subscribers' mappings."

**Explanation** This message is displayed before all the external subscriber mappings are removed from the database.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SYNC\_START: "Subscribers' database: starting synchronization process."

**Explanation** This message is displayed when synchronization of the party database using external management is started.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SYNC\_END: "Subscribers' database: synchronization process done."

**Explanation** This message is displayed when synchronization of the party database using external management is stopped.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_ALL\_ANONYMOUS\_GROUPS: "Removing all anonymous-subscribers groups."

**Explanation** This message is displayed in response to a command that is issued to remove all the anonymous subscriber groups.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_ALL\_TEMPLATES\_TO\_DEFAULT: "Setting all subscriber templates to default values."

**Explanation** This message is displayed in response to a command that is issued to set all the subscriber templates to their default values.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_MAX\_TIRS: "Setting maximum number of TIRs to: %u."

**Explanation** This message is displayed in response to a command that is issued to set a new upper limit of IP range to the Traffic Processor IP Range (TIR).

**Recommended Action** None.

**Error Message** %LOCAL7-6-RESET\_MAX\_TIRS: "Resetting maximum number of TIRs to default."

**Explanation** This message is displayed in response to a command that is issued to set the IP mappings, which are assigned to the traffic processor, to their default values.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ADD\_TIR: "Adding a TIR - Name

**Explanation** This message is displayed when a user tries to add the traffic processor and IP mappings for a specific IP or range of IP addresses from external management.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_TIR:"Removing a TIR - Name

**Explanation** This message is displayed when the traffic processor and IP mappings for a specific IP are removed using a command.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVE\_MAPPINGS\_IN\_RANGE: "Removing Subscriber mappings in IP Range

**Explanation** This message is displayed when the traffic processor and IP address mappings for a specific IP range are removed through external management.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REPLACE\_CFG\_OK: "Application replace started on slot %ld, replace is in progress.\nApplication file

**Explanation** This message is displayed when a request is issued from external management to replace the current application configuration without the service being disrupted.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REPLACE\_ENDED: "Application replace ended on slot %ld, replace finished."

**Explanation** This message is displayed when application replacement is completed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-TRAVERSING\_ALL: "slot number %d analyzing transport layer information"

**Recommended Action** This message is displayed when a request is made by a user from external management through the CLI to parse the transport layer instead of performing payload operation of a packet for analysis. The user can specify whether or not to scan only the payload or the entire transport layer of the packet for analysis.

**Recommended Action** None.

**Error Message** %LOCAL7-6-TRAVERSING\_ONLY\_PAYLOAD: "slot number %d analyzing payload only"

**Explanation** This message defines the details of the traverse layer in a particular slot with the slot number that is allowed to traverse only the payload.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DAEMON\_ENABLED: "Telnet daemon was enabled."

**Explanation** This message is displayed when the telnet process daemon is enabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DAEMON\_DISABLED: "Telnet daemon was disabled."

**Explanation** This message is displayed when the telnet process daemon is disabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DEBUG\_TELNET\_ACCESS: "<%s> access to debug-telnet (port 2300) "

**Explanation** This message is displayed when debug telnet access to port 2300 is enabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DEBUG\_SHELL\_ACCESS: "<%s> access to debug-shell (port 2301) "

**Explanation** This message is displayed when debug shell access to port 2301 is enabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DEBUG\_SSH\_ACCESS: "<%s> access to debug-ssh (port 2200) "

**Explanation** This message is displayed when debug SSH access to port 2200 is enabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-BIND\_VTY\_SERVICE : "Telnet service bound to management vlan (%u) "

**Explanation** This message provides the details about the telnet service that is added in VLAN management configurations, along with the VLAN ID.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNBIND\_VTY\_SERVICE: "Telnet service unbound from management vlan (%u) "

**Explanation** This message is displayed when the telnet service is unbound from the management VLAN.

**Recommended Action** None.

**Error Message** %LOCAL7-6-BIND\_SSH\_SERVICE: "SSH service bound to management vlan (%u) "

**Explanation** This message is displayed when the SSH service is bound with the management VLAN.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNBIND\_SSH\_SERVICE: "SSH service unbound from management vlan (%u) "

**Explanation** This message is displayed when the SSH service is unbound from the management VLAN.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SERVER\_ENABLED: "Web server enabled."

**Explanation** This message is displayed when the web server is enabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SERVER\_DISABLED: "Web server disabled."

**Explanation** This message is displayed when the web server is disabled.

**Recommended Action** None.

**Error Message** %LOCAL7-6-BIND\_SNMP\_SERVICE: "SNMP service binded to management vlan (%u) "

**Explanation** This message is displayed when the SNMP service is bound to the management VLAN.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNBIND\_SNMP\_SERVICE: "SNMP service un-binded from management vlan (%u) "

**Explanation** This message is displayed when the SNMP service is unbound from the management VLAN.

**Recommended Action** None.

**Error Message** %LOCAL7-6-NO\_CONNECTIONS\_OPEN: "No Formatter connection is open on category %d."

**Explanation** This message is displayed when no formatter connection is open in a category.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MSG: "<%s>"

**Explanation** This message provides details about the RPC client request to the server with its requester ID.

**Recommended Action** None.

**Error Message** %LOCAL7-6-USER\_FILES\_CLEAR: "Cleared user log files"

**Explanation** This message is displayed when user log files are cleared using the **clear logger device user-file-log** command.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOGGER\_STAM: "This a message with 5 parameters one %d two %d three %d four %d five %d"

**Explanation** This message is displayed by the debug message test function that is currently not in use.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOGGER\_USER\_INFO\_MSG: "<%s>"

**Explanation** This message is displayed while adding a user message to the corresponding user log using the **logger add-user-message** command.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DBG\_INIT\_OPENED\_NEW\_FILES: "DBG - failed opening files for read & write. New files were opened, old files deleted."

**Explanation** This message is displayed when the DBG fails to open the files to perform read and write operations. The new files are opened and the old files deleted. This occurs when an attempt is made to initialize the debug log files and these files are not found.

**Recommended Action** None.

**Error Message** %LOCAL7-6-TESTING\_INFO\_LEVEL: "syslog test message for info severity level"

**Explanation** This message is displayed to indicate the information severity level.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_BAD\_LOGIN: "Bad password attempted on a CLI session from <%s>."

**Explanation** This message is displayed when a wrong password is given by a user while logging into the CLI session.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LINK\_UP\_TRAP: "Link up trap generated for Mng interface %d."

**Explanation** This trap is generated by the SNMP when the managing interface is up.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SNMP\_TRAP: "<%s>"

**Explanation** All types of SNMP traps generate this message with the details of the traps.

**Recommended Action** None.

**Error Message** %LOCAL7-6-AUTHENTICATION\_FAILURE\_TRAP: "Authentication failure."

**Explanation** This message is generated when authentication failure of an SNMP trap occurs.

**Recommended Action** None.

**Error Message** %LOCAL7-6-OPERATIONAL\_STATUS\_WARNING\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated to indicate that the Cisco SCE platform is operational until one of the following states occur:

- Link on one of the line ports is down
- Management port link is down

- Temperature raised above threshold
- Voltage not in required range
- Fans problem
- Power supply problem
- Insufficient space on the disk



**Note** If the condition that causes the Cisco SCE platform to be in the Warning state is resolved, it means that when the link is up, the Cisco SCE platform will revert back to the operational state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-OPERATIONAL\_STATUS\_FAILURE\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated to indicate that the Cisco SCE platform will be in the failure state after reboot due to one of the following conditions:

- Power on test failure
- Three abnormal reboots in less than 20 minutes
- Platform configured to enter the failure mode consequent to failure-induced reboot, which is configurable using a CLI command



**Note** Depending on the cause of the failure, the management interface and the Cisco SCE platform configuration may or may not be active or available.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SYSTEM\_RESET\_BYUSER\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the system is reset by a user.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SYSTEM\_RESET\_BYFATAL\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the system is reset by a fatal trap.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SNMP\_COLDSTART\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the SNMP agent restarts.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_TEMP\_ALARMON\_TRAP : "<%s>"

**Explanation** This SNMP trap is generated when the chassis temperature alarm is in the On state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_TEMP\_ALARMOFF\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the chassis temperature alarm is in the OFF state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_VOLTAGE\_ALARMON\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the chassis voltage alarm is in the ON state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_FANS\_ALARMON\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the chassis fans alarm is in the ON state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_POWERSUPPLY\_ALARMON\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the chassis power supply alarm that is in the ON state is detected.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHASSIS\_LINEFEED\_ALARMON\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the chassis line feed alarm that is in the ON state is detected.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_ACTIVECONNECTION\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when one of the RDR formatter connections becomes the active connection.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_NOACTIVECONNECTION\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when there is no active connection between the RDR formatter and the collection manager.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_CONNECTION\_UP\_TRAP : "<%s>"

**Explanation** This SNMP trap is generated to indicate that one of the RDR formatter connections has been established.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_CONNECTION\_DOWN\_TRAP: "<%s>"

**Explanation** This SNMP trap indicates that one of the RDR formatter connections has been disconnected.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_FORMATTER\_DISCARDING\_TRAP : "<%s>"

**Explanation** This SNMP trap is generated when the agent entity detects that the reports sent to this RDR category are discarded.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RDR\_FORMATTER\_STOPPED\_DISCARDING\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the agent entity detects that the reports sent to this RDR category are not discarded.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_STARTED\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the agent entity accepts a new session.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_ENDED\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the agent entity detects the end of a session.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_DENIEDACCESS\_TRAP : "<%s>"

**Explanation** This SNMP trap is generated when the agent entity denies a session from an unauthorized source.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_BADLOGIN\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the agent entity detects an attempt to log in with a wrong password.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOGGER\_USERLOGISFULL\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when a user log file is full and the agent entity rolls to the next file.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SNTP\_CLOCKDRIFTWARN\_TRAP: "<%s>"

**Explanation** This trap is generated when the SNTP agent does not receive a time update for long, which may in turn cause a time drift.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ILLEGAL\_SUBSCRIBERMAPPING\_TRAP : "<%s>"

**Explanation** This trap is generated when an external entity tries to create an illegal or inconsistent subscriber mapping.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PULLREQUEST\_RETRYFAILED\_TRAP: "<%s>"

**Explanation** This trap is generated when an unknown subscriber is not identified even after the maximum number of retries.

**Recommended Action** None.

**Error Message** VASSERVER\_OPERATIONALSTATUS\_CHANGE\_TRAP: "<%s>"

**Explanation** This trap is generated when an agent entity detects that the VAS server's operational status has been changed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PORT\_OPERSTATUS\_CHANGE\_TRAP : "<%s>"

**Explanation** This trap is generated to indicate that there is a change in link status, that is, link is up or link is down.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MODULE\_OPER\_STATUS\_CHANGE : "<%s>"

**Explanation** This trap is generated to indicate the update redundancy status.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EM\_AGENT\_GENERIC\_TRAP: "<%s>"

**Explanation** This is a generic SNMP trap in the Enterprise manager agent.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MODULE\_OPER\_STATUS\_CHANGE: "<%s>"

**Explanation** This SNMP trap is generated when a module's operational status is changed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MODULE\_LOST\_REDUNDANCY: "<%s>"

**Explanation** This SNMP trap is generated when module redundancy is lost in Cisco SCE.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MODULE\_REDUNDANCY\_CONF\_MISMATCH: "<%s>"

**Explanation** This SNMP trap is generated when there is a mismatch in the configuration with module redundancy of Cisco SCE.

**Recommended Action** None.

**Error Message** %LOCAL7-6-MPLS\_VPN\_HW\_MAPPINGS\_EXCEEDED: "<%s>"

**Explanation** This SNMP trap is generated when Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) mappings exceed the limit.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVED\_KEYS: "SSH keys were removed."

**Explanation** This message is generated when the SSH keys are removed successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_ACCEPTED: "A telnet session from <%s> was established."

**Explanation** This message is generated when a telnet session is started successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_DENIED: "A telnet request from <%s> was denied - IP address not in ACL."

**Explanation** This message is generated when a telnet access is denied because of the corresponding IP address not being available in the Access Control List (ACL).

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_DENIED\_NO\_PASSWORD: "A telnet session from <%s> was terminated - user password not supplied."

**Explanation** This message is generated when a telnet access is denied because of the user password has not been received.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SESSION\_ENDED: "A telnet session from <%s> ended."

**Explanation** This message is generated when a telnet session is terminated successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DENIED\_NEW\_REQUEST: "An HTTP request from <%s> has been denied - IP address not in ACL."

**Explanation** This message is generated when a web server access request is denied because the IP address is not available in the ACL.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SM\_CONNECTION\_UP\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the Subscriber Manager connection is up.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SM\_CONNECTION\_DOWN\_TRAP: "<%s>"

**Explanation** This SNMP trap is generated when the Subscriber Manager connection is down.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SERVER\_STARTED: "SSH server started."

**Explanation** This message is generated when the RPC server is successfully started.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SERVER\_STOPPED: "SSH server stopped."

**Explanation** This message is generated when the RPC server is stopped successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-GENERATED\_KEYS: "Generated a new set of SSH keys."

**Explanation** This message is generated when the SSH keys get generated successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VLAN\_ADDED: "Added new management vlan %u"

**Explanation** This message, which is specific to Cisco SCE 8000, is generated when a new management VLAN interface is added. A virtual interface named bond0.vlanId is created during this action.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VLAN\_REMOVED: "Removed management vlan %u"

**Explanation** This message, which is specific to Cisco SCE 8000, is generated when an existing management VLAN interface named bond0.VlanId is removed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VLAN\_ASSIGN\_IP: "Assigned ip address

**Explanation** This message is generated when an IPv4 address is assigned to the management VLAN interface and the Cisco SCE routing table is updated with the newly added address.

**Recommended Action** None.

**Error Message** %LOCAL7-6-OSFP\_INFO\_MESSAGE: "<%s>"

**Explanation** This message is generated when the generic OSFP informational message is displayed when the signature file is loaded and processed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-INIT\_OK: "Subscriber database manager initialized successfully."

**Explanation** This message is generated when a subscriber database containing the corresponding address table, unmapped party table, and party table are initialized successfully as part of party database manager initialization.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CLOSED: "Party data base was closed."

**Explanation** This message is generated when all the party-related record files are closed as part of a system reboot or because of a watchdog failure.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXECUTE\_PARTY\_FILE\_INFO1: "executePartyFile() <%s>."

**Explanation** This message is generated when timeout occurs while waiting for another task to complete the related operation. This informational message is displayed when Cisco SCOS tries to execute the party and mapping files.

**Recommended Action** None.

**Error Message** %LOCAL7-6-REMOVING\_ALL\_INTRODUCED\_MAPPING: "Removing all introduced subscriber' mappings."

**Explanation** This message is displayed to indicate that all the externally introduced subscriber mappings have been removed from the database.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_SM\_CON\_STATE\_UP: "Subscriber Manager connection is up<%s>"

**Explanation** This message is generated when the Subscriber Manager connection is up. However, the status depends on the Subscriber Manager connection failure action.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_SM\_CON\_STATE\_DOWN: "Subscriber Manager connection is down, configured action is '<%s>'."

**Explanation** This message is generated when the Subscriber Manager connection is down. Configured action may be one of the following states: remove-mappings, Shut (and Remove-Mappings), force-failure, or none.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_SM\_ACTION\_CHANGED: "Subscriber Manager connection-failure action set to '<%s>'."

**Explanation** This message is generated when the Subscriber Manager connection failure action is changed to remove-mappings, force-failure, or none.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHANGE\_MODE\_AUTO: "Management Failover mode has been changed to automatic mode."

**Explanation** This message is generated when the management failover mode is changed to automatic mode.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CHANGE\_MODE\_MANUAL: "Management Failover mode has been changed to manual mode."

**Explanation** This message is generated when the management failover mode is changed to manual mode.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SIMBA\_USR\_HW\_MONITOR\_OK: "<%s>"

**Explanation** This message is displayed when any of the hardware component statuses change from the error state or warning state to the normal state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SIMBA\_USR\_ALL\_HW\_MONITORS\_OK: "All hardware monitors report status OK"

**Explanation** This message is generated when the status of all the hardware components that are monitored by the sanity check change from the error state or warning state to the normal state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PROBLEM\_IS\_OK: "<%s>"

**Explanation** The system operational status indicates the current status of the system. This message is displayed to indicate that the operational status mentioned in the description is not severe.

**Recommended Action** None.

**Error Message** %LOCAL7-6-EXECUTING\_CONFIG\_FILES: "Beginning execution of configuration files."

**Explanation** This message is displayed when the execution of the startup configuration, application configuration, and party database configuration files begins.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CONFIG\_FILES\_OK: "Configuration files executed with no errors."

**Explanation** This message is generated when all the startup configuration files are executed without any errors during the system boot process.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SSH\_ERROR: "Failed starting SSH server, error is %s."

**Explanation** This message is generated when Cisco SCE fails to start the SSH server during the system boot process that is mentioned in the error description.

**Recommended Action** None.

**Error Message** %LOCAL7-6-OPERATIONAL\_STATUS\_CHANGED: "<%s>"

**Explanation** This message is generated when the system operational status is changed as mentioned in the description.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LOSS\_OF\_SYNC: "Lost synchronization with peer '<%s>' - removing its subscribers"

**Explanation** This message is triggered by the Service Control Management Protocol (SCMP) engine when it detects the loss of synchronization with the peer identified by the corresponding peer name. Cisco SCE removes all the events sent to the peer connection and all the subscribers owned by that peer connection.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_CONNECTED: "Connection established with peer '<s>'"

**Explanation** This message is displayed when connection with the corresponding peer is established.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_CLOSE: "Closing connection with peer '<s>' - <s>"

**Explanation** This message is generated when any of the following conditions occur:

- When a user requests that a debug be closed.
- When a user requests that the connection be closed.
- When the SCMP engine is disabled.
- When Cisco SCE becomes the standby engine in the SCMP engine.
- When a keepalive session timeout occurs.
- When a peer-indicated connection is down.
- When the peer configuration is changed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_DISCONNECTED: "Lost connection with peer '<s>'"

**Explanation** This message is generated when connection with the corresponding peer is lost.

**Recommended Action** None.

**Error Message** %LOCAL7-6-KA\_RETRY\_EXCEEDED: "Keep-alive retries exceeded for peer '<s>' "

**Explanation** This message is generated when a keepalive message exceeds the maximum number of retries.

**Recommended Action** None.

**Error Message** %LOCAL7-6-PEER\_INDICATED\_DISCONNECTED: "Peer '<s>' replied that the connection is down"

**Explanation** This message is generated when the responses to the keepalive packets are received because the peer connection is down.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DB\_ENTRY\_HAS\_CHANGED: "database entry IP: %s vlan: %s MAC has changed from %s to %s"

**Explanation** This message is displayed when the MAC address is changed. This message shows that the MAC address has been changed from <old MAC> to <new MAC>.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DB\_ENTRY\_STATIC\_MAC\_IS\_DIFFERENT: "database static entry IP

**Explanation** This message is generated when the MAC address is static and the MAC address that is received is different from the current MAC address.

**Recommended Action** None.

**Error Message** %LOCAL7-6-INIT\_FC: "Flow data-base (FC) initialized"

**Explanation** This message is generated when the flow context database is initialized.

**Recommended Action** None.

**Error Message** %LOCAL7-6-ACTIVATE\_FC: "Flow data-base (FC) activated. Containing %d flows"

**Explanation** This message indicates that the flow context database is activated for RUC\_MaxFlowContexts flows.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SET\_CONFIG: "Set connection-mode: connection mode is: %s, box priority is: %s, fail-over mode is: %s, physically-connected link group is: %lu

**Explanation** This message indicates the redundancy connection mode set on the SCE, and other details, such as box priorities, the failover mode, and the physically connected link group.

**Recommended Action** None.

**Error Message** %LOCAL7-6-STATE\_TRANSITION: "state changed from <%s> to <%s>."

**Explanation** This message is generated when there is a change in the state of the Cisco SCE cascade topology from the present state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-USER\_FAILOVER: "Redundancy: User failover = %d."

**Explanation** This message indicates whether a user has requested for the failover or not. 0 indicates false and 1 indicates true.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SM\_CONNECTION\_STATUS\_CHANGE: "Redundancy: SM connection status changed from %s to %s."

**Explanation** This message is displayed to indicate that the Subscriber Manager connection state has changed and consequently, the log information state has also changed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SM\_FAILOVER: "Redundancy: SM connection status is down while up in peer box."

**Explanation** This message is displayed to indicate that the Subscriber Manager connection is down due to a session timeout. The connection status is verified in the cascade connection when the present Cisco SCE platform does not have the Subscriber Manager connection and tries to activate another Cisco SCE platform connection.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SM\_TAKEOVER: "Redundancy: SM connection status is up while down in peer box."

**Explanation** This message is displayed to indicate that the Subscriber Manager connection is down due to the session timeout. The connection status is verified in the cascade connection when one of the Cisco SCE platforms has the Subscriber Manager connection and tries to verify another Cisco SCE platform connection.

**Recommended Action** None.

**Error Message** %LOCAL7-6-SYSTEM\_CHANGE\_TO\_STANDBY: "Redundancy: User request - changed system to standby."

**Explanation** In the cascade state machine, this message is displayed to indicate that the system state has changed from the active state to the standby state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-FOUND\_NO\_IMPROPER\_CONNECTIONS :  
"RedundancyManager:Previously found improper cascade connections are now fixed/disconnected."

**Explanation** This message is displayed to indicate that no improper connections are indicated from the Remote Procedure Call (RPC) layer.

**Recommended Action** None.

**Error Message** %LOCAL7-6-NOTIFY\_USER\_EVENT\_ON: "Started filtering packets of type '%s' received on interface # %d (<%s>). module # %d. Reason

**Explanation** This message indicates that the attack filter event has occurred and starts filtering the given types of packets on the corresponding interface.

**Recommended Action** None.

**Error Message** %LOCAL7-6-NOTIFY\_USER\_EVENT\_OFF: "Stopped filtering packets of type '<%s>' received on interface # %d (<%s>). module # %d. Reason

**Explanation** This message indicates that an attack filter event has occurred, and stops filtering the given type of packets on the corresponding interface.

**Recommended Action** None.

**Error Message** %LOCAL7-6-UNFORCE\_LINK\_DOWN: "Link on port %d is unforced down."

**Explanation** This message is displayed when the link on a specific port is in the unforced down state.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_LC\_GROUP\_IS\_ACTIVE : "VAS Server Group %lu is now operative"

**Explanation** This message is displayed when the VAS server group becomes operational.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_LC\_SERVER\_IS\_UP: "VAS server %lu is UP"

**Explanation** This message is displayed when the VAS server is up.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_LC\_DETECTED\_VAS\_LINK\_FAILURE: "Detected a VAS failure on link %lu, switching VAS traffic to the other link"

**Explanation** This message is displayed when a VAS failure is detected on a given link and the VAS traffic is switched to another link.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_LC\_CHANGE\_TRAFFIC\_LINK\_OK : "VAS traffic link has been set to link %lu"

**Explanation** This message is generated when the VAS traffic link has been set to a given link.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_SERVER\_LOG\_EVENT\_STATE\_INIT: "Vas Health Check Monitor

**Explanation** This message is generated when the VAS health check monitor for a given VAS server is initialized.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_SERVER\_LOG\_EVENT\_STATE\_NOT\_CHECKED: "Vas Health Check Monitor

**Explanation** This message is generated when the VAS health check monitor for a given VAS server is stopped.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_SERVER\_LOG\_EVENT\_STATE\_UP: "Vas Health Check Monitor

**Explanation** This message is displayed to indicate that the VAS health check monitor state is up.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_SERVER\_LOG\_EVENT\_NO\_VLAN: "Vas Health Check Monitor

**Explanation** This message is generated when Cisco SCE is unable to run the VAS health check monitor for a given VAS server because the VLAN tag for the server is missing.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_MONITOR\_SET\_FF\_RULE : "Handling all UDP traffic in IP range of 0x%x

**Explanation** This message is displayed when you set the flow-filter configuration of the VAS health check for the UDP traffic in a given subscriber-side IP range.

**Recommended Action** None.

**Error Message** %LOCAL7-6-VAS\_HC\_MONITOR\_CLEAR\_FF\_RULE : "Removed special handling of all UDP traffic in IP range of 0x%x

**Explanation** This message is displayed when you set the flow-filter configuration of the VAS health check for the UDP traffic in a given subscriber-side IP range.

**Recommended Action** None.

**Error Message** %LOCAL7-6-LC\_INIT\_COMPLETED: "General RuC initialization completed"

**Explanation** This debug message is displayed when linecard initialization is completed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-RUC\_INIT\_COMPLETED: "RuC specific initialization completed"

**Explanation** This debug message is displayed to indicate that the initialization of a specific Traffic Processor or Master Processor is completed.

**Recommended Action** None.

**Error Message** %LOCAL7-6-CPLD\_POWER\_BOOT: "Power-down boot identified (CPLD) "

**Explanation** This debug message is displayed on a user log when the complex programmable logic device (CPLD) powers up successfully.

**Recommended Action** None.

**Error Message** %LOCAL7-6-DUMMY\_USER\_INFO: "Dummy Info User Message"

**Explanation** This is a dummy user informational message.

**Recommended Action** None.

**Error Message** %LOCAL7-6-APP\_MAIN\_STARTED: "SCE Application main process starting init phase."

**Explanation** This debug message is displayed when the Cisco SCE application's main process starts the initialization phase.

**Recommended Action** None.

## Warning Messages, Severity Level 4

**Warning Message** %LOCAL7-4-DBG\_FLUSH\_FILES\_FAILED: "DBG failure

**Explanation** This message is generated when an error occurs while flushing the current debug or statistics log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SCROLL\_TO\_END\_FAILED: "DBG failure

**Explanation** This message is generated when an error occurs while scrolling the current DBG log file till the end.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_FILL\_HEADER\_FAILED: "DBG failure: Failed to fill header."

**Explanation** This message is generated when a user tries to perform a write operation of a header for the DBG or statistics log file that does not exist.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SET\_STATE\_FAILED: "DBG failure

**Explanation** This warning message is displayed when a user tries to change the state of a DBG or statistics log file that does not exist.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SCROLL\_TO\_NEXT\_FAILED1: "DBG failure

**Explanation** This message is generated when the current DBG or statistics log file cannot be opened when a user tries to scroll the file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SCROLL\_TO\_NEXT\_FAILED1: "DBG failure

**Explanation** This message is generated when the current DBG or statistics log file does not open when a user tries to scroll the file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SCROLL\_TO\_NEXT\_FAILED2: "DBG failure

**Explanation** This message is generated while reopening a DBG or statistics log file after closing a DBG or statistics log file with memory size exceeding the maximum limit.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_REFRESH\_PROBLEM: "DBG problem

**Explanation** This message is generated when an error occurs while refreshing the DBG or statistics log file. The old logs are deleted and new logs are created automatically.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_REFRESH\_FAILED: "DBG failure

**Explanation** This message is generated while deleting the debug device when the corresponding file cannot be recovered even after refreshing the debug log file or the statistics log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_MESSAGE\_FAILED\_WRITE: "DBG message failed - failed to write message"

**Explanation** This message is generated when an error occurs while performing a write operation in the DBG or statistics log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_MESSAGE\_FAILED\_WRITE: "DBG message failed - failed to write message"

**Explanation** This warning message is generated when an error occurs while performing a write operation in the DBG or statistics log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_CLEAR\_FAILED: "DBG failure"

**Explanation** This message is generated when an error occurs while clearing the log messages in the DBG or statistics log files or while clearing the histogram files.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_OPEN\_FILES: "DBG Init failure"

**Explanation** This message is generated while opening new files for logging failure cases.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_OPEN\_HIST\_FILES: "DBG Init failure"

**Explanation** This message is generated when failure occurs while opening a new histogram file or an existing histogram file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_LOAD\_HIST\_FILES: "DBG Init failure: Failed loading histogram file (bad file or format)."

**Explanation** This message is generated when Cisco SCE fails to load the watermarks from the histogram file due to the following reasons:

- Failed to read and find the histogram file.
- Watermark found, but failed to be removed from the message hash.
- Watermark not found in the histogram file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_HEADERS\_CORRUPTED1: "DBG Init problem

**Explanation** This message is generated when the header obtained from the first debug log file is corrupted even if the file is not in the full, empty, or active state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_AFTER\_HC1: "DBG Init failure

**Explanation** This message is generated when there is an unsuccessful attempt to open or create a new debug file, and this operation is attempted when there is an error in the header obtained from the first debug log file because it is corrupted, that is, the file is not in the full, empty, or active state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_HEADERS\_CORRUPTED2: "DBG Init problem

**Explanation** This message is generated when the header obtained from the second debug log file is corrupted, that is, the file is not in the full, empty, or active state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_AFTER\_HC2: "DBG Init failure

**Explanation** This warning message is generated when the open or create operation of a new debug file fails. This operation is attempted when there is an error in the header obtained from the second debug log file because it is corrupted, that is, the file is not in the full, empty, or active state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_BOTH\_FULL: "DBG Init problem

**Explanation** This message is generated when the status of the headers obtained from both the debug log files are in the full state. Close the existing files and create or open a new file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_AFTER\_BF: "DBG Init failure

**Explanation** This message is generated when the create or open operation of a new file fails when the existing file is closed, with the status of the headers obtained from both the debug log files in the full state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_BOTH\_ACTIVE: "DBG Init problem

**Explanation** This message is generated when the status in the headers obtained from both the debug log files are in the active state. Close the existing second file and create a new first file or open an existing first file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_FAILED\_AFTER\_BA: "DBG Init failure

**Explanation** This message is generated when the task of creating or opening a new file fails after the existing log file is closed and when the status of the headers obtained from both the debug log files are in the full or active state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_DEVICE\_CREATION\_FAILED: "DBG Init failure

**Explanation** This message is generated when the creation of a logger device fails.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_SCROLL\_TO\_END\_FAILED: "DBG Init failure

**Explanation** This message is generated when the scrolling operation to the end of the file fails.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_INIT\_SCROLL\_TO\_NEXT\_FAILED: "DBG Init failure

**Explanation** This message is generated due to the following reasons:

- The log file is not available and the creation of a new file fails.
- The space in the file is not enough for the next message, and the creation of a new file fails.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_CLOSE\_FAIL\_SAVE\_HIST\_FILES: "DBG Close failure

**Explanation** This message is generated while closing the histogram file due to the following reasons:

- When the histogram file is not open.
- When there is no attempt to close the histogram file if it is already open.
- When serialization of a log fails or the histogram file fails while saving the file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_FLUSH\_FILES\_FAILED: "User log

**Explanation** This message is generated when the task of flushing a user log fails.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_SCROLL\_TO\_END\_FAILED: "User log

**Explanation** This message is generated when a user log file reaches the maximum file size.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_SECURE\_FILES\_FAILED: "User log

**Explanation** The message is generated when an error occurs while opening a user log file, which is in binary format, in read mode.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_SCROLL\_TO\_NEXT\_FAILED1: "User log

**Explanation** This message is generated when a file is inactive or an error occurs on opening the corresponding user log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_SCROLL\_TO\_NEXT\_FAILED2: "User log: Failed to scroll - closed a full file and couldn't reopen."

**Explanation** This warning message is generated when the existing user log file fails to reopen.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_INIT\_SCROLL\_TO\_END\_FAILED: "User log init failure

**Explanation** This message is generated when failure occurs while opening a user log file or when a user scrolls the file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-USER\_INIT\_SCROLL\_TO\_NEXT\_FAILED: "User log init failure

**Explanation** This message is generated when a user log file is in the inactive state and an error occurs while opening this log file or when the user log file is active and a blank space is available, but fails to open the file for writing.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-FOUND\_IMPROPER\_CONNECTIONS "RedundancyManager

**Explanation** This message is generated when the redundancy manager finds an improper cascade connection, with the ports being connected to the wrong ports on the peer box.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-LINK\_DOWN\_DETECTED "Link failure reflection

**Explanation** This message is generated when the link on a port is down and reflection gets activated.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-LINK\_DOWN\_DETECTED\_ON\_ALL\_PORTS "Link failure reflection on all ports

**Explanation** This message is generated when the link on a port is down and reflection gets activated on all the ports.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-FORCE\_LINK\_DOWN "Link failure reflection

**Explanation** This message is generated when link-failure reflection occurs when the link on a port is forced down by another port.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-FORCE\_LINK\_DOWN\_ON\_ALL\_PORTS "Link failure reflection on all ports

**Explanation** This message is displayed when link-failure reflection occurs on all the ports. The link on one port is forced down by another port.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-LIC\_AWARE\_ACTIVE "No Link reflection is done due two ports %d and %d on the same link are down and linecard aware mode is active"

**Explanation** This message is displayed because no link reflection occurs because two ports on the same link are down and the linecard-aware mode is active.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-ILLEGAL\_PACKET\_IN\_VAS\_HC\_RANGE "Got a packet on VAS Health Check IP range which does not match health check packet format. This may indicate a WRONG configuration"

**Explanation** This message is displayed because the packet that is obtained is not in the VAS health check IP range and does not match the health check packet format.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-VAS\_MIRROR\_PACKET\_BACK "Got a packet from a VAS server with VLAN tag %u, this packet was originally mirrored by the SCE. This may indicate a WRONG configuration"

**Explanation** This message is displayed because the packet obtained from the VAS server is a packet mirrored by Cisco SCE.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-VAS\_LC\_GROUP\_IS\_IN\_FAILURE "VAS Server Group %lu is in Failure state"

**Explanation** This message is displayed when the VAS server group is in the failure state.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-VAS\_LC\_SERVER\_IS\_DOWN "VAS server %lu is DOWN"

**Explanation** This message is displayed when the VAS server is down.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-VAS\_HC\_SERVER\_LOG\_EVENT\_STATE\_DOWN "Vas Health Check Monitor: NO vital signs from VAS server %lu."

**Explanation** This message is displayed when the VAS Health Check Server state is DOWN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-VAS\_HC\_SERVER\_LOG\_EVENT\_NO\_IPS "Vas Health Check Monitor

**Explanation** This message is displayed when the VAS Health Check Monitor does not run the check for the VAS server.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-STANDBY\_VIOLATION: "Subscriber operations are not permitted on standby box - discarding operation"

**Explanation** This message is displayed when the subscriber-related commands are executed when the Cisco SCE is on the standby mode.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DEBUG\_TELNET\_ACCESS\_FAILED: "Fail to <%s> debug-telnet (port 2300) "

**Explanation** This message is displayed when Cisco SCE fails to enable debug telnet access from the remote machines.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DEBUG\_SHELL\_ACCESS\_FAILED: "Fail to <%s> debug-shell (port 2301) "

**Explanation** This message is displayed when Cisco SCE fails to enable Cisco SCOS shell access from the remote machines.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DEBUG\_SSH\_ACCESS\_FAILED: "Fail to %s debug-ssh (port 2200) "

**Explanation** This message is displayed when Cisco SCE fails to enable Cisco SCOS SSH access from the remote machines.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-BIND\_VTY\_SERVICE\_FAILED: "Fail to bind telnet service to management vlan (%u) and address (<%s>)"

**Explanation** This message is displayed when the Cisco SCE fails to bind the telnet service to a corresponding management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-UNBIND\_VTY\_SERVICE\_FAILED: "Fail to un-bind telnet service from management vlan (%u) "

**Explanation** This message is displayed when Cisco SCE fails to unbind the telnet service from the corresponding management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-BIND\_SSH\_SERVICE\_FAILED: "Fail to bind ssh service to management vlan (%u) and address (<%s>)"

**Explanation** This message is displayed when Cisco SCE fails to bind the SSH service to a given management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-UNBIND\_SSH\_SERVICE\_FAILED: "Fail to un-bind ssh service from management vlan (%u)"

**Explanation** This message is displayed when Cisco SCE fails to unbind the SSH service to a given management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-BIND\_SNMP\_SERVICE\_FAILED: "Fail to bind SNMP service to management vlan (%u) and address (<%s>)"

**Explanation** This message is displayed when Cisco SCE fails to bind the SNMP service to a given management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-UNBIND\_SNMP\_SERVICE\_FAILED: "Fail to un-bind SNMP service from management vlan (%u)"

**Explanation** This message is displayed when Cisco SCE fails to unbind the SNMP service to a given management VLAN.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-HOSTNAME\_NOT\_FOUND: "Formatter connection host name was not found"

**Explanation** This message is displayed when the formatter connection of the corresponding host name is not found.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-LOGGER\_USER\_WARN\_MSG: "<%s>"

**Explanation** This message is displayed when a warning message is added to a user log file.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_SECURE\_FILES\_FAILED: "DBG failure: Failed to secure DBG files."

**Explanation** This message is generated when Cisco SCE fails to ensure that the dbg file exists and is not corrupt.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_MESSAGE\_MASKED: "DBG masked message - severity = %d , module = %u"

**Explanation** This message is generated when Cisco SCE tries to write a masked debug message with a given severity, from the corresponding module to the debug log.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_MESSAGE\_FAILED\_NO\_FILE: "DBG message failed - no file attached"

**Explanation** This message is displayed when Cisco SCE tries to write a file that does not exist.

**Recommended Action** None.

**Warning Message** %LOCAL7-4-DBG\_MESSAGE\_FAILED\_SCROLL: "DBG message failed - failed to scroll to next"

**Explanation** This warning message is displayed when Cisco SCE archives the existing file and fails to open a new file in place of the existing file.

**Recommended Action** None.

**Warning Messages, Severity Level 4**