Configuring the Connection

Revised: February 07, 2014, OL-24151-11

Introduction

Note For more information regarding the physical installation of the Cisco SCE8000 platform and cabling the connections, see the *Cisco SCE8000 10GBE 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, 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 SCE8000 GBE platform, which supports multiple links. In the SCE8000 10GBE, the number assigned to the sce-id parameter (0 or 1) will be defined as the of number of the physically-connected-link.

Note For backwards compatibility, the physically-connected-link parameter is currently still recognized.

  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)

Note If the *external-bypass* option is configured, two optical bypass devices must be properly connected, one on each link. 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.

Note If the *bypass* option is configured and the connection mode is 'inline-cascade', a single optical bypass device must be connected on link #0 (SPA bays 0 and 1). As explained above, the command is executed, but the system enters warning mode.

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 defines a primary Cisco SCE8000 in a cascaded inline topology. Link 0 is connected to this device, 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

The following table shows the commands used to monitor the connection mode.

Note that the **show** commands are entered in Viewer mode.

Command	Purpose
show interface linecard 0 connection-mode	Displays the connection mode configuration.
show interface linecard 0 sce-id	Displays the SCE-ID.
show interface linecard 0 cascade redundancy-status	Displays the current redundancy status of the SCE platform.
show interface linecard 0 cascade peer-sce-information	Displays information about the peer SCE platform.
show interface linecard 0 cascade connection-status	Displays information about the cascade connections.

Connection Mode Examples

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>
```

Viewing the SCE-ID: Example

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

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
```

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
```

Monitoring the Connection Status: Examples

The following example shows the output of this command in the case of two cascaded Cisco SCE8000 10GBE 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 3/3/0 at peer
Port 3/3/0 must be connected to port 3/2/0 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 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. (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.

From the SCE(config if)# prompt, type:

Command	Purpose
link mode all-links (forwarding|bypass|cutoff)	Enforces a specific desired mode.

External Optical Bypass

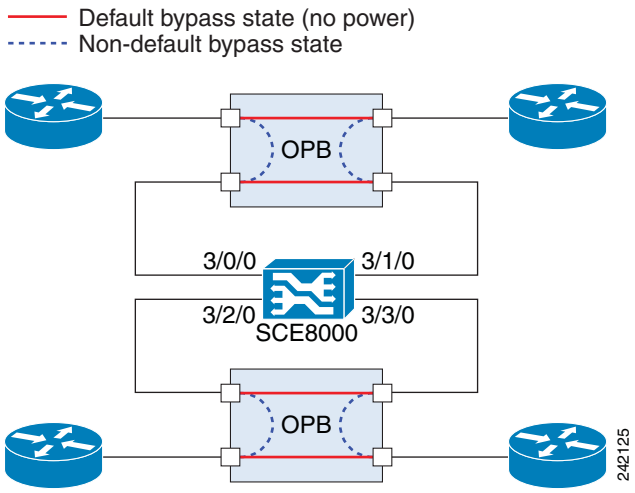
The Cisco SCE8000 supports connection to up to two external optical bypass devices. These protect the line against power failure or total hardware failure, which prevents the hardware card from bypassing the traffic. Each external optical device protects a single traffic link passing through the SCE 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 8-1.

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 8-1 External Optical Bypass Connectivity



How to Activate the External Bypass

From the SCE(config if)# prompt, type:

Command	Purpose
external-bypass	Activates the external bypass.

How to Deactivate the External Bypass

From the SCE(config if)# prompt, type:

Command	Purpose
no external-bypass	Deactivates the external bypass.

How to Set the External Bypass to the Default State

From the SCE(config if)# prompt, type:

Command	Purpose
default external-bypass	Sets the external bypass to the default state. The default state of the external optical bypass is deactivated.

How to Display the State of the External Bypass

From the SCE> prompt, type the following **show** command. Note that the **show** command is entered in the Viewer mode.

Command	Purpose
show interface linecard 0 external-bypass	Displays the state of the external bypass.

Output Sample: Both Optical Bypass Modules Functional

```
External bypass current state is 'not activated'.
External bypass failure state is 'activated'.
Amount of expected external bypass devices: 2 (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: 2 (automatically configured).
Warning: External bypass device expected but not detected on link #1
```

Hardware Bypass

The Cisco SCE8000 platform supports the Hardware Bypass feature. The main objective of this feature is to bypass the traffic of the configured static parties created in the hardware bypass mode at the hardware (SIP module) level, based on their IP address or IP range. By default, the hardware bypass mode is disabled. However, users can enable the hardware bypass mode through the **hw-bypass mode** CLI command.

Note Before performing the party configurations, Engage Service Management Language (SML) 3.7.0 application should be installed in interface linecard configuration mode.

How to Enable the Hardware Bypass Mode

From the SCE(config)#> prompt, type:

Command	Purpose
hw-bypass mode	Enables the hardware bypass mode of the Cisco SCE 8000 platform. It also allows you to set the hardware bypass state for the specified static parties when these parties are configured in this mode.

How to Disable the Hardware Bypass Mode

From the SCE(config)#> prompt, type:

Command	Purpose
no hw-bypass mode	Disables the hardware bypass mode of the Cisco SCE platform. It also allows you to reset the hardware bypass state for the specified static parties when these parties are configured in this mode.

How to Display the Status of the Hardware Bypass Mode

From the SCE(config)#> prompt, type:

Command	Purpose
show hw-bypass mode	Displays the hardware bypass status of the Cisco SCE 8000 platform.

The following example shows how to display the state of the hw-bypass mode:

```
SCE>enable 15
Password:<cisco>
SCE#>show hw-bypass mode
hw-bypass mode is enabled
SCE(config)#>
```

How to Set the Hardware Bypass Status for a Static Party

From the SCE(config)#> prompt, type:

Command	Purpose
party name *party-name* **hw-bypass**	Sets the hardware bypass status for a specified static party in the hardware bypass mode of the Cisco SCE 8000 platform.

How to Reset the Hardware Bypass Status of a Static Party

From the SCE(config)#> prompt, type:

Command	Purpose
no party name *party-name* **hw-bypass**	Resets the hardware bypass status for a specified static party in the hardware bypass mode of the Cisco SCE 8000 platform.

How to Display the Hardware Bypass Status of a Static Party

From the SCE(config)#> prompt, type:

Command	Purpose
show party name *party-name* **hw-bypass**	Displays the hardware bypass state of a specified static party in the hardware bypass mode of the Cisco SCE 8000 platform.

Note The hardware bypass action can be performed only on the static parties created in the hardware bypass mode.

The following example shows how to display the hardware bypass state of a specified static party:

```
SCE>enable 15
Password:<cisco>
SCE#>show party name [party-name] hw-bypass
SCE#> hw-bypass for party "[party-name]" is  disabled
```

How to the Set the IP Address for a Static Party

From the SCE(config)#> prompt, type:

Command	Purpose
party mapping ip-address *ip-address* **name** *party-name*	Sets the IP address for the specified static party in the SCE 8000 platform.

How to Set the IP Range for a Static Party

From the SCE(config)#> prompt, type:

Command	Purpose
party mapping ip-range *ip-address/mask-value* **name** *party-name*	Sets the IP range for a specified static party in the Cisco SCE 8000 platform.

Note If the mask value is not provided for the corresponding IP address, the complete mask value of 32 will be taken into consideration for the specified IP address.

How to Display the Startup Configuration Party Database

From the SCE(config)#> prompt, type:

Command	Purpose
show startup-config-party-db	Displays the contents of the startup configuration party database of the static parties that are configured in the Cisco SCE 8000 platform.

Note The configuration file contents will be displayed only if the corresponding startup configuration party database is copied from the running configuration party database.

The following example shows how to display the contents of the startup party database:

```
SCE>enable 15
Password:<cisco>
SCE#>show startup-config-party-db
#This is a party database configuration file (running-config-party-db) for static parties
only.
#Created on 13:34:02  UTC  TUE  July  12  2011
#cli-type 1
#version 1
hw-bypass mode
party name "N/A"
party name "[party-name]"
party mapping ip-address 24.11.52.128 name [party-name]
party mapping ip-address 110.10.10.10 name [party-name]
party name  [party-name] hw-bypass
SCE#>
```

How to Display the Currently Running Party Database Configuration

From the SCE(config)#> prompt, type:

Command	Purpose
show running-config-party-db	Displays the contents of the currently running party database configuration for the static parties that are configured in the Cisco SCE 8000 platform.

The following example shows how to display the contents of the running party database configuration:

```
SCE>enable 15
Password:<cisco>
SCE#>show running-config-party-db
#This is a party database configuration file (running-config-party-db) for static parties
only.
#Created on 13:34:02  UTC  TUE  July  12  2011
#cli-type 1
#version 1
hw-bypass mode
party name "N/A"
party name "[party-name]"
party mapping ip-address 24.11.52.128 name [party-name]
party mapping ip-address 110.10.10.10 name [party-name]
party name  [party-name] hw-bypass
```

```
SCE#>
```

How to Copy the Running Configuration Party Database to the Startup Configuration Party Database

From the SCE(config)#> prompt, type:

Command	Purpose
copy running-config-party-db startup-config-party-db	Enables the task of copying the currently running configuration party database to the startup configuration party database of the static parties that are configured on the Cisco SCE 8000 platform.

How to Copy the Startup Configuration Party Database and Create a Backup File

From the SCE(config)#> prompt, type:

Command	Purpose
copy startup-config-party-db *backup-file name*	Enables the task of copying the startup configuration party database and create a backup file of the configured static parties in the Cisco SCE 8000 platform.

Link Failure Reflection

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

From the SCE(config if)# prompt, type:

Command	Purpose
link failure-reflection	Enables link failure-reflection.

How to Disable Link Failure Reflection

From the SCE(config if)# prompt, type:

Command	Purpose
no link failure-reflection	Disables link failure-reflection.

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 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, due to the fact that 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, including MPLS VPN. (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)
  - VAS traffic forwarding mode enabled
  - 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).

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 asymmetric-routing-topology	Displays the asymmetric routing information.

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.

From the SCE(config if)# prompt, type:

Command	Purpose
force failure-condition	Forces a virtual failover condition. The system asks for confirmation `Forcing failure will cause a failover - do you want to continue? n` Type '**Y**' and press **Enter** to confirm the forced failure.
no force failure-condition	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**.

From the SCE(config)# prompt, type:

Command	Purpose
failure-recovery operation-mode operational|non-operational	Specifies 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

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.

From the SCE(config if)# prompt, type:

Command	Purpose
subscriber sm-connection-failure action [*force-failure* | *none* | *remove-mappings* | *shut*]	Specifies the action that the SCE platform will perform if the SCE-SM connection fails.
subscriber sm-connection-failure warning	Specifies that the system operational-status of the SCE platform should be 'warning' if the SCE-SM connection fails.

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

From the SCE(config if)# prompt, type:

Command	Purpose
subscriber sm-connection-failure timeout *interval*	Configures the connection timeout.