



CHAPTER 7

Configuring the Connection

Revised: February 15, 2011, OL-19896-07

Introduction

- [Configuring the Connection Mode, page 7-2](#)
- [Monitoring the Connection Mode and Related Parameters, page 7-3](#)
- [Configuring the Link Mode, page 7-6](#)
- [External Optical Bypass, page 7-7](#)
- [Link Failure Reflection, page 7-9](#)
- [Asymmetric Routing Topology, page 7-10](#)
- [Configuring a Forced Failure, page 7-11](#)
- [Configuring the Failure Recovery Mode, page 7-12](#)
- [Configuring the SCE Platform/SM Connection, page 7-13](#)



Note

For more information regarding the physical installation of the Cisco SCE8000 platform and cabling the connections, refer to the [Cisco SCE8000 GBE Installation and Configuration Guide](#) and in particular, the following sections:

- [Information About the SCE Platform](#) (illustrations of modules and information regarding LEDs and interfaces)
 - [The Cisco SCE8000 Optical Bypass](#) (information regarding the optical bypass module)
 - [Physical Topologies](#) (topology diagrams)
 - [Connecting the Line Ports to the Network](#) (cabling charts and diagrams)
-

Configuring the Connection Mode

The connection mode command allows you to configure the topology of the system in one command. The connection mode is determined by the physical installation of the SCE platform.



Caution

This command can only be used if the line card is in either **no-application** or **shutdown** mode. If an application is installed on the SCE platform, the command will fail with an error message and help instructions.

Options

The following topology-related parameters are included in the connection mode command. Note that some options are relevant for cascaded topologies only.

- **Connection mode** — Can be any one of the following, depending on the physical installation of the SCE platform:
 - Inline — single SCE platform inline
 - Receive-only — single SCE platform receive-only
 - Inline-cascade — two cascaded SCE platforms inline
 - Receive-only-cascade — two cascaded SCE platforms receive-only

Default — **inline**

- **sce-id** — In cascaded topologies, identifies the SCE platform, which in turn identifies the traffic links. Traffic links 0-7 are assigned to one SCE platform and links 8-15 are assigned to the other. These link numbers are used in the SCA BB Reporter reports as well as in the Global Control configuration menu in the SCA BB console.

Possible values are '0' and '1'.

Not applicable to single SCE platform topologies.
- **Priority** — This parameter defines which is the primary SCE platform. It is applicable only in a two SCE platform topology.

Possible values are 'primary' and 'secondary'

Not applicable to single SCE platform topologies.
- **On-failure** — This parameter determines the behavior of the system when the SCE platform either has failed or is booting:
 - cut the traffic (cutoff)
 - bypass the traffic (bypass)
 - automatically direct traffic through the external bypass module (external-bypass)

Default:

- inline mode: **external-bypass**
- inline-cascade mode: **bypass**

Not applicable to receive-only topologies.

**Note**

Do not change the connection mode unless the physical installation has been changed.

- Step 1** From the SCE(config if)# prompt, type **connection-mode (inline | receive-only | inline-cascade | receive-only-cascade) [sce-id (0|1)] [priority (primary | secondary)] on-failure (bypass|external-bypass|cutoff)** and press **Enter**.

Configuring the Connection Mode Examples

Example 1

This example defines a primary Cisco SCE8000 in a cascaded inline topology. This device is designated as SCE platform '0', and the link mode on failure is bypass (default).

```
SCE(config if)#connection-mode inline-cascade sce-id 0 priority primary
```

Example 2

This example defines a single-SCE platform, dual link, receive-only topology. The link mode **on-failure**, **sce-id**, and **priority** options are not applicable.

```
SCE(config if)#connection-mode receive-only
```

Monitoring the Connection Mode and Related Parameters

How to View the Current Connection Mode

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

Monitoring the Connection Mode: Examples

The following example shows the current configuration of the connection mode for a single platform.

```
SCE>enable 5
Password:<cisco>
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
SCE>
```

The following example shows the current configuration of the connection mode for a cascaded system.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 connection-mode
Slot 0 connection mode
Connection mode is inline-cascade
slot 0 sce-id is 1
slot 0 is secondary
slot 0 is connected to peer
slot failure mode is bypass
Redundancy status is active
SCE>
```

How to View the SCE-ID

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

Viewing the SCE-ID: Example

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 sce-id
slot 0 sce-id is 1
```

How to View the Current Link to Port Mappings

Step 1 From the SCE> prompt, type **show interface linecard 0 link-to-port-mapping** and press **Enter**.

Viewing the Current Link to Port Mappings: Example

The following example shows the link-to-port mapping.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 link-to-port-mapping
Link Id      | Upstream Port (Subscribers) | Downstream Port (Network)
-----|-----|-----
0            | 0/3/0/0                     | 0/3/0/1
1            | 0/3/0/2                     | 0/3/0/3
2            | 0/3/0/4                     | 0/3/0/5
3            | 0/3/0/6                     | 0/3/0/7
4            | 0/3/1/0                     | 0/3/1/1
5            | 0/3/1/2                     | 0/3/1/3
6            | 0/3/1/4                     | 0/3/1/5
7            | 0/3/1/6                     | 0/3/1/7
8 (cascade) | 1/3/0/0                     | 1/3/0/1
9 (cascade) | 1/3/0/2                     | 1/3/0/3
10 (cascade)| 1/3/0/4                     | 1/3/0/5
11 (cascade)| 1/3/0/6                     | 1/3/0/7
12 (cascade)| 1/3/1/0                     | 1/3/1/1
13 (cascade)| 1/3/1/2                     | 1/3/1/3
14 (cascade)| 1/3/1/4                     | 1/3/1/5
15 (cascade)| 1/3/1/6                     | 1/3/1/7
SCE>
```

How to View the Current Redundancy Status of the SCE Platform

-
- Step 1** From the SCE> prompt, type **show interface linecard 0 cascade redundancy-status** and press **Enter**.
-

Viewing the Current Redundancy Status of the SCE Platform: Example

The following example shows typical output of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade redundancy-status
Redundancy status is active
```

How to View Information about the Peer SCE Platform

-
- Step 1** From the SCE> prompt, type **show interface linecard 0 cascade peer-sce-information** and press **Enter**.
-

Viewing Information about the Peer SCE Platform: Example

The following example shows typical output of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade peer-sce-information
Peer SCE's IP address is 10.10.10.10
```

How to View Information about the Cascade Connections

-
- Step 1** From the SCE> prompt, type **show interface linecard 0 cascade connection-status** and press **Enter**.
-

Monitoring the Connection Status: Examples

The following example shows the output of this command in the case of two cascaded Cisco SCE8000 GBE platforms where the cascade interfaces have not been connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade connection-status
SCE is improperly connected to peer SCE
Please verify that each cascade port is connected to the correct port of the peer SCE.
Note that in the current topology, the SCE must be connected to its peer as follows:
Port 3/2/0 must be connected to port 3/2/0 at peer
Port 3/3/0 must be connected to port 3/3/0 at peer
SCE>
```

The following example shows the output of this command in the case of two cascaded SCE platforms where the cascade interfaces have been connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade connection-status
SCE is connected to peer SCE
SCE>
```

Configuring the Link Mode

About the Link Mode

The SCE8000-SIP jacket card can work in one of three link modes:

- 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. (Note that this is only relevant to inline topologies even though the configuration is available also when in receive-only mode.)

Options

The following link mode options are available:

- **Forwarding** — forwards traffic to the SCE platform for processing.
- **Bypass** — stops all forwarding of traffic to the SCE platform. Traffic still flows through the SCE platform, but is not processed by it in any way.
This does not affect the redundancy states.
- **Cutoff** — completely cuts off flow of traffic through the SCE platform.

Recommendations and restrictions

Note the following recommendations and restrictions:

- For the Cisco SCE8000 platform, the link mode setting is global, and cannot be set for each link separately. Therefore the **all-links** keyword must be used.
- Link mode is relevant only to inline topologies.
- The default link mode is forwarding.

When other link modes are selected, active service control is not available and any service control configuration will not be applicable.

- It is recommended that in cascaded topologies, both SCE platforms be configured for the same link mode, otherwise the service will be unpredictable.

-
- Step 1** From the SCE(config if)# prompt, type **link mode all-links (forwardingbypasslcutoff)** and press **Enter**.
-

Monitoring the Link Mode

How to View the Current Link Mode

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

External Optical Bypass

- [How to Activate the External Bypass, page 7-8](#)
- [How to Deactivate the External Bypass, page 7-8](#)
- [How to Set the External Bypass to the Default State, page 7-8](#)
- [How to Display the State of the External Bypass, page 7-9](#)

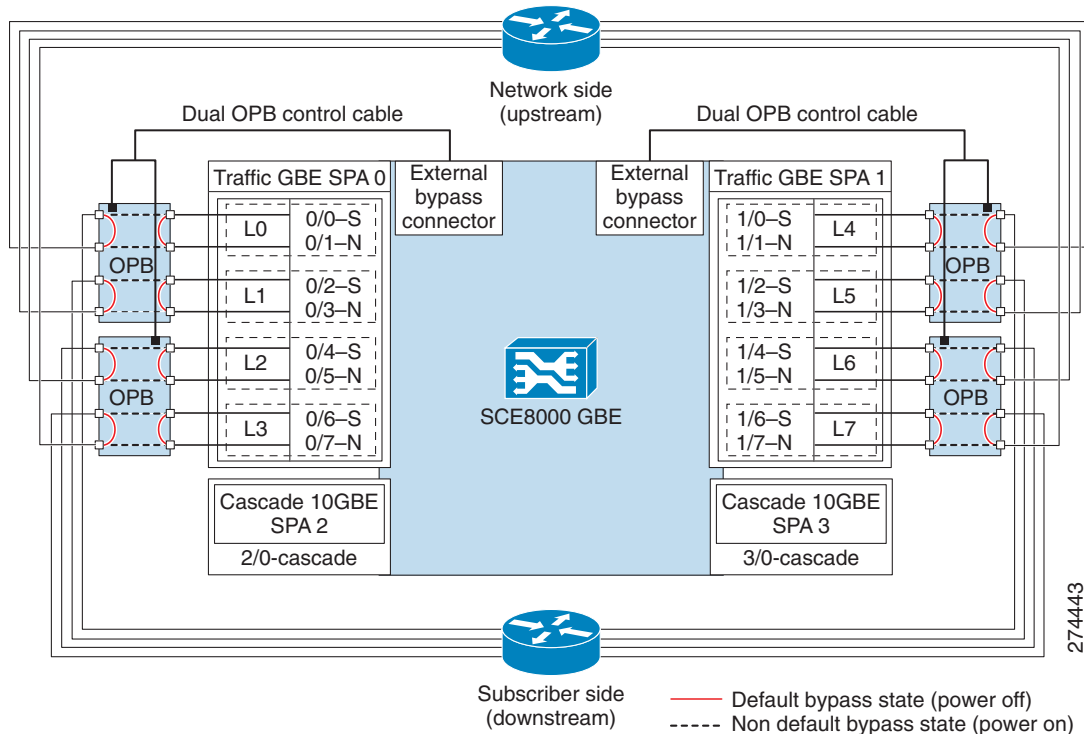
The Cisco SCE8000 supports connection to up to four external optical bypass devices. These protect the line against power failure or total hardware failure, which prevents the hardware card from bypassing the traffic. Each external optical device protects two traffic links passing through the SCE platform. The main objective of the external bypass is to provide automatic redundancy and failover support. However, the user can also manually enable the external bypass, assuming it is connected.

At power failure the external bypass is automatically activated. The external bypass can also be controlled by the software and by hardware in case of software failure.

In case of power failure, the bypass shortcuts the interfaces that are connected to the two sides of the Cisco SCE8000, bypassing all the traffic, as illustrated in [Figure 7-1](#).

The SCE8000 can detect the presence of each external optical bypass device, and warns the user by various means (CLI **show** command, system operational-state, SNMP traps) if an expected external bypass device is not detected as present.

Figure 7-1 External Optical Bypass Connectivity



How to Activate the External Bypass

Step 1 From the SCE(config if)# prompt, type **external-bypass** and press **Enter**.

How to Deactivate the External Bypass

Step 1 From the SCE(config if)# prompt, type **no external-bypass** and press **Enter**.

How to Set the External Bypass to the Default State

The default state of the external optical bypass is deactivated.

Step 1 From the SCE(config if)# prompt, type **default external-bypass** and press **Enter**.

How to Display the State of the External Bypass

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

Output Sample: All Optical Bypass Modules Functional

```
External bypass current state is 'not activated'.  
External bypass failure state is 'activated'.  
Amount of expected external bypass devices: 4 (automatically configured).
```

Output Sample: One Optical Bypass Module Not Detected

```
External bypass current state is 'not activated'.  
External bypass failure state is 'activated'.  
Amount of expected external bypass devices: 4 (automatically configured).  
Warning: External bypass device expected but not detected on link #1
```

Link Failure Reflection

- [How to Enable Link Failure Reflection, page 7-9](#)
- [How to Disable Link Failure Reflection, page 7-9](#)

In some topologies, link failure on one port must be reflected to the related port to allow the higher layer redundancy protocol in the network to detect the failure and function correctly.

The **link failure-reflection** command determines the behavior of the system when there is a link problem. The link failure-reflection command enables reflection of a link failure. Use the **no** form of this command to disable failure reflection on the link.

The default value is **disabled**.

How to Enable Link Failure Reflection

Step 1 From the SCE(config if)# prompt, type **link failure-reflection** and press **Enter**.

How to Disable Link Failure Reflection

Step 1 From the SCE(config if)# prompt, type **no link failure-reflection** and press **Enter**.

Asymmetric Routing Topology

- [Asymmetric Routing and Other Service Control Capabilities, page 7-10](#)
- [Enabling Asymmetric Routing, page 7-10](#)
- [Monitoring Asymmetric Routing, page 7-11](#)

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).

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)
- Classical open flow mode, including the following:
 - Flow-open-mode classical explicitly enabled (ROOT level configuration)
 - Analysis layer transport mode enabled (ROOT level configuration)
 - ‘no TCP bypass-establishment’ mode enabled (ROOT level configuration)
 - A traffic rule is configured for certain flows to use the classical open flow mode (ROOT level configuration)

Enabling Asymmetric Routing

The asymmetric routing mode is disabled by default. It is typically enabled by the SCA-BB application when applying an appropriate service configuration.

Note that the detection of uni-directional flows is done by the SCE platform regardless of the asymmetric routing mode, but the appropriate configuration will assure that the uni-directional flows are properly classified and controlled.

For more information, please see the [Cisco Service Control Application for Broadband User Guide](#).

Monitoring Asymmetric Routing

Use the command below to display the following information regarding asymmetric routing:

- Current status of asymmetric routing mode (enabled or disabled)
- TCP unidirectional flows ratio: the ratio of TCP unidirectional flows to total TCP flows per traffic processor, calculated over the period of time since the SCE platform was last reloaded (or since the counters were last reset).

Step 1 From the SCE> prompt, type **show interface linecard 0 asymmetric-routing-topology** and press **Enter**.

Monitoring Asymmetric Routing: Example

This example shows how to display the current asymmetric routing information.

```
SCE>show interface linecard 0 asymmetric routing-topology
Asymmetric Routing Topology mode is disabled
TCP Unidirectional flows ratio statistics:
=====
Traffic Processor 1   : 0%
Traffic Processor 2   : 0%
Traffic Processor 3   : 0%
Traffic Processor 4   : 0%
Traffic Processor 5   : 0%
Traffic Processor 6   : 0%
Traffic Processor 7   : 0%
Traffic Processor 8   : 0%
Traffic Processor 9   : 0%
Traffic Processor 10  : 0%
Traffic Processor 11  : 0%
Traffic Processor 12  : 0%
```

Note that the statistics are updated only if the system is configured to work in Enhanced Open Flow (i.e. following settings are disabled: Classical Open Flow mode, VAS, TCP no bypass est, etc.). The statistics are updated once every two minutes
SCE>

Configuring a Forced Failure

Use the following commands to force a virtual failure condition, and to exit from the failure condition when performing an application upgrade.

- [How to Force a Virtual Failure, page 7-12](#)
- [How to Exit from a Virtual Failure, page 7-12](#)

How to Force a Virtual Failure

-
- Step 1** From the SCE(config if)# prompt, type **force failure-condition** and press **Enter**.
The system asks for confirmation
- Forcing failure will cause a failover - do you want to continue? n
- Step 2** Type 'Y' and press **Enter** to confirm the forced failure.
-

How to Exit from a Virtual Failure

-
- Step 1** From the SCE(config if)# prompt, type **no force failure-condition** and press **Enter**.
Exits from the virtual failure condition.
-

Configuring the Failure Recovery Mode

The **failure-recovery operation-mode** command defines the behavior of the system after boot resulting from failure.

Options

The following options are available:

- **operational** — after failure, the system will return to operational mode.
- **non-operational** — after failure, the system will remain not operational.

The default value is **operational**.

-
- Step 1** From the SCE(config)# prompt, type **failure-recovery operation-mode operational|non-operational** and press **Enter**.
Specify the desired failure recovery mode.
-

Configure the Failure Recovery Mode: Examples

Example 1

This example sets the system to boot as non-operational after a failure.

```
SCE(config)#failure-recovery operation-mode non-operational
```

Example 2

This example sets the system to the default failure recovery mode.

```
SCE(config)# default failure-recovery operation-mode
```

Configuring the SCE Platform/SM Connection

- [Configuring the Behavior of the SCE Platform in Case of Failure of the SM, page 7-13](#)
- [Configuring the SM-SCE Platform Connection Timeout, page 7-14](#)

The user can configure the behavior of the SCE platform in case of failure of the Subscriber Manager (SM):

- If SM functionality is critical to the operation of the system — configure the desired behavior of the SCE platform if any loss of connection with the SM (may be due either to failure of the SM or failure of the connection itself).
- If SM functionality is not critical to the operation of the system — no action needs to be configured. In this case you can specify that the system operational-status of the SCE platform should be 'warning' when the link is down.

Configuring the Behavior of the SCE Platform in Case of Failure of the SM

Options

The following options are available:

- **action**—The specified action will be performed in case of loss of connection between the SCE platform and the SM.

Possible actions are:

- **force-failure** — Force failure of SCE platform. The SCE platform then acts according to the behavior configured for the failure state.
- **remove-mappings** — Remove all current subscriber mappings.
- **shut** — The SCE platform shuts down and quits providing service.
- **none** (default) — Take no action.
- **warning**—The system operational-status of the SCE platform should be 'warning' in case of loss of connection between the SCE platform and the SM. No action is taken.

To specify the action that the SCE platform will perform if the SCE-SM connection fails, use this command.

-
- Step 1** From the SCE(config if)# prompt, type **subscriber sm-connection-failure action [force-failure|none|remove-mappings|shut]** and press **Enter**.
-

To specify that the system operational-status of the SCE platform should be 'warning' if the SCE-SM connection fails, use this command.

Step 1 From the SCE(config if)# prompt, type **subscriber sm-connection-failure warning** and press **Enter**.

Configuring the SM-SCE Platform Connection Timeout

You can also configure the timeout interval; the length of time that the SM-SCE platform connection is disrupted before a failed connection is recognized and the configured behavior is applied.

Options

The following option is available:

- **interval** — the timeout interval in seconds

Step 1 From the SCE(config if)# prompt, type **subscriber sm-connection-failure timeout *interval*** and press **Enter**.
