CHAPTER 7

Configuring the Connection

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.

Note 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 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**

Note When the 'inline-cascade' connection mode is configured, extra care should be given to the configuration of the link shapers.

Note Configuring the shaper in an aggressive manner might result in very high rate of tail-dropped packets. In extreme situations, packets that are used for the High Availability protocol monitoring and control may be dropped. Thus, an extreme situation could result in false detection of a failure in the SCE platform and an unnecessary switchover between the active and standby SCE platforms.

- **Physically-connected-links** — In cascaded topologies, defines which link is connected to this SCE platform.

  Possible values are 'link-0' and 'link-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)** [**physically-connected-links** (**link 0 | link 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 physically-connected-links link-0  priority
primary
```

Example 2

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

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

Monitoring the Connection Mode

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

Displays the connection mode configuration.

Monitoring the Connection Mode: Example

The following example shows how to display the current configuration of the connection mode.

```
SCE>show interface linecard 0 connection-mode
Slot 0 connection mode
Connection mode is inline
slot failure mode is bypass
Redundancy status is standalone
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 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

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 (forwarding|bypass|cutoff)** and press **Enter**.

External Optical Bypass

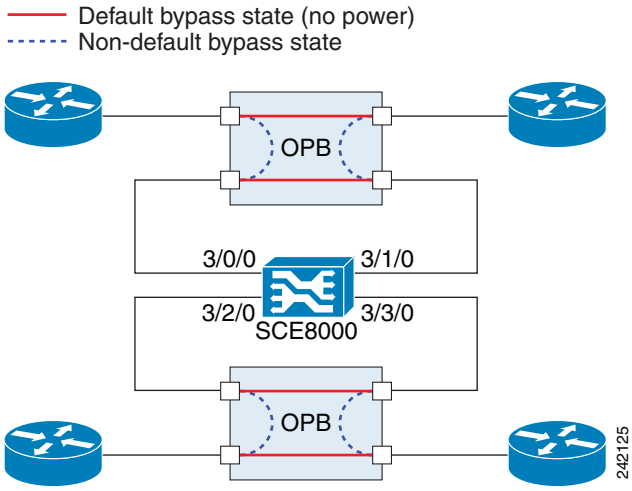
The Cisco SCE8000 supports connection to up to two external optical bypass devices. These protect the line against power failure or total hardware failure, which prevents the hardware card from bypassing the traffic. Each external optical device protects a single traffic link passing through the SCE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

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

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

Enables link failure-reflection.

How to Disable Link Failure Reflection

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

Disables link failure-reflection.

Enabling and Disabling Link Failure Reflection on All Ports

The **link reflection on all ports** feature extends the link failure reflection feature. It allows the user to determine whether all ports should be taken down if a single port link fails.

In certain topologies, when a failure state occurs on one link, the link state must be reflected to all ports to signal any element using this SCE platform that the device is in a failure state, and therefore cannot be used.

In **link reflection on all ports** mode, all ports of the SCE platform are forced down and the link state of the first port is reflected on all the ports.

When recovering from the failure state, the forced down ports (the other link) are brought up only after the first failed port (link) has recovered. In addition, the reflection algorithm will not try to reflect failure for this link again for the next 15 seconds, to avoid link stability problems on auto-negotiation.

Options

The following options are available:

- The **on-all-ports** keyword enables reflection of a link failure to all ports.
- Use the **no** form of this command to disable failure reflection to all ports (the **on-all-ports** keyword is not used in the **no** form of the command).

The default value is **disabled**.

How to Enable Link Failure Reflection on All Ports

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

Enables failure reflection to all ports.

How to Disable Link Failure Reflection on All Ports

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

Disables failure reflection to all ports.

Configuring Link Failure Reflection in Linecard-Aware Mode

The **linecard-aware-mode** option is an additional extension of the link failure reflection feature for use in MGSCP topologies. Use this option when the subscriber-side interface and the corresponding network-side interface of the same link are connected to the same linecard in the router.

This mode reflects a failure of one port to the other three ports of the SCE platform differently, depending on different failure conditions, as follows:

- One interface of the SCE8000 is down: Link failure is reflected to the all other SCE platform ports.
- Two reciprocal ports of the SCE8000 are down simultaneously, indicating a possible problem in the linecard of the router to which the SCE platform is connected: In this case the failure is not reflected to any of the other interfaces. This allows the second link in the SCE platform to continue functioning without interruption.

Use the **no** form of this command with the **linecard-aware-mode** keyword to disable the linecard aware mode without disabling link failure reflection itself.

How to Enable Linecard-Aware Mode

Step 1 From the SCE(config if)# prompt, type **link failure-reflection on-all-ports linecard-aware-mode** and press **Enter**.

Enables failure reflection to all ports with linecard aware mode.

How to Disable Linecard-Aware Mode

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

Disables linecard aware mode.

Note Tthis command does not disable link failure reflection on all ports.

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 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**.

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.

- 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

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**.

Configures the connection timeout.