
# Redundancy and Failover

**Revised: February 07, 2014, OL-29134-02**

## Introduction

# Redundancy and Failover



This chapter presents the Failover and redundancy capabilities of the Cisco SCE 8000 platform. It first defines relevant terminology, as well as pertinent theoretical aspects of the redundancy and failover solution. It then explains specific recovery procedures for both single and dual link topologies. It also explains specific update procedures to be used in a cascaded Cisco SCE platform deployments. When failover is required in a deployment, a topology with two cascaded Cisco SCE 8000 platforms is used. This cascaded solution provides both network link failover, and failover of the functionality of the Cisco SCE platform, including updated subscriber state.

## Terminology and Definitions

Following is a list of definitions of terms used in the chapter as they apply to the Cisco failover solution, which is based on cascaded Cisco SCE platforms.

- Failover—A situation in which the Cisco SCE platform experiences a problem that makes it impossible for it to provide its normal functionality, and a second Cisco SCE platform device immediately takes over for the failed Cisco SCE platform.
- Hot standby—When two Cisco SCE platforms are deployed in a failover topology, one Cisco SCE platform is active, while the second Cisco SCE platform is in standby, receiving from the active Cisco SCE platform all subscriber state updates and keep alive messages.
- Primary/Secondary—The terms Primary and Secondary refer to the default status of a particular Cisco SCE platform. The Primary Cisco SCE Platform is active by default, while the Secondary device is the default standby. Note that these defaults apply only when both devices are started together. However, if the primary Cisco SCE platform fails and then recovers, it will not revert to active status, but remains in standby status, while the secondary device remains active.
- Subscriber state failover—A failover solution in which subscriber state is saved.

## Redundant Topologies

The Cisco SCE 8000 includes SPA Interface Processor card with an internal electrical bypass module, which provides the capability of preserving the network link in case of failure. However, preserving the Cisco SCE platform functionality in case of a failure, requires a redundant Cisco SCE platform. Cisco provides a unique solution for this scenario, through deploying two cascaded Cisco SCE platforms.

The cascading is implemented by connecting the two Cisco SCE platforms using two of the data links. In each Cisco SCE platform, two of the four data interfaces are connected to each of the network links, while the other two data interfaces are used for cascading between the Cisco SCE platforms. (See the *Cisco SCE8000 10GBE Installation and Configuration Guide* for specific cabling procedures for redundant topologies.) The cascade ports are used for transferring network traffic, keep-alive messages and subscriber state updates.

# External Bypass

The Cisco SCE 8000 platform can control an external bypass device, which bypasses the traffic during a power failure and also under specific control command from the Cisco SCE 8000. The Cisco SCE 8000 automatically activates the external bypass device during reload for the short period (less than 10 seconds) in which the SPA Interface Processor card does not forward traffic between traffic ports. In addition, the Cisco SCE 8000 can be configured to activate the external bypass device in the following cases:

- After executing the **external-bypass** command , until the **no external-bypass** command is executed
- When the Cisco SCE 8000 is in failure state.

Note that in a cascaded configuration, an external bypass device should be connected only for the traffic ports. The cascade ports should be directly connected between the two Cisco SCE 8000 platforms (see Figure 11-1).

# Hardware Bypass

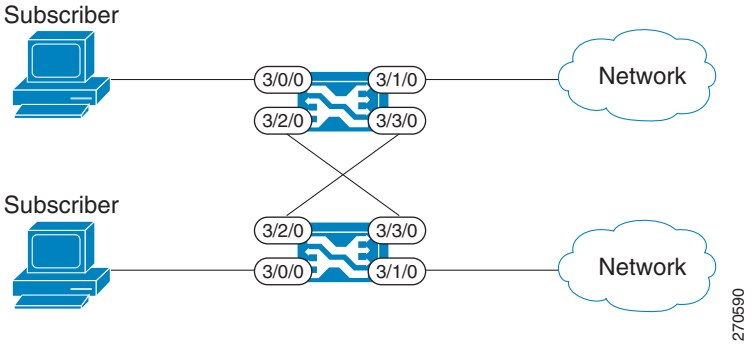
The Cisco SCE 8000 platform can support the hardware bypass, which bypasses the traffic of the configured static parties created in the hw-bypass mode at the hardware (SIP module) level based on their IP address or the IP address range.

**Note** The static parties created only in the hw-bypass mode are bypassed.

# In-line Dual Link Redundant Topology

This topology serves inline deployments where the Cisco SCE platform functionality should be preserved in case of a failure, in addition to preserving the network link (Figure 11-1).

***Figure 11-1 In-line Dual Link Redundant Topology***




# Failure Detection

The Cisco SCE 8000 platform has several types of mechanisms for detecting failures:

- Internal failure detection—The Cisco SCE platform monitors for hardware and software conditions such as overheating and fatal software errors.
- Inter-device failure detection—The Cisco SCE platform sends periodic keep-alive messages via the cascade ports
- The Cisco SCE platform-Subscriber Manager (SM) communication failure detection—A failure to communicate with the SM may be regarded as a cause for failover. However, this communication failure is not necessarily a problem in the Cisco SCE platform. If the connection to the SM of the active Cisco SCE platform has failed, while the connection to the SM of the standby Cisco SCE platform is alive, a failover process will be initiated to allow the Cisco SCE platform proper exchange of information between the Cisco SCE platforms and the SM.
- Link failure—The system monitors all three types of links for failures:
  - Traffic port link failure—Traffic cannot flow through the Cisco SCE platform.
  - Cascade port link failure—Traffic cannot flow between the Cisco SCE platforms through the cascade ports.
  - Management port link failure—This is not a failure that interrupts traffic on the link in and of itself. However, when SM is used, management port link failure will cause an SM connection failure and this, in turn, will be declared as a failure of the Cisco SCE platform.

  This type of failure, in most cases, does not require reboot of the Cisco SCE platform. When the connection with the SM is re-established the Cisco SCE platform is again ready for hot standby. If both Cisco SCE platforms lose their connections with the SM, it is assumed that it is the SM which has failed, thus, no action will be taken in the Cisco SCE platform.

# Link Failure Reflection

The Cisco SCE platforms are transparent at Layers 2 and 3. The Cisco SCE 8000 platform operates in promiscuous mode, and the network elements on both sides of the Cisco SCE platform, are using the MAC address of the other network element when forwarding traffic.

To assist the network elements on both sides of the Cisco SCE platform to identify the link failures as quickly as possible, the Cisco SCE platform supports a functionality of reflecting to the other side of the Cisco SCE platforms events of link failure. When the link on one side of the Cisco SCE platform fails, the corresponding link on the other side is forced down, to reflect the failure. Link failure reflection is done on the traffic ports. When operating in deployments of single Cisco SCE platform with two data links, link failure is reflected between the two ports of each link.

When working with two cascaded Cisco SCE platforms, link failure is reflected in two cases:

- Reflection between the traffic ports of each Cisco SCE platform.
- If there is a failure in the cascade port link, the two Cisco SCE platforms can no longer support proper processing of the two links, since the traffic flowing on the standby Cisco SCE platform's link must be forwarded to the active Cisco SCE platform for processing. In this case the link failure is reflected from the cascade ports to the traffic ports of the standby Cisco SCE platform, in order to force the network to switch all the traffic only through the link of the active Cisco SCE platform.

# Hot Standby and Failover

The failover solution requires two Cisco SCE platforms connected in a cascade manner.



## Hot Standby

In failover solution, one of the Cisco SCE platforms is used as the active Cisco SCE platform and the other is used as the standby. Although traffic enters both the active and the standby Cisco SCE platforms, all traffic processing takes place in the Cisco SCE platform which is currently the active one. The active Cisco SCE platform processes the traffic coming on both links, its own link and the link connected to the standby Cisco SCE platform, as follows

- All traffic entering the active Cisco SCE platform through its traffic ports is processed in that Cisco SCE platform and then forwarded to the line.
- All traffic entering the standby Cisco SCE platform through its traffic ports is forwarded through the cascade ports to the active Cisco SCE platform where it is processed, and then returned to the standby Cisco SCE platform through the cascade ports to be forwarded to the original line from which it came.

Since only one Cisco SCE platform processes all traffic at any given time, split flows, which are caused by asymmetrical routing, that exist in the two data links are handled correctly.

To support subscriber-state failover, both Cisco SCE platforms hold subscriber states for all parties, and subscriber state updates are exchanged between the active Cisco SCE platform and the standby. This way, if the active Cisco SCE platform fails, the standby Cisco SCE platform is able to start serving the line immediately with a minimum loss of subscriber-state.

The two Cisco SCE platforms also use the cascade channel for exchanging periodic keep-alive messages.

## Failover

In failover solution, the two Cisco SCE platforms exchange keep alive messages via the cascade ports. This keep alive mechanism enables fast detection of failures between the Cisco SCE platforms and fast failover to the standby Cisco SCE platform when required.

If the active Cisco SCE platform fails, the standby Cisco SCE platform then assumes the role of the active Cisco SCE platform.

The failed Cisco SCE platform uses its electrical bypass mechanism, which is a hardware entity that is separate from the main board and processors, to forward traffic to the other Cisco SCE platform, and to forward processed traffic back to the link. The previously standby Cisco SCE platform now processes all the traffic of this other link that is forwarded to it by the previously active Cisco SCE platform in addition to the traffic of its own link.

When the failed Cisco SCE platform recovers, it will remain in standby, while the previously standby Cisco SCE platform remains active. Switching the Cisco SCE platforms back to their original roles may be performed manually, if required, after the failed Cisco SCE platform has either recovered or been replaced.

If the failure is in the standby Cisco SCE platform, it will continue to forward traffic to the active Cisco SCE platform and back to its link, while the active Cisco SCE platform continues to provide its normal processing functionality to the traffic of the two links.

**Note** For information regarding the synchronization of subscriber information between cascaded Cisco SCE platforms and the effect of failover on the subscriber databases, see "Anonymous Groups and Subscriber Templates" section on page 10-7.

There are three user-configurable options that are relevant in a situation when a Cisco SCE platform fails:

- **Bypass—**Maintain the link in bypass mode (continue sending traffic to the other Cisco SCE platform, and then continue forwarding the processed traffic back to the link). The incoming traffic in the failed Cisco SCE platform is forwarded to the working Cisco SCE platform, where it is processed and then sent back to the original Cisco SCE platform and back to the link. This is the default configuration.
  - Effect on the network link—Negligible.
  - Effect on the Cisco SCE platform functionality—The effect on the Cisco SCE platform functionality is dependent on the failed Cisco SCE platform.
  - If the failure is in the standby Cisco SCE platform—The active Cisco SCE platform continues providing its normal functionality, processing the traffic of the two links.
  - If the failure is in the active Cisco SCE platform—The standby Cisco SCE platform takes over processing the traffic, and becomes the active Cisco SCE platform.
- **Cutoff—**Change the link of the failed Cisco SCE platform to cutoff (layer 1) forcing the network to switch all traffic through the line of the working Cisco SCE platform. This will, of course, decrease the network capacity by 50%, but may be useful in some cases.

  This option is available for use in special cases, and requires special configuration.
  - Effect on the network link—The network loses 50% of its capacity (until the failed Cisco SCE platform has recovered).
  - Effect on the Cisco SCE platform functionality—The effect on the Cisco SCE platform functionality is dependent on the failed Cisco SCE platform.
  - If the failure is in the standby Cisco SCE platform—The active Cisco SCE platform continues providing its normal functionality, processing the traffic of the two links.
  - If the failure is in the active Cisco SCE platform—The standby Cisco SCE platform takes over processing the traffic, and becomes the active Cisco SCE platform.
- **External-bypass—**Activate the external bypass device connected to the failed Cisco SCE platform, passing all traffic through the line without being serviced by the failed Cisco SCE platform. Although this may cause the traffic passing through the other link (that of the non-failed Cisco SCE platform) to get service in split-flow conditions if asymmetric routing is present, it may be useful in some cases.

  This option is available for use in special cases, and requires special configuration.
  - Effect on the network link—Negligible

– Effect on the Cisco SCE platform functionality—Since the active Cisco SCE platform only sees the traffic of a single link, split-flow effects might occur. The link connected to the failed Cisco SCE platform gets no service.

# Hardware Crash Mode

There are three hardware components that operate together to produce the desired behavior upon failure of the Cisco SCE 8000 platform:

- external optical bypass: In a cascade setup, if the traffic links are connected to external optical bypass modules, the optical bypass may be either activated or deactivated by the hardware during a failure.

  The external optical bypasses protect against a second Cisco SCE 8000 platform failure. In the case of a second failure, if a bypass module is connected to the last Cisco SCE 8000 to fail, it will be enabled. This preserves one of the network links, assuming the *on-failure* configuration is is **bypass** . If the *on-failure* configuration is **external-bypass** , the external optical bypass is activated even during a single failure by the failed Cisco SCE platform.

- internal electrical bypass: The Cisco SCE 8000 contains internal electrical bypasses connecting SPA modules 0 and 2 and modules 1 and 3. These bypasses transmit the traffic to and from the cascade connections between the platforms.

- SPA modules: Under some conditions (such as if the *on-failure* configuration is **cutoff**), the SPA modules are disabled when failure occurs.

The collective behavior of these three components is known as the hardware crash mode and is dependent on the configuration of the *on-failure* parameter of the **connection-mode** command, as well as whether the platform is the active or standby platform.

In the standby platform, hardware crash mode behavior is as follows for:

For **on-failure bypass**:

- The external optical bypass, if installed, is deactivated (traffic is sent to the platform).
- The electrical bypass is enabled (cascade ports transmit traffic to the active platform for processing)
- The SPA modules are enabled (all ports and links are functioning)

This means that whether the standby platform is operational or has failed, it transmits traffic to the active platform for processing via the electrical bypasses.

For **on-failure cutoff**:

- The external optical bypass, if installed, is deactivated (traffic is sent to the platform).
- The electrical bypass is disabled.
- The SPA modules are powered off.

This means that if the standby platform fails, the link connected to it Cisco SCE is severed.

For **on-failure external-bypass**:

- The external optical bypass is activated (traffic is bypassed).
- The electrical bypass is enabled between ports 0 and 1. (This is a special configuration, done just in case the optical bypass device does not function, which has a very low probability.)
- The SPA modules are enabled (all ports and links are functioning)

This means that when the standby Cisco SCE platform is failed, the external optical bypass is used to ensure link continuity at the expense of not servicing the traffic on that link.

In the active platform, the hardware crash mode behavior is exactly the same as on a standby platform. The active platform assumes that when it fails, the standby platform will take over and process the traffic.

If the standby platform has failed, failure of the active platform means that the entire system has failed (this state is also called a 'second failure'). The hardware crash mode behavior in the active platform in this case depends on the configuration of the *on-failure* parameter, which determines whether traffic is bypassed via the external bypass, if installed, maintaining traffic flow through one link, although with no processing, or whether traffic is completely cut off.

If the standby platform has failed and the *on-failure* configuration is **bypass** or **external-bypass**, hardware crash mode behavior in the active platform is as follows:

- The external optical bypass is activated (traffic is bypassed via the external bypass).
- The electrical bypass is enabled between ports 0 and 1. (This is a special configuration, done just in case the optical bypass device does not function, which has a very low probability)
- The SPA modules are enabled (all ports and links are functioning)

Since neither platform is operational at this point, there is no processing taking place and traffic is simply bypassed via the external optical bypass. If external optical bypass modules are not installed, traffic is cut off.

If the standby platform has failed and the *on-failure* configuration is **cutoff**, hardware crash mode behavior in the active platform is as follows:

- The external optical bypass, if installed, is deactivated (traffic is sent to the platform).
- The electrical bypass is disabled (cascade ports do not transmit traffic to the standby platform since it is also not operational)
- The SPA modules are disabled (ports and links are not functioning)

Since neither platform is operational at this point, there is no processing taking place. In addition, although traffic reaches the platform, since the internal bypasses as well as all the ports are disabled, this results in a 'dead end' , cutting off all traffic on both links.

# Failure in the Cascade Connection

The effect of a failure in the cascade connection between the two Cisco SCE platforms depends on whether one or both connections fail:

- Only one cascade connection is down—In this case, both Cisco SCE platforms can still communicate, so each still knows the status of the peer.

  As long as one cascade connection remains up, the standby will cut off its traffic links so that all traffic is routed via the active Cisco SCE platform. Therefore, split flow is avoided, but at the expense of half line capacity.
- Both cascade links are down—In this case, neither Cisco SCE platform knows anything about the status of the peer. Each platform then works in standalone mode, which means that each Cisco SCE platform processes on its own traffic only. This results in split flows.

# Installing a Cascaded System

This section outlines the installation procedures for a redundant solution with two cascaded Cisco SCE platforms.

For information on topologies and connections, see the *Cisco SCE8000 10GBE Installation and Configuration Guide* .

For details of the CLI commands, see the *Cisco SCE8000 CLI Command Reference*.

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

**Step 1** Install both Cisco SCE platforms, power them up, and perform the initial system configuration.

**Step 2** If external optical bypass modules are installed, make sure they are connected correctly and are operational. Use the **show external-bypass** command.

**Step 3** Connect both Cisco SCE platforms to the management station.

**Step 4** Connect the cascade ports.

The cascade ports may be connected either directly in Layer 1 (dark fibers) or through a switch. When connecting the cascade ports through a switch, it is important to assign each cascade link to a different VLAN, otherwise the traffic will be forwarded incorrectly (between different links) by the switch.

**Step 5** Set topology configurations for each Cisco SCE platform via the connection-mode options. (See "Topology-Related Parameters for Redundant Topologies" section on page 11-13)

**Step 6** Make sure that the Cisco SCE platforms have synchronized and active Cisco SCE platform was selected. Use the **show interface linecard 0 connection-mode** command.

**Step 7** If you want to start in bypass mode, change the link mode to bypass in both Cisco SCE platforms. The bypass mode will be applied only to the active Cisco SCE platform. (See "About the Link Mode" section on page 8-6.)

**Step 8** Verify the link mode configuration. (See "Monitoring the System" section on page 11-14.) Use the **show interface linecard 0 link mode** command.

**Step 9** Connect the traffic port of Cisco SCE platform #0. This will cause a momentary down time until the network elements from both sides of the Cisco SCE platform auto-negotiate with it and start working (when working inline).

**Step 10** Connect the traffic port of Cisco SCE platform #1, this will cause a momentary down time until the network elements from both sides of the Cisco SCE platform auto-negotiate with it and start working (when working inline).

**Step 11** When full control is needed, change the link mode on both Cisco SCE platforms on both links to 'forwarding'. It is recommended to first configure the active Cisco SCE platform and then the standby. (See "About the Link Mode" section on page 8-6.)

**Step 12** You can now start working with the Subscriber Manager.

**Note** Cisco SCE devices does not support downgrading from Cisco SCE Release 3.8.0 and later to Cisco SCE Releases earlier than Release 3.8.0 when the devices are configured in a cascade setup. To downgrade the devices to Cisco SCE Releases earlier than Release 3.8.0, remove the devices from the cascade setup and configure the devices as standalone devices, and then start the downgrade procedure. Note that this downgrade procedure may cause a service disruption.

# Recovery



This section specifies the procedure for recovery after a failure. The purpose of the recovery procedure is to restore the system to fully functional status. After the recovery procedure, the behavior of the system is the same as after installation.

A failed Cisco SCE platform may either recover automatically or be replaced (manual recovery). Whether recovery is automatic or manual depends on the original cause of the failure:

- Power failure—Manual or automatic recovery can be implemented.
- Any failure resulting in a reboot—Manual or automatic recovery can be implemented (this is configurable).
- 3-consecutive reboots within half an hour—Manual recovery only
- Cascade ports link-failure—Automatic recovery when link revives.
- Traffic link failure—Automatic recovery when link revives.
- Failure in the communications with the SM—Automatic by SM decisions after connection is re-established.
- Hardware malfunction—Manual recovery, after replacing the malfunctioning Cisco SCE platform.

## Replacing the Cisco SCE Platform (Manual Recovery)

This is done in two stages, first manual installation steps performed by the technician, and then automatic configuration steps performed by the system.



### Manual Steps

**Step 1** Disconnect the failed Cisco SCE platform from the network

**Step 2** Connect a new Cisco SCE platform to the management link and the cascade links (leave network ports disconnected.)

**Step 3** Configure the Cisco SCE platform.

**Step 4** Basic network configurations done manually (first time).

**Step 5** Load application software (*Service Control Application for Broadband* ) to the Cisco SCE platform. Provide application configuration.

**Step 6** Connect the traffic ports to the network links.

### Automatic Steps (in parallel with the manual steps, requires no user intervention):

**Step 1** Establishment of inter-Cisco SCE platform communication.

**Step 2** Synchronization with the SM.

**Step 3** Copying updated subscriber states from the active Cisco SCE platform to the standby.

## Reboot Only (Fully Automatic Recovery)

**Step 1** Reboot of the Cisco SCE platform.

**Step 2** Basic network configurations.

**Step 3** Establishment of inter-Cisco SCE platform communication.

**Step 4** Selection of the active Cisco SCE platform.

**Step 5** Synchronization of the recovered Cisco SCE platform with the SM.

**Step 6** Copying updated subscriber states from the active Cisco SCE platform to the standby.

# 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

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

- **Connection mode—**Redundancy is achieved by cascading two Cisco SCE platforms. Therefore the connection mode for both Cisco SCE platforms may be either:
  - Inline-cascade
  - Receive-only-cascade
- **sce-id—**For each of the cascaded Cisco SCE platforms, this parameter defines the number of the link (0 or 1) connected to this Cisco SCE platform.

  The sce-id parameter, which identifies the Cisco 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 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.

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

## Configuring the Connection Mode

Use the following command to configure the connection mode, including the following parameters.

- inline/receive only
- sce-id (physically connected link)
- behavior upon failure of the Cisco SCE platform
- primary/secondary

To configure the connection mode, use the following command.

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

| Command | Purpose |
|---|---|
| **connection-mode (inline-cascade\|receive-only-cascade) sce-id {0\|1}priority {primary\|secondary} on-failure {bypass \| external-bypass\|cutoff}** | Configures the connection mode. |

## Examples

#### EXAMPLE 1

Use the following command to configure the primary Cisco SCE platform in a two-Cisco SCE platform inline topology. Link 1 is connected to this Cisco SCE platform and the behavior of the Cisco SCE platform if a failure occurs is *bypass* , which is the default.

```
SCE(config-if)#connection-mode inline-cascade sce-id 1 priority primary
```

#### EXAMPLE 2

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

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

# Monitoring the System

Use the following commands to view the current connection mode and link mode parameters.

## How to View the Current Connection Mode

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0 connection-mode** | Displays the current connection mode. |

#### 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 Cisco SCE-ID

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0 sce-id** | Displays the Cisco SCE-ID. |

#### Viewing the Cisco 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 Cisco SCE Platform

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0** cascade **redundancy-status** | Displays the current redundancy status of the Cisco SCE platform. |

#### Viewing the Current Redundancy Status of the Cisco 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 Cisco SCE Platform

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0** cascade **peer-sce-information** | Displays information about the peer Cisco SCE platform. |

#### Viewing Information about the Peer Cisco 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

From the SCE> prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0** cascade **connection-status** | Displays information about the cascade connections. |

#### Monitoring the Connection Status: Examples

The following example shows the output of this command in the case of two cascaded Cisco SCE 8000 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 Cisco 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>
```

## How to View the Current Link to Port Mappings

From the SCE> prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0 link-to-port-mapping** | Displays the current link to port mappings. |

#### 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-mappings
Link Id | Upstream Port <Out>| Downstream Port <Out>
------------------------------------------------------------
0       | 0/2                | 0/1
SCE>
```

## How to View the Current Link Mode

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show interface linecard 0 link mode** | Displays the current link mode. |

# Configuring 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:

| Commands | Purpose |
|---|---|
| **force failure-condition** | Forces the Cisco SCE platform into a virtual failure state. |
| **no force failure-condition** | Exits from the virtual failure state. |

# System Upgrades



In a redundant solution, it is important that firmware and/or application upgrades be performed in such a way that line and service are preserved.

Refer to the following sections for instructions on how to perform these procedures on two cascaded Cisco SCE platforms:

- Upgrade the firmware only
- Upgrade the application only
- Upgrade both the firmware and the application at the same time

**Note** When upgrading only one component (either firmware only or application only), always verify that the upgraded component is compatible with the component that was not upgraded.

## Firmware Upgrade (package installation)

**Step 1** Install package on both Cisco SCE platforms (open the package and copy configuration).

**Step 2** Reload the standby Cisco SCE platform.

**Step 3** Wait until the standby finishes synchronizing and is ready to work.

**Step 4** Make sure that the connection mode configurations are correct.

**Step 5** Reload the active Cisco SCE platform.

**Step 6** After the former active Cisco SCE platform reboots and is ready to work manually, it may be left as standby or we can manually switch the Cisco SCE platforms to their original state.

## Application Upgrade

**Step 1** Unload the application in the standby Cisco SCE platform.

**Step 2** Load new application to the standby Cisco SCE platform.

**Step 3** Make sure that the connection mode configurations are correct.

**Step 4** Wait until the standby Cisco SCE platform finishes synchronizing and is ready to work.

**Step 5** Force failure condition in the active Cisco SCE platform.

**Step 6** Upgrade the application in the former active Cisco SCE platform.

**Step 7** Remove the force failure condition in that platform.

**Step 8** After the former active Cisco SCE platform recovers and is ready to work, it may remain the standby or can be manually switched back to active.

## Simultaneous Upgrade of Firmware and Application

**Step 1** In the standby Cisco SCE platform:

- **a.** Uninstall the application.
- **b.** Upgrade the firmware (this includes a reboot).
- **c.** Install the new application.

**Step 2** Force-failure in the active Cisco SCE platform.

This makes the updated Cisco SCE platform the active one, and it begins to give the NEW service.

**Step 3** Repeat step 1 for the (now) standby Cisco SCE platform.

Since this includes a reboot, it is not necessary to undo the force failure command.