



Configuring Stateful Switchover

Last Updated: March 14, 2011

The Stateful Switchover (SSO) feature works with Nonstop Forwarding (NSF) in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The primary objective of SSO is to improve the availability of networks constructed with Cisco routers. SSO performs the following functions:

- Maintains stateful protocol and application information to retain user session information during a switchover.
- Enables line cards to continue to forward network traffic with no loss of sessions, providing improved network availability.
- Provides a faster switchover relative to high system availability.
- [Finding Feature Information, page 1](#)
- [Prerequisites for Stateful Switchover, page 2](#)
- [Restrictions for Stateful Switchover, page 2](#)
- [Information About Stateful Switchover, page 9](#)
- [How to Configure Stateful Switchover, page 25](#)
- [Configuration Examples for Stateful Switchover, page 36](#)
- [Additional References, page 42](#)
- [Feature Information for Stateful Switchover, page 44](#)
- [, page 47](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Prerequisites for Stateful Switchover

- [General Prerequisites, page 2](#)
- [Cisco 10000 Series Devices Prerequisites, page 2](#)
- [Cisco 7500 Series Internet Router Platform Prerequisites, page 2](#)

General Prerequisites

- For hardware-redundant platforms, two Route Processors (RPs) must be installed in the chassis, each running the same version or a compatible version of the Cisco software.
- Before copying a file to flash memory, be sure that ample space is available in flash memory. Compare the size of the file you are copying to the amount of available flash memory shown. If the space available is less than the space required by the file you will copy, the copy process will not continue and an error message similar to the following will be displayed:

```
%Error copying tftp://image@server/tftpboot/filelocation/imagename (Not enough space on device).
```

- Distributed Cisco Express Forwarding must be enabled on any networking device configured to run SSO.
- For Nonstop Forwarding (NSF) support, neighbor routers must be running NSF-enabled images, though SSO need not be configured on the neighbor device.

Cisco 10000 Series Devices Prerequisites

- On Cisco 10000 series devices only, to boot both Performance Routing Engines (PREs) from the TFTP boot server, you must use the **ip address negotiated** command in interface configuration mode to enable DHCP on the PRE. Otherwise, you will get a duplicate IP address error because of the synchronization of the IP address from the active to the standby Route Processor (RP).

Cisco 7500 Series Internet Router Platform Prerequisites

- On the Cisco 7507 and Cisco 7513 routers, any combination of RSP8 and RSP16 devices, or any combination of RSP2 and RSP4, are required.

Restrictions for Stateful Switchover

- [General Restrictions for SSO, page 3](#)
- [Configuration Mode Restrictions, page 3](#)
- [Switchover Process Restrictions, page 3](#)

- [ATM Restrictions, page 3](#)
- [Frame Relay and Multilink Frame Relay Restrictions, page 4](#)
- [PPP Restrictions, page 5](#)
- [Cisco 12000 Series Internet Router Platform Restrictions, page 5](#)
- [Cisco 10000 Series Internet Router Platform Restrictions, page 6](#)
- [Cisco 7500 Series Internet Router Platform Restrictions, page 7](#)
- [Cisco 7304 Router Platform Restrictions, page 8](#)
- [Cisco ASR 1000 Series Routers Restrictions, page 8](#)

General Restrictions for SSO

- Both RPs must run the same Cisco software image. If the RPs are operating different Cisco software images, the system reverts to RPR mode even if SSO is configured.
- Configuration changes made through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- Load sharing between dual processors is not supported.
- The Hot Standby Routing Protocol (HSRP) is not supported with Cisco Nonstop Forwarding with Stateful Switchover. Do not use HSRP with Cisco Nonstop Forwarding with Stateful Switchover.
- Enhanced Object Tracking (EOT) is not stateful switchover-aware and cannot be used with HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) in SSO mode.
- Multicast is not SSO-aware and restarts after switchover; therefore, multicast tables and data structures are cleared upon switchover.

Configuration Mode Restrictions

- The configuration registers on both RPs must be set the same for the networking device to behave the same when either RP is rebooted.
- During the startup (bulk) synchronization, configuration changes are not allowed. Before making any configuration changes, wait for a message similar to the following:

```
%HA-5-MODE:Operating mode is sso, configured mode is sso.
```

- On the Cisco 7304 router, a message similar to the following appears (the actual slot number depends on which slot has the active processor):

```
%HA-6-STANDBY_READY: Standby RP in slot n  
is operational in SSO mode
```

Switchover Process Restrictions

- If the router is configured for SSO mode, and the active RP fails before the standby is ready to switch over, the router will recover through a full system reset.

ATM Restrictions

- Label-controlled ATM (LC-ATM) functionality does not co-exist with SSO in this release.

- The ATM line protocol does not support stateful switchover capability for the following features in this release:
 - SVCs
 - Switched virtual paths (SVPs)
 - Tagged virtual circuits (TVCs)
 - Point-to-multipoint SVC
 - Integrated Local Management Interface (ILMI)
 - Signaling and Service Specific Connection Oriented Protocol (SSCOP)
 - ATM Connection Manager, permanent virtual circuit (PVC) discovery, ATM applications
 - Backward or version compatibility
 - Statistics and accounting
 - Zero ATM cell loss

Frame Relay and Multilink Frame Relay Restrictions

- The following Frame Relay features are not synchronized between the active and standby RPs in this release: Frame Relay statistics; enhanced LMI (ELMI); Link Access Procedure, Frame Relay (LAPF); SVCs; and subinterface line state.



Note

The subinterface line state is determined by the PVC state, which follows the line card protocol state on DCE interfaces, and is learned from first LMI status exchange after switchover on DTE interfaces.

- Frame Relay SSO is supported with the following features:
 - Serial interfaces
 - DTE and DCE LMI (or no keepalives)
 - PVCs (terminated and switched)
 - IP
- When no LMI type is explicitly configured on a DTE interface, the autosensed LMI type is synchronized.
- LMI sequence numbers are not synchronized between the active and standby RPs by default.

LMI keepalive messages contain sequence numbers so that each side (network and peer) of a PVC can detect errors. An incorrect sequence number counts as one error. By default, the switch declares the line protocol and all PVCs down after three consecutive errors. Although it seems that synchronizing LMI sequence numbers might prevent dropped PVCs, the use of resources required to synchronize LMI sequence numbers for potentially thousands of interfaces (channelized) on larger networking devices might be a problem in itself. The networking device can be configured to synchronize LMI sequence numbers. Synchronization of sequence numbers is not necessary for DCE interfaces.

- Changes to the line protocol state are synchronized between the active and standby RPs. The line protocol is assumed to be up on switchover, providing that the interface is up.
- PVC state changes are not synchronized between the active and standby RPs. The PVC is set to the up state on switchover provided that the line protocol state is up. The true state is determined when the first full status message is received from the switch on DTE interfaces.
- Subinterface line state is not synchronized between the active and standby RPs. Subinterface line state is controlled by the PVC state, by configuration settings, or by the hardware interface state when the PVC is up. On switchover, the subinterface state is set to up, providing that the subinterfaces are not

shut down and the main interface is up and the line protocol state is up. On DTE devices, the correct state is learned after the first LMI status exchange.

- Dynamic maps are not synchronized between the active and standby RPs. Adjacency changes as a result of dynamic map change are relearned after switchover.
- Dynamically learned PVCs are synchronized between the active and standby RPs and are relearned after the first LMI status exchange.
- For Multilink Frame Relay bundle links, the state of the local bundle link and peer bundle ID is synchronized.
- For a Multilink Frame Relay bundle, the peer ID is synchronized.

PPP Restrictions

- The following PPP features are not supported in this release: dialer; authentication, authorization, and accounting (AAA), IPPOOL, Layer 2 (L2X), Point-to-Point Tunneling Protocol (PPTP), Microsoft Point-to-point Encryption (MPPE), Link Quality Monitoring (LQM), link or header compression, bridging, asynchronous PPP, and XXCP.
- We recommend that the keepalive value be set to 20 seconds on Cisco 7500 series routers for each peer in a PPP connection.

Cisco 12000 Series Internet Router Platform Restrictions

- On Cisco 12000 series devices with three or more RPs in a chassis, after negotiation of active and standby RP, the non-active (remaining) RPs do not participate in router operation.
- On the Cisco 12000 and 7500 series routers, if any changes to the fabric configuration happen simultaneously with an RP switchover, the chassis is reset and all line cards are reset.
- On the Cisco 12000 series and 10000 series Internet routers, if a switchover occurs before the bulk synchronization step is complete, the new active RP may be in inconsistent states. The router will be reloaded in this case.
- SSO does not support TFTP boot operation on the Cisco 12000 series Internet routers. The software images must be downloaded to the flash memory cards on the router.
- Any line cards that are not online at the time of a switchover (line cards not in Cisco software running state) are reset and reloaded on a switchover.
- The following line cards support SSO and Cisco NSF:
 - All Engine-0, Engine-2, and Engine-4 Packet over SONET (PoS) line cards
 - All Engine-0 ATM line cards
 - All nonchannelized DS3 and E3 line cards
 - All Engine-0 channelized line cards
 - 1XGE and 3XGE line cards
- The following Engine-0 line cards are supported:
 - 4-port OC-3 PoS
 - 1-port OC-12 PoS
 - 1-port O-12 ATM
 - 4-port OC-3 ATM
 - 6-port DS3
 - 12-port DS3
 - 6-port E3

- 12-port E3
- 6-port CT3
- 1-port CHOC-12->DS3
- 6-port CT3->DS1
- 1-port CHOC-12/STM4->OC-3/STM1 POS
- 2-port CHOC-3/STM-1->DS1/E1
- The following Engine-1 line cards are supported:
 - 2-Port OC-12/STM-4c DPT
- The following Engine-2 line cards are supported:
 - 1-port OC-48 POS
 - 1-port OC-48/STM-16c DPT
 - 4-port OC-12 POS
 - 8-port OC-3 POS
 - 8-port OC-3/STM-1c ATM
 - 16-port OC-3 POS
- The following Engine-4 line cards are supported:
 - 1-port OC-192 POS
 - 4-port OC-48 POS
- The following IP Service Engine (ISE) line cards are supported:
 - 4-port OC-3c/STM-1c POS/SDH ISE
 - 8-port OC-3c/STM-1c POS/SDH ISE
 - 16-port OC-3c/STM-1c POS/SDH ISE
 - 4-port OC-12c/STM-4c POS/SDH ISE
 - 1-port OC-48c/STM-16c POS/SDH ISE
 - 4-port channelized OC-12/STM-4 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE
 - 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE
 - 4-port OC-12c/STM-4c DPT ISE

Cisco 10000 Series Internet Router Platform Restrictions

- When configuring boot variables, booting from the TFTP boot server is not supported except on Cisco 10000 series Internet routers only.
- Both RPs must run the same Cisco software image. If the RPs are operating different Cisco software images, the system reverts to RPR mode even if SSO is configured. On the Cisco 10000 series Internet router, the system reverts to RPR+ mode.
- If a switchover occurs before the bulk synchronization step is complete, the new active RP may be in an inconsistent state. The router will be reloaded in this case.
- SSO supports TFTP boot operation on the Cisco 10000 series Internet routers.
- The following line cards support SSO and Cisco NSF:
 - 6-port Universal (Channelized or Clear-channel) DS3
 - 8-port E3/DS3
 - 1-port OC-12 POS
 - 6-port OC-3 POS
 - 1-port Gigabit Ethernet
 - 1-port Channelized OC-12

- 4-port Channelized STM1
- 24-port channelized E1/T1
- 1-port OC-12 ATM
- 4-port OC-3 ATM

Cisco 7500 Series Internet Router Platform Restrictions

- On the Cisco 7500 series routers, if any changes to the fabric configuration happen simultaneously with an RP switchover, the chassis is reset and all line cards are reset.
- On Cisco 7500 series routers configured for SSO mode, during synchronization between the active and standby RPs, the configured mode will be RPR. After the synchronization is complete, the operating mode will be SSO. If a switchover occurs before the synchronization is complete, the switchover will be in RPR mode.
- On Cisco 7500 series routers, legacy IPs will default to RPR mode and must be reloaded. If three or more legacy IPs are present, then all the line cards, including the VIPs, must be reloaded.
- SSO does not support TFTP boot operation on the Cisco 7500 series Internet routers. The software images must be downloaded to the flash memory cards on the router.
- SSO operates only on a Cisco 7500 series Internet router that has VIPs as the port adapters. Systems with legacy interface processors not compatible with RPR+ or SSO mode will always get reset and reloaded upon switchover.
- To support SSO, a router must have either a combination of two RSP8 and RSP16 devices or a combination of RSP2 and RSP4 devices. A combination of RSP8 or RSP16 with RSP2 or RSP4 devices on a platform is not supported. Only the Cisco 7507 and Cisco 7513 support dual processors, which is required to support SSO.
- Simultaneous changes to the configuration from multiple CLI sessions is not allowed. Only one configuration session is allowed to enter into configuration mode at a time, other sessions will not be able to enter into configuration mode.
- Using “send break” to break or pause the system is not recommended and may cause unpredictable results. To initiate a manual switchover, use the **redundancy force-switchover** command.
- The following line cards support SSO and Cisco NSF:
 - PA-MC-E3, 1-port multichannel E3 port adapter (PA)
 - PA-MC-T3, 1-port multichannel T3 PA
 - PA-MC-2E1/120, 2-port multichannel E1 PA with G.703 120-ohm interface
 - PA-MC-2TE1, 2-port multichannel T1 PA with integrated channel service unit (CSU) and data service unit (DSU) devices
 - PA-MC-2T3+, 2-port multichannel T3 PA
 - PA-MC-4T, 4-port multichannel T1 PA with integrated CSU and DSU devices
 - PA-MC-8T1, 8-port multichannel T1 PA with integrated CSU and DSU devices
 - PA-MC-8DSX1, 8-port multichannel DS1 PA with integrated DSUs
 - PA-MC-8E1/120, 8-port multichannel E1 PA with G.703 120-ohm interface
 - PA-4T+, 4-port serial PA enhanced
 - PA-8T-V35, 8-port serial V.35 PA
 - PA-8T-232, 8-port serial 232 PA
 - PA-8T-X21, 8-port serial X.21 PA
 - PA-E3, 1-port E3 serial PA with E3 DSU
 - PA-T3+, 1-port T3 serial PA enhanced
 - PA-2E3, 2-port E3 serial PA with E3 DSUs

- PA-2T3+, 2-port T3 serial PA enhanced
- PA-H, 1-port High-Speed Serial Interface (HSSI) PA
- PA-2H, 2-port HSSI PA
- PA-2FE-TX, 2-port Ethernet 100BASE-TX PA
- PA-2FE-FX, 2-port Ethernet 100BASE-FX PA
- PA-FE-TX, 1-port Fast Ethernet 100BASE-TX PA
- PA-FE-FX, 1-port Fast Ethernet 100BASE-FX PA
- PA-4E 4-port, Ethernet 10BASE-T PA
- PA-8E 8-port, Ethernet 10BASE-T PA
- PA-A3-E3, 1-port ATM enhanced E3 PA
- PA-A3-T3, 1-port ATM enhanced DS3 PA
- PA-A3-OC3MM, 1-port ATM enhanced OC-3c/STM-1 multimode PA
- PA-A3-OC3SMI, 1-port ATM enhanced OC-3c/STM-1 single-mode (IR) PA
- PA-A3-OC3SML, 1-port ATM enhanced OC-3c/STM-1 single-model (LR) PA
- PA-POS-OC3MM, 1-port PoS OC-3c/STM-1 multimode PA
- PA-POS-OC3SMI, 1-port PoS OC-3c/STM-1 single-mode (IR) PA
- PA-POS-OC3SML, 1-port PoS OC-3c/STM-1 single-mode (LR) PA
- PA-A3-8E1IMA, 8-port ATM inverse multiplexer E1 (120-ohm) PA
- PA-A3-8T1IMA, 8-port ATM inverse multiplexer T1 PA
- PA-4E1G/75, 4-port E1 G.703 serial PA (75-ohm/unbalanced)
- PA-4E1G/120, 4-port E1 G.703 serial PA (120-ohm/balanced)
- PA-MCX-8TE1
- PA-MCX-4TE1
- PA-MCX-2TE1
- All VIP2 and VIP4 line cards
- PA/VIP Combinations: Gigabit-Ethernet IP (GEIP) and GEIP+

Cisco 7304 Router Platform Restrictions

- Switchovers in SSO mode will not cause the reset of any line cards.
- Interfaces on the RP itself are not stateful and will experience a reset across switchovers. The GE interfaces on the RPs are reset across switchovers and do not support SSO.
- SSO does not support TFTP boot operation on Cisco 7304 series routers. The software images must be downloaded to the flash memory cards on the router.
- On the Cisco 7304 routers, the two RPs must be the same type, either both NSE-100 or both NPE-G100. Mixing the two types is not supported.
- The presence of the PCI port adapter carrier card will force the system to fall back to the RPR redundancy mode.
- In Cisco IOS releases 12.2(20)S to 12.2(20)S2, the presence of the PA carrier card (7300-CC-PA) or the SPA carrier card (MSC-100) forces the system to RPR mode.
- In Cisco IOS Release 12.2(20)S3, both the PA carrier card and SPA carrier card support SSO mode. The PA carrier card does not support RPR+ mode.
- In Cisco IOS Release 12.2(20)S4 and later releases, all line cards support RPR+ and SSO modes.

Cisco ASR 1000 Series Routers Restrictions

- Only RPR and SSO are supported on the Cisco ASR 1000 series routers.
- RPR and SSO can be used on the Cisco ASR 1000 series router to enable a second Cisco software process on a single RP. This configuration option is only available on Cisco ASR 1002 and Cisco ASR 1004 routers. On all other Cisco ASR 1000 series routers, the second Cisco software process can run on the standby RP only.
- A second Cisco software process can only be enabled using RPR or SSO if the RP is using 4 GB of DRAM. The **show version** command output shows the amount of DRAM configured on the router.

Information About Stateful Switchover

- [SSO Overview, page 9](#)
- [Redundancy Modes, page 11](#)
- [Route Processor Synchronization, page 14](#)
- [Switchover Operation, page 16](#)
- [Virtual Template Manager for SSO, page 18](#)
- [SSO-Aware Protocols and Applications, page 18](#)

SSO Overview

SSO provides protection for network edge devices with dual RPs that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

In Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

On Cisco ASR 1000 series routers, SSO can also be used to enable a second Cisco software process on the same RP. This second Cisco IOS process acts as a standby process for the active Cisco software process, and also allows certain subpackages to be upgraded without experiencing any router downtime.

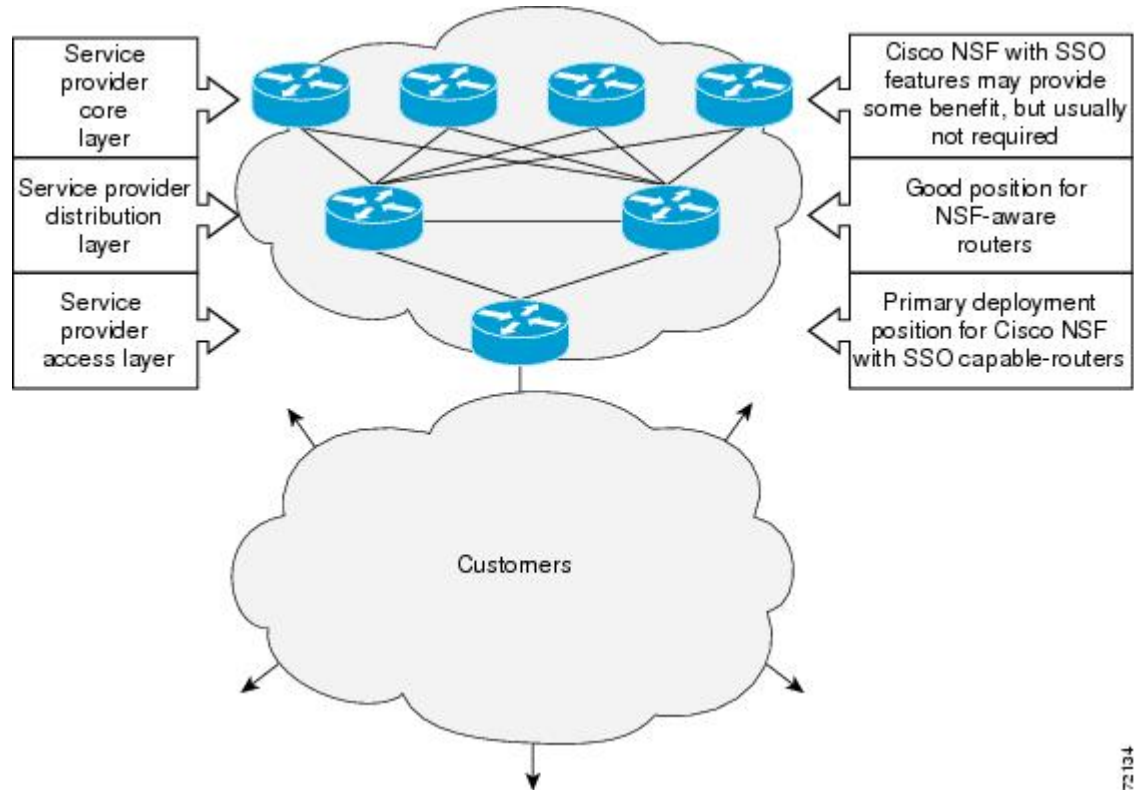
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

SSO is used with the Cisco Nonstop Forwarding (NSF) feature. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, thereby reducing loss of service outages for customers.

The figure below illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is primarily at the access layer (edge) of the service provider network. A fault at this

point could result in loss of service for enterprise customers requiring access to the service provider network.

Figure 1: Cisco NSF with SSO Network Deployment: Service Provider Networks

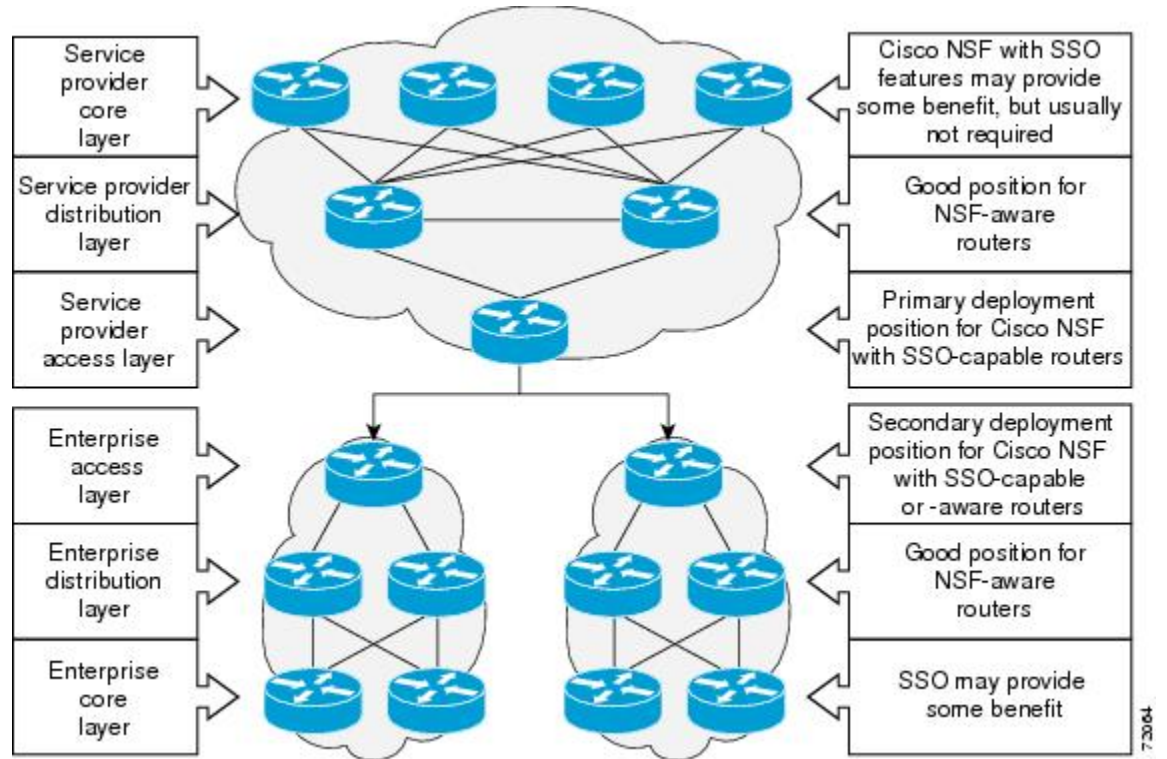


For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF and SSO features at the core layer of your network; however, consult your network design engineers to evaluate your specific site requirements.

Additional levels of availability may be gained by deploying Cisco NSF with SSO at other points in the network where a single point of failure exists. The figure below illustrates an optional deployment strategy that applies Cisco NSF with SSO at the enterprise network access layer. In this example, each access point in the enterprise network represents another single point of failure in the network design. In the event of a

switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Figure 2: Cisco NSF with SSO Network Deployment: Enterprise Networks



Redundancy Modes

- [High System Availability, page 11](#)
- [Route Processor Redundancy Mode, page 11](#)
- [Route Processor Redundancy Plus, page 12](#)
- [Stateful Switchover Mode, page 12](#)
- [Redundancy Modes by Platform and Software Release, page 12](#)

High System Availability

HSA mode allows you to install two RPs in a single router to improve system availability. This mode is available only on Cisco 7500 series routers. Supporting two RPs in a router provides the most basic level of increased system availability through a “cold restart” feature. A cold restart means that when one RP fails, the other RP reboots the router. Thus, the router is never in a failed state for very long, thereby increasing system availability.

Route Processor Redundancy Mode

Router Processor Redundancy (RPR) allows Cisco software to be booted on the standby processor prior to switchover (a cold boot). In RPR, the standby RP loads a Cisco software image at boot time and initializes

itself in standby mode; however, although the startup configuration is synchronized to the standby RP, system changes are not. In the event of a fatal error on the active RP, the system switches to the standby processor, which reinitializes itself as the active processor, reads and parses the startup configuration, reloads all of the line cards, and restarts the system.

Route Processor Redundancy Plus

In RPR+ mode, the standby RP is fully initialized. For RPR+ both the active RP and the standby RP must be running the same software image. The active RP dynamically synchronizes startup and the running configuration changes to the standby RP, meaning that the standby RP need not be reloaded and reinitialized (a hot boot).

Additionally, on the Cisco 10000 and 12000 series Internet routers, the line cards are not reset in RPR+ mode. This functionality provides a much faster switchover between the processors. Information synchronized to the standby RP includes running configuration information, startup information (Cisco 7304, Cisco 7500, Cisco 10000, and Cisco 12000 series networking devices), and changes to the chassis state such as online insertion and removal (OIR) of hardware. Line card, protocol, and application state information is not synchronized to the standby RP.

Stateful Switchover Mode

SSO mode provides all the functionality of RPR+ in that Cisco software is fully initialized on the standby RP. In addition, SSO supports synchronization of line card, protocol, and application state information between RPs for supported features and protocols (a hot standby).

Redundancy Modes by Platform and Software Release



Note

During normal operation, SSO is the only supported mode for the Cisco 10000 series Internet routers.

The five tables below show redundancy modes by platform and release.

Table 1: Redundancy Modes by Platform in Cisco IOS Release 12.2S

Platform	Mode	12.2 (18)S	12.2 (20)S	12.2 (25)S
7304	HSA	No	Yes	Yes
	RPR	No	Yes	Yes
	RPR+	No	Yes	Yes
	SSO	--	Yes	Yes
7500	HSA	Yes	No	Yes
	RPR	Yes	No	Yes
	RPR+	Yes	No	Yes
	SSO	Yes	No	Yes

Table 2: Redundancy Modes by Platform in Cisco IOS Release 12.2SB

Platform	Mode	12.2(28)SB	12.2(31)SB2
7304	HSA	No	Yes
	RPR	No	Yes
	RPR+	No	Yes
	SSO	No	Yes
10000	HSA	No	No
	RPR	Yes	Yes
	RPR+	Yes	Yes
	SSO	Yes	Yes

Table 3: Redundancy Modes by Platform in Cisco IOS Release 12.2SR

Platform	Mode	12.2 (33) SRA	12.2(33) SRB	12.2(33) SRC
7600	HSA	No	No	No
	RPR	Yes	Yes	Yes
	RPR+	Yes	Yes	Yes
	SSO	Yes	Yes	Yes

Table 4: Redundancy Modes by Platform in Cisco IOS Release 12.2SX

Platform	Mode	12.2 (33)SXH
CAT6500	HSA	No
	RPR	Yes
	RPR+	Yes
	SSO	Yes

Table 5: Redundancy Modes by Platform in Cisco IOS Release 12.0S

Platform	Mode	Redundancy Mode Support in Cisco IOS Software Releases
12.0(22)S	12.0(23)S	12.0(24)S 12.0(26)S 12.0(28)S

Platform	Mode	Redundancy Mode Support in Cisco IOS Software Releases				
7500	HSA	Yes	Yes	Yes	Yes	Yes
	RPR	Yes	Yes	Yes	Yes	Yes
	RPR+	Yes	Yes	Yes	Yes	Yes
	SSO	Yes	Yes	Yes	Yes	Yes
10000	HSA	No	No	No	No	No
	RPR	No	No	No	No	No
	RPR+	Yes	Yes	Yes	Yes	Yes
	SSO	Yes	Yes	Yes	Yes	Yes
12000	HSA	No	No	No	No	No
	RPR	Yes	Yes	Yes	Yes	Yes
	RPR+	Yes	Yes	Yes	Yes	Yes
	SSO	Yes	Yes	Yes	Yes	Yes

Route Processor Synchronization

In networking devices running SSO, both RPs must be running the same configuration so that the standby RP is always ready to assume control if the active RP fails.

To achieve the benefits of SSO, synchronize the configuration information from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. This synchronization occurs in two separate phases:

- While the standby RP is booting, the configuration information is synchronized in bulk from the active RP to the standby RP.
- When configuration or state changes occur, an incremental synchronization is conducted from the active RP to the standby RP.
- [Bulk Synchronization During Initialization, page 14](#)
- [Incremental Synchronization, page 15](#)

Bulk Synchronization During Initialization

When a system with SSO is initialized, the active RP performs a chassis discovery (discovery of the number and type of line cards and fabric cards, if available, in the system) and parses the startup configuration file.

The active RP then synchronizes this data to the standby RP and instructs the standby RP to complete its initialization. This method ensures that both RPs contain the same configuration information.

Even though the standby RP is fully initialized, it interacts only with the active RP to receive incremental changes to the configuration files as they occur. Executing CLI commands on the standby RP is not supported.

During system startup, the startup configuration file is copied from the active RP to the standby RP. Any existing startup configuration file on the standby RP is overwritten. The startup configuration is a text file stored in the NVRAM of the RP. It is synchronized whenever you perform the following operations:

- The command **copy system:running-config nvram:startup-config** is used.
- The command **copy running-config startup-config** is used.
- The command **write memory** is used.
- The command **copy filename nvram:startup-config** is used.
- SNMP SET of MIB variable ccCopyEntry in CISCO_CONFIG_COPY MIB is used.
- System configuration is saved using the **reload** command.
- System configuration is saved following entry of a forced switchover command.

Incremental Synchronization

After both RPs are fully initialized, any further changes to the running configuration or active RP states are synchronized to the standby RP as they occur. Active RP states are updated as a result of processing protocol information, external events (such as the interface becoming up or down), or user configuration commands (using Cisco IOS commands or Simple Network Management Protocol [SNMP]) or other internal events.

Changes to the running configuration are synchronized from the active RP to the standby RP. In effect, the command is run on both the active and the standby RP.

Configuration changes caused by an SNMP set operation are synchronized on a case-by-case basis. Only two SNMP configuration set operations are supported:

- **shut** and **no-shut** (of an interface)
- **link up/down trap enable/disable**

Routing and forwarding information is synchronized to the standby RP:

- State changes for SSO-aware protocols (ATM, Frame Relay, PPP, High-Level Data Link Control [HDLC]) or applications (SNMP) are synchronized to the standby RP.
- Cisco Express Forwarding (CEF) updates to the Forwarding Information Base (FIB) are synchronized to the standby RP.

Chassis state changes are synchronized to the standby RP. Changes to the chassis state due to line card insertion or removal are synchronized to the standby RP.

Changes to the line card states are synchronized to the standby RP. Line card state information is initially obtained during bulk synchronization of the standby RP. Following bulk synchronization, line card events, such as whether the interface is up or down, received at the active processor are synchronized to the standby RP.

The various counters and statistics maintained in the active RP are not synchronized because they may change often and because the degree of synchronization they require is substantial. The volume of information associated with statistics makes synchronizing them impractical.

Not synchronizing counters and statistics between RPs may create problems for external network management systems that monitor this information.

Switchover Operation

- [Switchover Conditions, page 16](#)
- [Switchover Time, page 16](#)
- [Online Removal of the Active RP, page 17](#)
- [Single Line Card Reload, page 17](#)
- [Fast Software Upgrade, page 17](#)
- [Core Dump Operation, page 18](#)

Switchover Conditions

An automatic or manual switchover may occur under the following conditions:

- A fault condition that causes the active RP to crash or reboot--automatic switchover
- The active RP is declared dead (not responding)--automatic switchover
- The command is invoked--manual switchover

The user can force the switchover from the active RP to the standby RP by using a CLI command. This manual procedure allows for a graceful or controlled shutdown of the active RP and switchover to the standby RP. This graceful shutdown allows critical cleanup to occur.

**Note**

This procedure should not be confused with the graceful shutdown procedure for routing protocols in core routers--they are separate mechanisms.

**Caution**

The SSO feature introduces a number of new command and command changes, including commands to manually cause a switchover. The **reload** command does not cause a switchover. The **reload** command causes a full reload of the box, removing all table entries, resetting all line cards, and interrupting nonstop forwarding.

Switchover Time

The time required by the device to switch over from the active RP to the standby RP varies by platform:

- On the Cisco 7500 series devices, switchover time is approximately 30 seconds.
- On the Cisco 7304 and Cisco 10000 series devices, switchover time is only a few seconds.
- On the Cisco 12000 series devices, switchover time due to a manual switchover or due to automatic switchover caused by an error is only a few seconds. If the switchover is caused by a fault on the active RP, the standby RP will detect the problem following the switchover timeout period, which is set to three seconds by default.
- On the Cisco ASR 1000 series routers, switchover time is only a few seconds.

Although the newly active processor takes over almost immediately following a switchover, the time required for the device to begin operating again in full redundancy (SSO) mode can be several minutes, depending on the platform. The length of time can be due to a number of factors including the time needed for the previously active processor to obtain crash information, load code and microcode, and synchronize configurations between processors and line protocols and Cisco NSF-supported protocols.

The impact of the switchover time on packet forwarding depends on the networking device:

- On the Cisco 7500 series devices, forwarding information is distributed, and packets forwarded from the same line card should have little to no forwarding delay; however, forwarding packets between line cards requires interaction with the RP, meaning that packet forwarding might have to wait for the switchover time. The switchover time on Cisco 7500 series devices is also dependent on the type of RSPs installed on the system.
- On the Cisco 10000 series devices, Cisco Express Forwarding information resides on the RP, so packet forwarding can be impacted momentarily while the switchover occurs.
- On the Cisco 12000 series devices, complete forwarding information is distributed to the line cards, so packet forwarding is not impacted as long as the line cards are working.

Online Removal of the Active RP

For Cisco 7500 series routers, online removal of the active RSP will automatically switch the redundancy mode to RPR. Online removal of the active RSP causes all line cards to reset and reload, which is equivalent to an RPR switchover, and results in a longer switchover time. When it is necessary to remove the active RP from the system, first issue a switchover command to switch from the active RSP to the standby RSP. When a switchover is forced to the standby RSP before the previously active RSP is removed, the network operation benefits from the continuous forwarding capability of SSO.

For Cisco 7304, Cisco 10000, and Cisco 12000 series Internet routers that are configured to use SSO, online removal of the active RP automatically forces a stateful switchover to the standby RP.

Single Line Card Reload

In Cisco 7500 series routers, a line card might fail to reach the quiescent state as a result of a hardware or software fault. In such cases, the failing line card must be reset. We recommend using the Single Line Card Reload (SLCR) feature to provide maximum assurance that SSO will continue forwarding packets on unaffected interfaces during switchover.



Note

SLCR is not required on the Cisco 7304 router or on Cisco 10000 and 12000 series Internet routers.

The SLCR feature allows users to correct a line card fault on a Cisco 7500 series router by automatically reloading the microcode on a failed line card. During the SLCR process, all physical lines and routing protocols on the other line cards of the network backplane remain active.

The SLCR feature is not enabled by default. When you enable SSO, RPR+, or RPR, it is important that you enable SLCR also. For information on how to load and configure SLCR, refer to the *Cisco 7500 Single Line Card Reload* feature module.

Fast Software Upgrade

You can use Fast Software Upgrade (FSU) to reduce planned downtime. With FSU, you can configure the system to switch over to a standby RP that is preloaded with an upgraded Cisco software image. FSU reduces outage time during a software upgrade by transferring functions to the standby RP that has the upgraded Cisco software preinstalled. You can also use FSU to downgrade a system to an older version of Cisco software or have a backup system loaded for downgrading to a previous image immediately after an upgrade.

SSO must be configured on the networking device before performing FSU.

**Note**

During the upgrade process, different images will be loaded on the RPs for a short period of time. During this time, the device will operate in RPR or RPR+ mode, depending on the networking device.

Core Dump Operation

In networking devices that support SSO, the newly active primary processor runs the core dump operation after the switchover has taken place. Not having to wait for dump operations effectively decreases the switchover time between processors.

Following the switchover, the newly active RP will wait for a period of time for the core dump to complete before attempting to reload the formerly active RP. The time period is configurable. For example, on some platforms an hour or more may be required for the formerly active RP to perform a core dump, and it might not be site policy to wait that much time before resetting and reloading the formerly active RP. In the event that the core dump does not complete within the time period provided, the standby is reset and reloaded regardless of whether it is still performing a core dump.

The core dump process adds the slot number to the core dump file to identify which processor generated the file content.

**Note**

Core dumps are generally useful only to your technical support representative. The core dump file, which is a very large binary file, must be transferred using the TFTP, FTP, or remote copy protocol (rcp) server and subsequently interpreted by a Cisco Technical Assistance Center (TAC) representative that has access to source code and detailed memory maps.

Virtual Template Manager for SSO

The virtual template manager feature for SSO provides virtual access interfaces for sessions that are not HA-capable and are not synchronized to the standby router. The virtual template manager uses a redundancy facility (RF) client to allow the synchronization of the virtual interfaces in real time as they are created.

The virtual databases have instances of distributed FIB entries on line cards. Line cards require synchronization of content and timing in all interfaces to the standby processor to avoid incorrect forwarding. If the virtual access interface is not created on the standby processor, the interface indexes will be corrupted on the standby router and line cards, which will cause problems with forwarding.

SSO-Aware Protocols and Applications

SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

SSO-aware applications are either platform-independent, such as in the case of line protocols or platform-dependent (such as line card drivers). Enhancements to the routing protocols (Cisco Express Forwarding,

Open Shortest Path First, and Border Gateway Protocol [BGP]) have been made in the SSO feature to prevent loss of peer adjacency through a switchover; these enhancements are platform-independent.

- [Line Protocols, page 19](#)
- [Quality of Service, page 24](#)
- [IPv6 Support for Stateful Switchover, page 24](#)
- [Line Card Drivers, page 24](#)
- [APS, page 24](#)
- [Routing Protocols and Nonstop Forwarding, page 25](#)
- [Network Management, page 25](#)
- [SSO for Circuit Emulation Services, page 25](#)

Line Protocols

SSO-aware line protocols synchronize session state information between the active and standby RPs to keep session information current for a particular interface. In the event of a switchover, session information need not be renegotiated with the peer. During a switchover, SSO-aware protocols also check the line card state to learn if it matches the session state information. SSO-aware protocols use the line card interface to exchange messages with network peers in an effort to maintain network connectivity.

- [Supported Line protocols by Platform, page 19](#)
- [ATM Stateful Switchover, page 21](#)
- [Frame Relay and Multilink Frame Relay Stateful Switchover, page 22](#)
- [PPP and Multilink PPP Stateful Switchover, page 23](#)
- [HDLC Stateful Switchover, page 23](#)

Supported Line protocols by Platform

The five tables below indicate which line protocols are supported on various platforms and releases.

Table 6: Line Protocol Support in Cisco IOS Release 12.2S

Protocol	Platform	12.2 (18)S	12.2 (20)S	12.2 (25)S
ATM	Cisco 7304	No	Yes	Yes
	Cisco 7500	Yes	No	Yes
Frame Relay and Multilink Frame Relay	Cisco 7304	No	Yes	Yes
	Cisco 7500	Yes	No	Yes
PPP and Multilink PPP	Cisco 7304	No	Yes	Yes
	Cisco 7500	Yes	No	Yes
HDLC	Cisco 7304	No	Yes	Yes
	Cisco 7500	Yes	No	Yes

Table 7: Line Protocol Support in Cisco IOS Release 12.2SB

Protocol	Platform	12.2 (28)SB	12.2(31)SB2
ATM	Cisco 7304	Yes	Yes
	Cisco 10000	Yes	Yes
Frame Relay and Multilink Frame Relay	Cisco 7304	Yes	Yes
	Cisco 10000	Yes	Yes
PPP and Multilink PPP	Cisco 7304	Yes	Yes
	Cisco 10000	Yes	Yes
HDLC	Cisco 7304	Yes	Yes
	Cisco 10000	Yes	Yes

Table 8: Line Protocol Support in Cisco IOS Release 12.2SR

Protocol	Platform	12.2(33)SRA	12.2(33)SRB	12.2(33)SRC
ATM	Cisco 7600	Yes	Yes	Yes
Frame Relay and Multilink Frame Relay	Cisco 7600	Yes	Yes	Yes
PPP and Multilink PPP	Cisco 7600	Yes	Yes	Yes
HDLC	Cisco 7600	Yes	Yes	Yes

Table 9: Line Protocol Support in Cisco IOS Release 12.2SX

Protocol	Platform	12.2(33)SXH
ATM	Cisco CAT6500	Yes
	Cisco 7600	Yes
Frame Relay and Multilink Frame Relay	Cisco CAT6500	Yes ¹
	Cisco 7600	Yes
PPP and Multilink PPP	Cisco CAT6500	Yes
	Cisco 7600	Yes
HDLC	Cisco CAT6500	Yes
	Cisco 7600	Yes

¹ Frame Relay is supported, but Multilink Frame Relay is not.

Table 10: Line Protocol Support in Cisco IOS Release 12.0S

Protocol	Platform	12.0 (22)S	12.0 (23)S	12.0 (24)S	12.0 (26)S	12.0(28)S
ATM	Cisco 7500	Yes	Yes	Yes	Yes	Yes
	Cisco 10000	Yes	Yes	Yes	Yes	Yes
	Cisco 12000	Yes	Yes	Yes	Yes	Yes
Frame Relay and Multilink Frame Relay	Cisco 7500	Yes	Yes	Yes	Yes	Yes
	Cisco 10000	Yes	Yes	Yes	Yes	Yes
	Cisco 12000	No	No	No	No	Yes
PPP and Multilink PPP	Cisco 7500	Yes	Yes	Yes	Yes	Yes
	Cisco 10000	Yes	Yes	Yes	Yes	Yes
	Cisco 12000	Yes	Yes	Yes	Yes	Yes
HDLC	Cisco 7500	Yes	Yes	Yes	Yes	Yes
	Cisco 10000	Yes	Yes	Yes	Yes	Yes
	Cisco 12000	Yes	Yes	Yes	Yes	Yes

ATM Stateful Switchover

With stateful switchover, ATM dynamic state information is synchronized between the active RP and standby RP. Thus when the active RP fails, the standby RP can take over without spending excessive time relearning the dynamic state information, and forwarding devices can continue to forward packets with only a few seconds of interruption (less on some platforms).



Note

ATM SSO is not configurable and runs by default on networking devices configured with ATM and Redundancy Mode SSO.

Permanent Virtual Circuits

For ATM to support forwarding during and after switchover, ATM permanent virtual circuits (PVCs) must remain up not only within the networking device, but also within the ATM network.

In an ATM network, all traffic to or from an ATM interface is prefaced with a virtual path identifier (VPI) and virtual channel identifier (VCI). A VPI-VCI pair is considered a single virtual circuit. Each virtual circuit is a private connection to another node on the ATM network. In ATM SSO, the VPI-VCI pair is associated with a virtual circuit descriptor (VCD). ATM SSO uses VCD information in synchronizing VPI-VCI information to the standby RP.

Each virtual circuit is treated as a point-to-point or point-to-multipoint mechanism to another networking device or host and can support bidirectional traffic. On point-to-point subinterfaces, or when static mappings are configured, Inverse Address Resolution Protocol (ARP) need not run. In cases where dynamic address mapping is used, an Inverse ARP protocol exchange determines the protocol address to VPI-VCI mapping for the PVC. This process occurs as soon as the PVC on a multipoint subinterface makes

the transition to active. If that process fails for some reason, the remote networking device may drop the Inverse ARP request if it has not yet seen the PVC transition to active. Inverse ARP runs every 60 seconds to relearn the dynamic address mapping information for the active RP.

ATM OAM Managed PVC or SVC Timeout

Operation, Administration, and Maintenance (OAM) F5 loopback cells must be echoed back on receipt by the remote host, thus demonstrating connectivity on the PVC between the router and the remote host. With ATM SSO, OAM loopback cells received on an interface must be echoed within 15 seconds before a PVC or switched virtual circuit (SVC) is declared down. By default, the OAM timeout is set to 10 seconds, followed by at most five retries sent at 1-second intervals. In the worst case, a switchover will begin just before expiration of the 10-second period, meaning that the PVC will go down within 5 seconds on the remote networking device if switchover has not completed within 5 seconds.



Note

Timers at remote ATM networking devices may be configurable, depending on the remote device owner.

Frame Relay and Multilink Frame Relay Stateful Switchover

With stateful switchover, Frame Relay and Multilink Frame Relay dynamic state information is synchronized between the active RP and standby RP. Thus when the active RP fails, the standby RP can take over without spending excessive time relearning the dynamic state information, and forwarding devices can continue to forward packets with only a few seconds of interruption (less on some platforms).

Permanent Virtual Circuits

For Frame Relay and Multilink Frame Relay to support forwarding during and after switchover, Frame Relay PVCs must remain up not only within the networking device, but also within the Frame Relay network.

In many cases the networking devices are connected to a switch, rather than back-to-back to another networking device, and that switch is not running Cisco software. The virtual circuit state is dependent on line state. PVCs are down when the line protocol is down. PVCs are up when the line protocol is up and the PVC status reported by the adjacent switch is active.

On point-to-point subinterfaces, or when static mappings are configured, Inverse ARP need not run. In cases where dynamic address mapping is used, an Inverse ARP protocol exchange determines the protocol address to data-link connection identifier (DLCI) mapping for the PVC. This exchange occurs as soon as the multipoint PVC makes the transition to active. If the exchange fails for some reason, for example, the remote networking device may drop the Inverse ARP request if it has not yet seen the PVC transition to active--any outstanding requests are run off a timer, with a default of 60 seconds.

Keepalive Messages

A crucial factor in maintaining PVCs is the delivery of Local Management Interface (LMI) protocol messages (keepalives) during switchover. This keepalive mechanism provides an exchange of information between the network server and the switch to verify that data is flowing.

If a number of consecutive LMI keepalives messages are lost or in error, the adjacent Frame Relay device declares the line protocol down and all PVCs on that interface are declared down within the Frame Relay network and reported as such to the remote networking device. The speed with which a switchover occurs is crucial to avoid the loss of keepalive messages.

The line protocol state depends on the Frame Relay keepalive configuration. With keepalives disabled, the line protocol is always up as long as the hardware interface is up. With keepalives enabled, LMI protocol

messages are exchanged between the networking device and the adjacent Frame Relay switch. The line protocol is declared up after a number of consecutive successful LMI message exchanges.

The line protocol must be up according to both the networking device and the switch. The default number of exchanges to bring up the line protocol is implementation-dependent: Three is suggested by the standards; four is used on a Cisco Frame Relay switch, taking 40 seconds at the default interval of 10 seconds; and two is used on a Cisco networking device acting as a switch or when connected back-to-back. This default number could be extended if the LMI “autosense” feature is being used while the LMI type expected on the switch is determined. The number of exchanges is configurable, although the switch and router may not have the same owner.

The default number of lost messages or errors needed to bring down the line is three (two on a Cisco router). By default, if a loss of two messages is detected in 15 to 30 seconds, then a sequence number or LMI type error in the first message from the newly active RP takes the line down.

If a line goes down, consecutive successful LMI protocol exchanges (default of four over 40 seconds on a Cisco Frame Relay switch; default of two over 20 seconds on a Cisco device) will bring the line back up again.

PPP and Multilink PPP Stateful Switchover

With stateful switchover, specific PPP state information is synchronized between the active RP and standby RP. Thus when the active RP fails, the standby RP can take over without spending excessive time renegotiating the setup of a given link. As long as the physical link remains up, forwarding devices can continue to forward packets with only a few seconds of interruption (less on some platforms). Single-link PPP and Multilink PPP (MLP) sessions are maintained during RP switchover for IP connections only.

PPP and MLP support many Layer 3 protocols such as IPX and IP. Only IP links are supported in SSO. Links supporting non IP traffic will momentarily renegotiate and resume forwarding following a switchover. IP links will forward IP traffic without renegotiation.

A key factor in maintaining PPP session integrity during a switchover is the use of keepalive messages. This keepalive mechanism provides an exchange of information between peer interfaces to verify data and link integrity. Depending on the platform and configuration, the time required for switchover to the standby RP might exceed the keepalive timeout period. PPP keepalive messages are started when the physical link is first brought up. By default, keepalive messages are sent at 10-second intervals from one PPP interface to the other PPP peer.

If five consecutive keepalive replies are not received, the PPP link would be taken down on the newly active RP. Caution should be used when changing the keepalive interval duration to any value less than the default setting.

Only in extremely rare circumstances could the RP switchover time exceed the default 50-second keepalive duration. In the unlikely event this time is exceeded, the PPP links would renegotiate with the peers and resume IP traffic forwarding.

**Note**

PPP and MLP are not configurable and run by default on networking devices configured with SSO.

HDLC Stateful Switchover

With stateful switchover, High-Level Data Link Control (HDLC) synchronizes the line protocol state information. Additionally, the periodic timer is restarted for interfaces that use keepalive messages to verify link integrity. Link state information is synchronized between the active RP and standby RP. The line

protocols that were up before the switchover remain up afterward as long as the physical interface remains up. Line protocols that were down remain down.

A key factor in maintaining HDLC link integrity during a switchover is the use of keepalive messages. This keepalive mechanism provides an exchange of information between peer interfaces to verify data is flowing. HDLC keepalive messages are started when the physical link is first brought up. By default, keepalive messages are sent at 10-second intervals from one HDLC interface to the other.

HDLC waits at least three keepalive intervals without receiving keepalive messages, sequence number errors, or a combination of both before it declares a line protocol down. If the line protocol is down, SSO cannot support continuous forwarding of user session information in the event of a switchover.

**Note**

HDLC is not configurable and runs by default on networking devices configured with SSO.

Quality of Service

The modular QoS CLI (MQS)-based QoS feature maintains a database of various objects created by the user, such as those used to specify traffic classes, actions for those classes in traffic policies, and attachments of those policies to different traffic points such as interfaces. With SSO, QoS synchronizes that database between the primary and secondary RP.

IPv6 Support for Stateful Switchover

IPv6 neighbor discovery supports SSO using Cisco Express Forwarding. When switchover occurs, the Cisco Express Forwarding adjacency state, which is checkpointed, is used to reconstruct the neighbor discovery cache.

Line Card Drivers

Platform-specific line card device drivers are bundled with the Cisco software image for SSO and are correct for a specific image, meaning they are designed to be SSO-aware.

Line cards used with the SSO feature periodically generate status events that are forwarded to the active RP. Information includes the line up or down status, and the alarm status. This information helps SSO support bulk synchronization after standby RP initialization and support state reconciliation and verification after a switchover.

Line cards used with the SSO feature also have the following requirements:

- Line cards must not reset during switchover.
- Line cards must not be reconfigured.
- Subscriber sessions may not be lost.

**Note**

The standby RP communicates only with the active RP, never with the line cards. This function helps to ensure that the active and standby RP always have the same information.

APS

RPR+ and SSO support allow the automatic protection switching (APS) state to be preserved in the event of failover.

Routing Protocols and Nonstop Forwarding

Cisco nonstop forwarding (NSF) works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. When a networking device restarts, all routing peers of that device usually detect that the device went down and then came back up. This down-to-up transition results in what is called a “routing flap,” which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Cisco NSF helps to suppress routing flaps, thus improving network stability.

Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards to remain up through a switchover and to be kept current with the FIB on the active RP is key to Cisco NSF operation.

A key element of Cisco NSF is packet forwarding. In Cisco networking devices, packet forwarding is provided by Cisco Express Forwarding. Cisco Express Forwarding maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature eliminates downtime during the switchover.

Cisco NSF supports the BGP, IS-IS, and OSPF routing protocols. In general, these routing protocols must be SSO-aware to detect a switchover and recover state information (converge) from peer devices. Each protocol depends on Cisco Express Forwarding to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables.

**Note**

Distributed Cisco Express Forwarding must be enabled in order to run NSF.

Network Management

Network management support for SSO is provided through the synchronization of specific SNMP data between the active and standby RPs. From a network management perspective, this functionality helps to provide an uninterrupted management interface to the network administrator.

**Note**

Synchronization of SNMP data between RPs is available only when the networking device is operating in SSO mode.

SSO for Circuit Emulation Services

SSO for circuit emulation services (CES) for TDM pseudowires provides the ability to switch an incoming DS1/T1/E1 on one SPA to another SPA on same SIP or onto a different SIP.

How to Configure Stateful Switchover

- [Copying an Image onto an RP, page 26](#)

- [Setting the Configuration Register and Boot Variable, page 27](#)
- [Configuring SSO, page 28](#)
- [Configuring Frame Relay and Multilink Frame Relay Autosynchronization LMI Sequence Numbers, page 29](#)
- [Verifying SSO Configuration, page 30](#)
- [Performing a Fast Software Upgrade, page 31](#)
- [Troubleshooting Stateful Switchover, page 33](#)

Copying an Image onto an RP



Note

To copy a consolidated package or subpackages onto active and standby RPs on the Cisco ASR 1000 Series Router, see the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

SUMMARY STEPS

1. `enable`
2. `copy tftp {slot | disk}device-number : filename`
3. `copy tftp {slave | stby-}{slot | disk}device-number : filename`
4. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>copy tftp {slot disk}device-number : filename</code></p> <p>Example:</p> <pre>Router# copy tftp slot0:image1</pre>	<p>Copies a Cisco software image onto the flash device of the active RP.</p>
Step 3	<p><code>copy tftp {slave stby-}{slot disk}device-number : filename</code></p> <p>Example:</p> <pre>Router# copy tftp stby-slot0:image1</pre>	<p>Copies a Cisco software image onto the flash device of the standby RP.</p>
Step 4	<p><code>exit</code></p> <p>Example:</p> <pre>Router# exit</pre>	<p>Exits to user EXEC mode.</p>

Setting the Configuration Register and Boot Variable



Note

Following the reload, each RP is in its default mode: The Cisco 7304 router boots in SSO mode; the Cisco 7500 series router reboots in HSA mode; the Cisco 10000 series Internet router boots in SSO mode, and the Cisco 12000 series Internet router reboots in RPR mode.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **no boot system** { **flash** [*flash-fs*][:*partition-number*][:*filename*] | **ftpfilename** [*ip-address*]}
5. **boot system** { **flash** [*flash-fs*][:*partition-number*][:*filename*] | **tftpfilename** [*ip-address*]}
6. **config-register** *value*
7. **exit**
8. **copy running-config startup-config**
9. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show version Example: Router# show version	Obtains the current configuration register setting.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	no boot system { flash [<i>flash-fs</i>][: <i>partition-number</i>][: <i>filename</i>] ftpfilename [<i>ip-address</i>]} Example: Router(config)# no boot system flash	(Optional) Clears any existing system flash or TFTP boot image specification.
Step 5	boot system { flash [<i>flash-fs</i>][: <i>partition-number</i>][: <i>filename</i>] tftpfilename [<i>ip-address</i>]}	Specifies the filename of stored image in flash memory or, for Cisco 10000, on a TFTP server.

	Command or Action	Purpose
	<p>Example:</p> <p>Example:</p> <pre>Router(config)# boot system flash</pre>	
Step 6	<p>config-register <i>value</i></p> <p>Example:</p> <pre>Router(config)# config-register 0x2102</pre>	Modifies the existing configuration register setting to reflect the way in which you want to load a system image.
Step 7	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Router# copy running-config startup-config</pre>	Saves the configuration changes to the startup configuration file.
Step 9	<p>reload</p> <p>Example:</p> <pre>Router# reload</pre>	Reboots both RPs on the device to ensure that changes to the configuration take effect.

Configuring SSO



Note

Cisco 7304 routers and Cisco 10000 series Internet routers operate in SSO mode by default after reloading the same version of SSO-aware images on the device. No configuration is necessary.

Image to be used by active or standby RP at initialization must be available on the local flash device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hw-module slot** *slot-number* **image** *file-spec*
4. **redundancy**
5. **mode sso**
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	hw-module slot <i>slot-number</i> image <i>file-spec</i> Example: Router(config)# hw-module slot 6 image slot0:rsp-pv-mz	(Optional) For Cisco 7500 series devices only. Specifies the image to be used by an RP at initialization. <ul style="list-style-type: none"> Repeat this step for both the active and standby RPs.
Step 4	redundancy Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 5	mode sso Example: Router(config)# mode sso	Sets the redundancy configuration mode to SSO on both the active and standby RP. <p>NoteAfter configuring SSO mode, the standby RP will automatically reset.</p>
Step 6	end Example: Router(config-red)# end	Exits redundancy configuration mode and returns the router to privileged EXEC mode.
Step 7	copy running-config startup-config Example: Router# copy running-config startup-config	Saves the configuration changes to the startup configuration file.

Configuring Frame Relay and Multilink Frame Relay Autosynchronization LMI Sequence Numbers

SUMMARY STEPS

1. enable
2. configure terminal
3. frame-relay redundancy auto-sync lmi-sequence-numbers

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	frame-relay redundancy auto-sync lmi-sequence-numbers Example: Router(config)# frame-relay redundancy auto-sync lmi-sequence-numbers	Configures automatic synchronization of Frame Relay LMI sequence numbers between the active RP and the standby RP.

Verifying SSO Configuration**SUMMARY STEPS**

1. enable
2. show redundancy [clients | counters | history | switchover history | states]
3. show redundancy states

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show redundancy [clients counters history switchover history states]	Displays SSO configuration information.

	Command or Action	Purpose
	Example: Router# show redundancy	
Step 3	show redundancy states Example: Router# show redundancy states	Verifies that the device is running in SSO mode.

Performing a Fast Software Upgrade



Note

During the upgrade process, different images will be loaded on the RPs for a very short period of time. If a switchover occurs during this time, the device will recover in HSA, RPR or RPR+ mode, depending on the networking device.

SUMMARY STEPS

1. enable
2. copy tftp {slot | disk} device-number:filename
3. copy tftp {slave | stby-} {slot | disk } device-number : filename
4. configure terminal
5. no hw-module slot slot-number image file-spec
6. hw-module slot slot-number image file-spec
7. no boot system flash [flash-fs:][partition-number:][filename]
8. boot system flash [flash-fs:][partition-number:][filename]
9. config-register value
10. exit
11. copy running-config startup-config
12. hw-module standby-cpu reset
13. reload standby-cpu
14. redundancy force-switchover [main-cpu]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	<p>copy tftp {slot disk}<i>device-number:filename</i></p> <p>Example:</p> <pre>Router# copy tftp slot0:image1</pre>	Copies a Cisco software image onto the flash device of the active RP.
Step 3	<p>copy tftp {slave stby-}{slot disk } <i>device-number : filename</i></p> <p>Example:</p> <pre>Router# copy tftp stby-slot0:image1</pre> <p>Example:</p>	Copies a Cisco software image onto the flash device of the standby RP.
Step 4	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 5	<p>no hw-module slot <i>slot-number image file-spec</i></p> <p>Example:</p> <pre>Router(config)# no hw-module slot 6 image slot0:rsp-pv-mz</pre>	<p>For Cisco 7500 series routers only. Clears existing configuration entries for the specified image on an RSP. Configuration entries are additive, and the networking device will use the first image found in the configuration file.</p> <ul style="list-style-type: none"> Repeat this step for both the active and standby RSPs.
Step 6	<p>hw-module slot <i>slot-number image file-spec</i></p> <p>Example:</p> <pre>Router(config)# hw-module slot 6 image slot0:image1</pre>	<p>For Cisco 7500 series routers only. Specifies the image to be used by the RSP at initialization. Configuration entries are additive, and the networking device will use the first image found in the configuration file.</p> <ul style="list-style-type: none"> Repeat this step for both the active and standby RSPs.
Step 7	<p>no boot system flash [<i>flash-fs:</i>][<i>partition-number:</i>] [<i>filename</i>]</p> <p>Example:</p> <pre>Router(config)# no boot system flash</pre>	Clears the current boot image filename from the configuration file.
Step 8	<p>boot system flash [<i>flash-fs:</i>][<i>partition-number:</i>] [<i>filename</i>]</p> <p>Example:</p> <pre>Router(config)# boot system flash</pre>	Specifies the filename of a boot image stored in flash memory.
Step 9	<p>config-register <i>value</i></p>	Modifies the existing configuration register setting to reflect the way in which you want to load a system image.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config)# config-register 0x2102</pre>	
Step 10	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 11	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Router# copy running-config startup-config</pre>	Saves the configuration changes to your startup configuration in NVRAM so that the router will boot with the configuration you have entered.
Step 12	<p>hw-module standby-cpu reset</p> <p>Example:</p> <pre>Router# hw-module standby-cpu reset</pre>	Resets and reloads the standby processor with the specified Cisco software image, and executes the image.
Step 13	<p>reload standby-cpu</p> <p>Example:</p> <pre>Router# reload standby-cpu</pre>	(Optional) For Cisco 12000 series Internet routers only. Resets and reloads the standby processor with the specified Cisco software image, and executes the image.
Step 14	<p>redundancy force-switchover [main-cpu]</p> <p>Example:</p> <pre>Router# redundancy force-switchover</pre>	<p>Forces a switchover to the standby RP.</p> <ul style="list-style-type: none"> For Cisco 10000 series Internet routers: The main-cpu keyword is required.

Troubleshooting Stateful Switchover

- The standby RP was reset, but there are no messages describing what happened--To display a log of SSO events and clues as to why a switchover or other event occurred, enter the **show redundancy history** command on the newly active RP.
- The show redundancy states command shows an operating mode that is different than what is configured on the networking device--On certain platforms the output of the **show redundancy states** command displays the actual operating redundancy mode running on the device, and not the configured mode as set by the platform. The operating mode of the system can change depending on system events. For example, SSO requires that both RPs on the networking device be running the same software image; if the images are different, the device will not operate in SSO mode, regardless of its configuration.
- Reloading the device disrupts SSO operation--The SSO feature introduces a number of commands, including commands to manually cause a switchover. The reload command is not an SSO command. This command causes a full reload of the box, removing all table entries, resetting all line cards, and

thereby interrupting network traffic forwarding. To avoid reloading the box unintentionally, use the **redundancy force-switchover** command.

- During a software upgrade, the networking device appears to be in a mode other than SSO--During the software upgrade process, the show redundancy command indicates that the device is running in a mode other than SSO.
This is normal behavior. Until the FSU procedure is complete, each RP will be running a different software version. While the RPs are running different software versions, the mode will change to either RPR or RPR+, depending on the device. The device will change to SSO mode once the upgrade has completed.
- On the Cisco 7500 series router, the previously active processor is being reset and reloaded before the core dump completes--Use the **crashdump-timeout** command to set the maximum time that the newly active processor waits before resetting and reloading the previously active processor.
- You can enter ROM monitor mode by restarting the router and then pressing the Break key or issuing a **send break** command from a telnet session during the first 60 seconds of startup.The send break function can be useful for experienced users or for users under the direction of a Cisco Technical Assistance Center (TAC) representative to recover from certain system problems or to evaluate the cause of system problems.
- On the Cisco 7500 series router, issuing a **send break** does not cause a system switchover--This is normal operation on the Cisco 7500 series router. Using **send break** to break or pause the system is not recommended and may cause unpredictable results. To initiate a manual switchover, use the **redundancy force-switchover** command.
- You can enter ROM monitor mode by restarting the router and then pressing the Break key or issuing a **send break** command from a telnet session during the first 60 seconds of startup.The send break function can be useful for experienced users or for users under the direction of a Cisco Technical Assistance Center (TAC) representative to recover from certain system problems or to evaluate the cause of system problems.
- On Cisco 10000 and 12000 series Internet routers, if a standby RP is present, the system will detect the break and complete a switchover; however, this is not the recommended procedure for initiating a switchover. To initiate a manual switchover, use the **redundancy force-switchover** command.
- [Troubleshooting SSO, page 34](#)

Troubleshooting SSO

SUMMARY STEPS

1. **enable**
2. **crashdump-timeout** [*mm* | *hh* : *mm*]
3. **debug atm ha-error**
4. **debug atm ha-events**
5. **debug atm ha-state**
6. **debug frame-relay redundancy**
7. **debug ppp redundancy** [**detailed** | **event**]
8. **debug redundancy** { **all** | **ui** | **clk** | **hub** }
9. **show diag** [*slot-number* | **chassis** | **subslot** *slot / subslot*] [**details** | **summary**]
10. **show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **switchover history** | **states** | **inter-device**]
11. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>crashdump-timeout [<i>mm</i> <i>hh</i> : <i>mm</i>]</p> <p>Example: router(config-red)# crashdump-timeout</p>	<p>Set the longest time that the newly active RP will wait before reloading the formerly active RP.</p>
Step 3	<p>debug atm ha-error</p> <p>Example: Router# debug atm ha-error</p>	<p>Debugs ATM HA errors on the networking device.</p>
Step 4	<p>debug atm ha-events</p> <p>Example: Router# debug atm ha-events</p>	<p>Debugs ATM HA events on the networking device.</p>
Step 5	<p>debug atm ha-state</p> <p>Example: Router# debug atm ha-state</p>	<p>Debugs ATM high-availability state information on the networking device.</p>
Step 6	<p>debug frame-relay redundancy</p> <p>Example: Router# debug frame-relay redundancy</p>	<p>Debugs Frame Relay redundancy on the networking device.</p>
Step 7	<p>debug ppp redundancy [<i>detailed</i> <i>event</i>]</p> <p>Example: Router# debug ppp redundancy</p>	<p>Debugs PPP redundancy on the networking device.</p>
Step 8	<p>debug redundancy { <i>all</i> <i>ui</i> <i>clk</i> <i>hub</i> }</p> <p>Example: Router# debug redundancy all</p>	<p>Debugs redundancy on the networking device.</p>
Step 9	<p>show diag [<i>slot-number</i> <i>chassis</i> <i>subslot slot / subslot</i>] [details summary]</p>	<p>Displays hardware information for the router.</p>

	Command or Action	Purpose
	Example: Router# show diag	
Step 10	show redundancy [clients counters debug-log handover history switchover history states inter-device] Example: Router# show redundancy	Displays the redundancy configuration mode of the RP. Also displays information about the number of switchovers, system uptime, processor uptime, and redundancy state, and reasons for any switchovers.
Step 11	show version Example: Router# show version	Displays image information for each RP.

Configuration Examples for Stateful Switchover

- [Example Verifying that SSO Is Configured on Various Platforms, page 36](#)
- [Example Verifying that SSO Is Operating on the Device, page 38](#)
- [Example Verifying SSO Protocols and Applications, page 40](#)

Example Verifying that SSO Is Configured on Various Platforms

In the following several examples, the **show redundancy** command is used to verify that SSO is configured on the device. Sample output is provided for several platforms.

Cisco 7304 Router

```
Router# show redundancy

Redundant System Information :
Available system uptime = 2 minutes
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = none
Hardware Mode = Duplex
Configured Redundancy Mode = SSO
Operating Redundancy Mode = SSO
Maintenance Mode = Disabled
Communications = Up
Current Processor Information :
Active Location = slot 0
Current Software state = ACTIVE
Uptime in current state = 2 minutes
Image Version = Cisco Internetwork Operating System Software
IOS (tm) 7300 Software (C7300-P-M), Version 12.2(20)S6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

In the following several examples, the **show redundancy** command is used to verify that SSO is configured on the device. Sample output is provided for several platforms.

Cisco 7304 Router

```

Router# show redundancy

Redundant System Information :
Available system uptime = 2 minutes
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = none
Hardware Mode = Duplex
Configured Redundancy Mode = SSO
Operating Redundancy Mode = SSO
Maintenance Mode = Disabled
Communications = Up
Current Processor Information :
Active Location = slot 0
Current Software state = ACTIVE
Uptime in current state = 2 minutes
Image Version = Cisco Internetwork Operating System Software
IOS (tm) 7300 Software (C7300-P-M), Version 12.2(20)S6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 29-Oct-04 14:39
BOOT =
CONFIG_FILE =
BOOTLDR = bootdisk:c7300-boot-mz.121-13.EX1
Configuration register = 0x0
Peer Processor Information :
Standby Location = slot 2
Current Software state = STANDBY HOT
Uptime in current state = 1 minute
Image Version = Cisco Internetwork Operating System Software
IOS (tm) 7300 Software (C7300-P-M), Version 12.2(20)S6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 29-Oct-04 14:39
BOOT =
CONFIG_FILE =
BOOTLDR = bootdisk:c7300-boot-mz.121-13.EX1
Configuration register = 0x0

```

Cisco 7500 Series Router

```

Router# show redundancy
Operating mode is sso
redundancy mode sso
hw-module slot 6 image disk0:rsp-pv-mz
hw-module slot 7 image disk0:rsp-pv-mz
Active in slot 6
Standby in slot 7
The system total uptime since last reboot is 2 weeks, 23 hours 41 minutes.
The system has experienced 4 switchovers.
The system has been active (become master) for 21 hours 1 minute.
Reason for last switchover: User forced.

```

Cisco 10000 Series Internet Router

```

Router# show redundancy
PRE A (This PRE)   : Active
PRE B              : Standby
Operating mode     : SSO
Uptime since this PRE switched to active : 13 hours, 51 minutes
Total system uptime from reload         : 15 hours, 8 minutes
Switchovers this system has experienced : 2
Standby failures since this PRE active  : 0
The standby PRE has been up for         : 13 hours, 47 minutes
Standby PRE information...
Standby is up.
Standby has 524288K bytes of memory.

```

```

Standby BOOT variable = disk0:c10k-p10-mz
Standby CONFIG_FILE variable =
Standby BOOTLDR variable =
Standby Configuration register is 0x2102
Standby version:
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (C10K-P10-M), Version 12.0(20020221:082811)
 [REL-bowmore.ios-weekly 100]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 21-Feb-02 03:28
Active version:
Cisco Internetwork Operating System Software
IOS (am) 10000 Software (C10K-P10-M), Version 12.0(20020221:082811)
 [REL-bowmore.ios-weekly 100]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 21-Feb-02 03:28

```

Cisco 12000 Series Internet Router

```

Router# show redundancy
Active GRP in slot 4:
Standby GRP in slot 5:
Preferred GRP: none
Operating Redundancy Mode: SSO
Auto synch: startup-config running-config
switchover timer 3 seconds [default]

```

Cisco ASR 1000 Series Router

```

Router# show redundancy states
my state = 13 -ACTIVE
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit ID = 48
Redundancy Mode (Operational) = rpr
Redundancy Mode (Configured) = rpr
Redundancy State = rpr
Maintenance Mode = Disabled
Manual Swact = enabled
Communications = Up
client count = 66
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0

```

Example Verifying that SSO Is Operating on the Device

In the following several examples, the **show redundancy** command with the **states** keyword is used to verify that SSO is configured on the device. Sample output is provided for several platforms.

Cisco 7304 Router

```

Router# show redundancy states
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit ID = 0
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured) = SSO
Split Mode = Disabled
Manual Swact = Enabled
Communications = Up
client count = 18
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0

```

Cisco 7500 Series Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit ID = 7
Redundancy Mode = sso
Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up
client count = 12
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

Cisco 10000 Series Internet Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit = Preferred Primary
Unit ID = 0
Redundancy Mode = SSO
Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up
client count =14
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

Cisco 12000 Series Internet Router

```
Router# show redundancy states

my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit ID = 4
Redundancy Mode = SSO
Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up
client count = 14
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x
```

Cisco ASR 1000 Series Router

```
Router# show redundancy states
    my state = 13 -ACTIVE
    peer state = 4  -STANDBY COLD
        Mode = Duplex
        Unit ID = 48
    Redundancy Mode (Operational) = rpr
    Redundancy Mode (Configured) = rpr
    Redundancy State              = rpr
        Maintenance Mode = Disabled
    Manual Swact = enabled
    Communications = Up
        client count = 66
    client_notification_TMR = 30000 milliseconds
        RF debug mask = 0x0
```

Example Verifying SSO Protocols and Applications

Enter the **show redundancy** command with the **client** keyword to display the list of applications and protocols that have registered as SSO protocols or applications. You can also verify the list of supported line protocols.

Cisco 7304 Router

```
Router# show redundancy clients

clientID = 0 clientSeq = 0 RF_INTERNAL_MSG
clientID = 29 clientSeq = 60 Redundancy Mode RF
clientID = 25 clientSeq = 130 CHKPT RF
clientID = 1314 clientSeq = 137 7300 Platform RF
clientID = 22 clientSeq = 140 Network RF Client
clientID = 24 clientSeq = 150 CEF RRP RF Client
clientID = 5 clientSeq = 170 RFS client
clientID = 23 clientSeq = 220 Frame Relay
clientID = 49 clientSeq = 225 HDLC
clientID = 20 clientSeq = 310 IPROUTING NSF RF cli
clientID = 21 clientSeq = 320 PPP RF
clientID = 34 clientSeq = 350 SNMP RF Client
clientID = 52 clientSeq = 355 ATM
clientID = 35 clientSeq = 360 History RF Client
clientID = 54 clientSeq = 530 SNMP HA RF Client
clientID = 75 clientSeq = 534 VRF common
clientID = 57 clientSeq = 540 ARP
clientID = 65000 clientSeq = 65000 RF_LAST_CLIENT
```

Cisco 7500 Series Router

```
Router# show redundancy clients

clientID = 0 clientSeq = 0 RF_INTERNAL_MSG
clientID = 25 clientSeq = 130 CHKPT RF
clientID = 22 clientSeq = 140 Network RF Client
clientID = 24 clientSeq = 150 CEF RRP RF Client
clientID = 37 clientSeq = 151 MDFS RRP RF Client
clientID = 23 clientSeq = 220 FRAME RELAY
clientID = 49 clientSeq = 225 HDLC
clientID = 20 clientSeq = 310 IPROUTING NSF RF cli
clientID = 21 clientSeq = 320 PPP RF
clientID = 34 clientSeq = 330 SNMP RF Client
clientID = 29 clientSeq = 340 ATM
clientID = 35 clientSeq = 350 History RF Client
clientID = 50 clientSeq = 530 SNMP HA RF Client
clientID = 65000 clientSeq = 65000 RF_LAST_CLIENT
```

Cisco 10000 Series Internet Routers

```
Router# show redundancy clients

clientID = 0 clientSeq = 0 RF_INTERNAL_MSG
clientID = 25 clientSeq = 130 CHKPT RF
clientID = 22 clientSeq = 140 Network RF Client
clientID = 24 clientSeq = 150 CEF RRP RF Client
clientID = 26 clientSeq = 160 C10K RF Client
clientID = 5 clientSeq = 170 RFS client
clientID = 23 clientSeq = 220 Frame Relay
clientID = 49 clientSeq = 225 HDLC
clientID = 20 clientSeq = 310 IPROUTING NSF RF cli
clientID = 21 clientSeq = 320 PPP RF
clientID = 34 clientSeq = 330 SNMP RF Client
clientID = 29 clientSeq = 340 ATM
clientID = 35 clientSeq = 350 History RF Client
clientID = 65000 clientSeq = 65000 RF_LAST_CLIENT
```


Cisco 12000 Series Internet Router

```

Router# show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 25     clientSeq = 130    CHKPT RF
clientID = 27     clientSeq = 132    C12K RF COMMON Client
clientID = 30     clientSeq = 135    Redundancy Mode RF
clientID = 22     clientSeq = 140    Network RF Client
clientID = 24     clientSeq = 150    CEF RRP RF Client
clientID = 37     clientSeq = 151    MDFS RRP RF Client
clientID = 5      clientSeq = 170    RFS client
clientID = 23     clientSeq = 220    Frame Relay
clientID = 49     clientSeq = 225    HDLC
clientID = 20     clientSeq = 310    IPROUTING NSF RF cli
clientID = 21     clientSeq = 320    PPP RF
clientID = 34     clientSeq = 330    SNMP RF Client
clientID = 29     clientSeq = 340    ATM
clientID = 35     clientSeq = 350    History RF Client
clientID = 50     clientSeq = 530    SNMP HA RF Client
clientID = 65000 clientSeq = 65000 RF_LAST_CLIENT

```

Cisco ASR 1000 Series Router

```

Router# show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 29     clientSeq = 60     Redundancy Mode RF
clientID = 139    clientSeq = 62     IfIndex
clientID = 25     clientSeq = 69     CHKPT RF
clientID = 1340   clientSeq = 90     ASR1000-RP Platform
clientID = 1501   clientSeq = 91     Cat6k CWAN HA
clientID = 78     clientSeq = 95     TSPTUN HA
clientID = 305    clientSeq = 96     Multicast ISSU Conso
clientID = 304    clientSeq = 97     IP multicast RF Clie
clientID = 22     clientSeq = 98     Network RF Client
clientID = 88     clientSeq = 99     HSRP
clientID = 114    clientSeq = 100    GLBP
clientID = 1341   clientSeq = 102    ASR1000 DPIDX
clientID = 1505   clientSeq = 103    Cat6k SPA TSM
clientID = 1344   clientSeq = 110    ASR1000-RP SBC RF
clientID = 227    clientSeq = 111    SBC RF
clientID = 71     clientSeq = 112    XDR RRP RF Client
clientID = 24     clientSeq = 113    CEF RRP RF Client
clientID = 146    clientSeq = 114    BFD RF Client
clientID = 306    clientSeq = 120    MFIB RRP RF Client
clientID = 1504   clientSeq = 128    Cat6k CWAN Interface
clientID = 75     clientSeq = 130    Tableid HA
clientID = 401    clientSeq = 131    NAT HA
clientID = 402    clientSeq = 132    TPM RF client
clientID = 5      clientSeq = 135    Config Sync RF clien
clientID = 68     clientSeq = 149    Virtual Template RF
clientID = 23     clientSeq = 152    Frame Relay
clientID = 49     clientSeq = 153    HDLC
clientID = 72     clientSeq = 154    LSD HA Proc
clientID = 113    clientSeq = 155    MFI STATIC HA Proc
clientID = 20     clientSeq = 171    IPROUTING NSF RF cli
clientID = 100    clientSeq = 173    DHCP
clientID = 101    clientSeq = 174    DHCPD
clientID = 74     clientSeq = 183    MPLS VPN HA Client
clientID = 34     clientSeq = 185    SNMP RF Client
clientID = 52     clientSeq = 186    ATM
clientID = 69     clientSeq = 189    AAA
clientID = 118    clientSeq = 190    L2TP
clientID = 82     clientSeq = 191    CCM RF
clientID = 35     clientSeq = 192    History RF Client
clientID = 90     clientSeq = 204    RSVP HA Services
clientID = 70     clientSeq = 215    FH COMMON RF CLIENT
clientID = 54     clientSeq = 220    SNMP HA RF Client
clientID = 73     clientSeq = 221    LDP HA
clientID = 76     clientSeq = 222    IPRM
clientID = 57     clientSeq = 223    ARP
clientID = 50     clientSeq = 230    FH_RF_Event_Detector

```

clientID = 1342	clientSeq = 240	ASR1000 SpaFlow
clientID = 1343	clientSeq = 241	ASR1000 IF Flow
clientID = 83	clientSeq = 255	AC RF Client
clientID = 84	clientSeq = 257	AToM manager
clientID = 85	clientSeq = 258	SSM
clientID = 102	clientSeq = 273	MQC QoS
clientID = 94	clientSeq = 280	Config Verify RF cli
clientID = 135	clientSeq = 289	IKE RF Client
clientID = 136	clientSeq = 290	IPSEC RF Client
clientID = 130	clientSeq = 291	CRYPTO RSA
clientID = 148	clientSeq = 296	DHCPv6 Relay
clientID = 4000	clientSeq = 303	RF_TS_CLIENT
clientID = 4005	clientSeq = 305	ISSU Test Client
clientID = 93	clientSeq = 309	Network RF 2 Client
clientID = 205	clientSeq = 311	FEC Client
clientID = 141	clientSeq = 319	DATA DESCRIPTOR RF C
clientID = 4006	clientSeq = 322	Network Clock
clientID = 225	clientSeq = 326	VRRP
clientID = 65000	clientSeq = 336	RF_LAST_CLIENT

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco High Availability commands	<i>Cisco IOS High Availability Command Reference</i>
DHCP proxy client	ISSU and SSO--DHCP High Availability Features module in the <i>Cisco IOS IP Addressing Services Configuration Guide</i>
MPLS high availability	MPLS High Availability: Overview module in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>
NSF/SSO - 802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the <i>Cisco IOS Carrier Ethernet Configuration Guide</i>
NSF/SSO - Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>
NSF/SSO - E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the <i>Cisco IOS Carrier Ethernet Configuration Guide</i>
SSO - BFD (Admin Down)	Bidirectional Forwarding Detection module in the <i>Cisco IOS IP Routing: BFD Configuration Guide</i>
SSO GLBP	GLBP SSO module in the <i>Cisco IOS IP Application Services Configuration Guide</i>

Related Topic	Document Title
SSO HSRP	Configuring HSRP module in the <i>Cisco IOS IP Application Services Configuration Guide</i>
<ul style="list-style-type: none"> MFIB: IPv4 SSO/ISSU NSF/SSO - IPv4 Multicast SSO - IPv4 MFIB 	Monitoring and Maintaining Multicast HA Operations (NSF/SSO and ISSU) module in the <i>Cisco IOS IP Multicast Configuration Guide</i>
SSO and RPR on the Cisco ASR 1000 series routers	<i>Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</i>
SSO VRRP	Configuring VRRP module in the <i>Cisco IOS IP Application Services Configuration Guide</i>
Basic IPv6 configuration	Implementing IPv6 Addressing and Basic Connectivity module in the <i>Cisco IOS IPv6 Configuration Guide</i>
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Stateful Switchover

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Table 11: Feature Information for Cisco Stateful Switchover

Feature Name	Releases	Feature Information
Stateful Switchover (SSO)	12.0(22)S 12.0(23)S 12.0(24)S 12.2(20)S 12.2(18)S 12.2(33)SRA	<p>This feature was introduced:</p> <p>In 12.0(23)S, support was added for 1xGE and 3xGE line cards on the</p> <p>In 12.0(24)S, support was added for the following line cards on the</p> <ul style="list-style-type: none"> • Engine 1 <ul style="list-style-type: none"> ◦ 2-port OC-12/STM-4c DPT • Engine 2 <ul style="list-style-type: none"> ◦ 1-port OC-48/STM-16c DPT ◦ 8-port OC-3/STM-1c ATM • IP Service Engine (ISE) <ul style="list-style-type: none"> ◦ 4-port OC-3c/STM-1c POS/SDH ISE

Feature Name	Releases	Feature Information
		<ul style="list-style-type: none"> ◦ 8-port OC-3c/STM-1c POS/SDH ISE ◦ 16-port OC-3c/STM-1c POS/SDH ISE ◦ 4-port OC-12c/STM-4c POS/SDH ISE ◦ 1-port OC-48c/STM-16c POS/SDH ISE ◦ 4-port channelized OC-12/STM-4 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE ◦ 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE <p>In 12.0(26)S, support was added for the following line cards on the</p> <ul style="list-style-type: none"> • 4-port OC-12c/STM-4c DPT ISE <p>In 12.2(20)S, support was added for the Cisco 7304 router.</p>
CEM SSO/ISSU	12.2(33)SRC	This feature was introduced.
Dynamic Host Configuration Protocol (DHCP) On Demand Address Pool (ODAP) client/server	12.2(31)SB2	This feature was updated to be SSO-compliant.
MFIB: IPv4 SSO/ISSU	12.2(33)SRE	This feature was introduced.
NSF/SSO - IPv4 Multicast	12.2(33)SRE	This feature was introduced.
NSF/SSO - IPv6 Multicast	12.2(33)SRE	This feature was introduced.
NSF/SSO--Virtual Private LAN Services	12.2(33)SXI4 15.0(1)S	This feature was introduced.
Route Processor Redundancy Plus (RPR+)	12.2(20)S	This feature was introduced on the Cisco 7304 router.
SSO- Automatic Protection Switching (APS)	12.2(28)SB	This feature was introduced.
SSO - BFD (Admin Down)	12.2(33)SB	This feature was introduced.

Feature Name	Releases	Feature Information
SSO - DHCP proxy client	12.2(31)SB2 12.2(33)SRC	This feature was updated to be SSO-compliant. In 12.2(33)SRC, this feature was introduced.
SSO - DHCP relay on unnumbered interface	12.2(31)SB2	This feature was updated to be SSO-compliant.
SSO - DHCP server	12.2(31)SB2	This feature was updated to be SSO-compliant.
SSO - Gateway Load Balancing Protocol (GLBP)	12.2(31)SB2 12.2(33)SXH	This feature was updated to be SSO-compliant.
SSO - HDLC	12.2(28)SB 15.0(1)S	This feature was introduced.
SSO - HSRP	12.2(33)SXH 15.0(1)S Cisco IOS XE 3.1.0SG	This feature was introduced.
SSO - IPv4 MFIB	12.2(33)SRE	This feature was introduced.
SSO - MLPPP	12.2(28)SB	This feature was introduced.
SSO - Multilink Frame Relay	12.2(25)S 12.2(31)SB2 12.2(33)SRB 15.0(1)S	This feature was introduced. In 12.2(28)S, support was added for the Cisco 12000 series Internet router. In 12.2(31)SB2, support was added for the Cisco 10000 series Internet router. In 12.2(33)SRB, this feature was updated to be SSO compliant.
SSO - Multilink PPP (MLP)	15.0(1)S	This feature is supported.
SSO - PPP	12.2(33)SRB 15.0(1)S	This feature was updated to be SSO-compliant.
SSO - PPPoA	12.2(31)SB2	This feature was updated to be SSO-compliant.
SSO - PPPoE	12.2(31)SB2	This feature was updated to be SSO-compliant.
SSO - PPPoE IPv6	12.2(33)SXE	This feature was introduced.
SSO - Quality of Service (QoS)	12.2(25)S 15.0(1)S	This feature was introduced.
SSO - VRRP	12.2(33)SRC 15.0(1)S	This feature was introduced.
Virtual template manager SSO	12.2(33)SRC	This feature was introduced.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.