CHAPTER 7

Configuring the Connection

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

Introduction

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

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

  - 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 whether the system cuts the traffic (cutoff) or bypasses it (bypass) when the SCE platform either has failed or is booting.

  Default — **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|cutoff)** and press **Enter**.

Configuring the Connection Mode: Examples

Example 1

This example defines the primary device in a two-SCE platform redundant, inline topology. Link 0 is connected to this device, and the link mode on failure is bypass.

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

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 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**.

Displays the connection mode configuration.

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 cutoff
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 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 Cascade Connections

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

Monitoring Cascade Connection: Examples

The following example shows the output of this command in the case of two cascaded SCE 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 0/3 must be connected to port 0/4 at peer
Port 0/4 must be connected to port 0/3 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
```

How to Configure 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 four possible modes of operation:

- bypass
- forwarding
- cutoff
- sniffing

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 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.
- **Sniffing** — allows the SCE platform to forward traffic on the specified link through the bypass mechanism while still analyzing the traffic passively.

  Sniffing is permitted to be configured for all links, only (use the **all-links** option).
- **Cutoff** — completely cuts off flow of traffic through the specified link.
- link# — the number of the link being configured

  Use the **all-links** option to apply the configuration to all links

Recommendations and restrictions

Note the following recommendations and restrictions:

- Since the SCE 1000 platform has only one link, the link is not specified.
- Since the SCE 2000 platforms have more than one link, it is required to specify the link. The link designations are different for the GBE and FE platforms, as follows:
  - SCE 2000 4xGBE — GBE1-GBE2/GBE3-GBE4
  - SCE 2000 4/8xFE — LINK1/LINK2
- Use the **all-links** option to configure the link mode for all links (SCE 2000 platforms only).
- It is recommended that both links be configured together. Use the **all-links** option.

- 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 will be unpredictable.
- Sniffing can only be configured for all links, therefore, to configure sniffing, the all-links option is required, not just recommended.
- 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.

Step 1 From the SCE(config if)# prompt, type `link mode [`*linknumber* `|all-links] [forwarding|bypass|sniffing|cutoff]` and press **Enter**.

Configures the link mode for the specified link.

Configuring 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, 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*.

How to Monitor 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   :   2%
Traffic Processor 2   :   7%
Traffic Processor 3   :   0%
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. (See Managing Application Files, page 3-10.)

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**' 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.

Configuring 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.

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

Options

The following options are available:

- **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.

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

Configures the action of the SCE platform in the case of failure of the connection to the SM.

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.

Enabling and Disabling 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.

Note The **link reflection on all ports** feature cannot be used in a cascade mode, because in this mode one of the links is used to provide redundancy.

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(configif)# 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 the Linecard-Aware Mode (Cisco SCE 2000 Only)

- How to Enable the Linecard-Aware Mode, page 7-15
- How to Disable the Linecard-Aware Mode, page 7-15

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 of the SCE 2000 platform 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 2000 differently, depending on different failure conditions, as follows:

- One interface of the SCE 2000 is down: Link failure is reflected to the all other SCE platform ports.
- Two reciprocal ports of the SCE 2000 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 the Linecard-Aware Mode

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

Enables failure reflection to all ports with linecard aware mode.

How to Disable the 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 that this command does not disable link failure reflection on all ports.