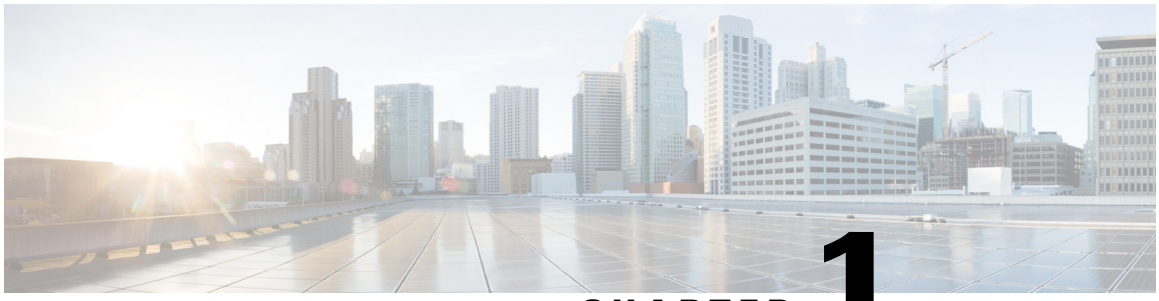
High Availability Configuration Guide, Cisco IOS Release 15S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring Stateful Switchover

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

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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

Prerequisites for Stateful Switchover

General Prerequisites

-
- 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).
```

-
- 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

- Configuration changes made through SNMP may not be automatically configured on the standby RP after a switchover occurs.
- 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.
```

```
%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: 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.

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 Aggregation Services Routers Restrictions

- Only RPR and SSO are supported on Cisco ASR 1000 Aggregation Services routers.

- RPR and SSO can be used on Cisco ASR 1000 Aggregation Services routers 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 Aggregation Services 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.
- Enabling software redundancy on the Cisco ASR 1001, 1002, and 1004 routers can reduce the Cisco IOS memory by more than half and adversely affect control plane scalability. We recommend that you use hardware redundant platforms, such as the Cisco ASR 1006 or 1013 routers, in networks where both scalability and high availability are critical.

Information About Stateful Switchover

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.

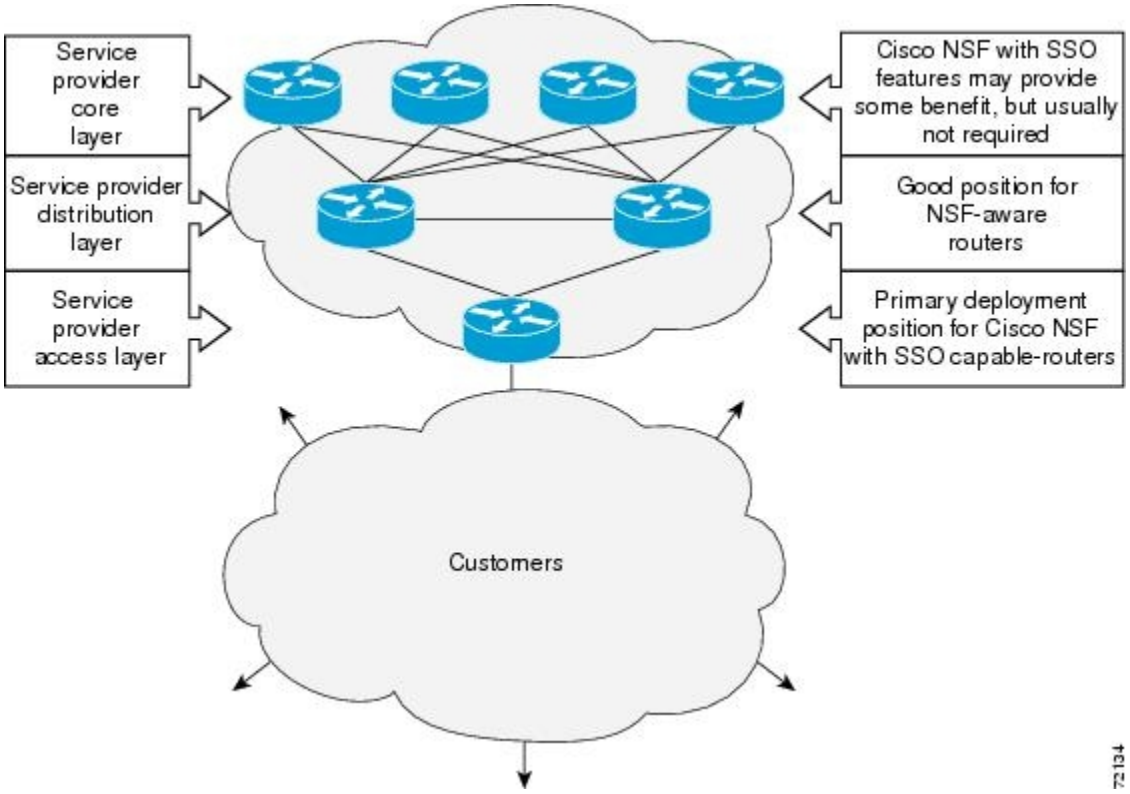
In Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between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

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

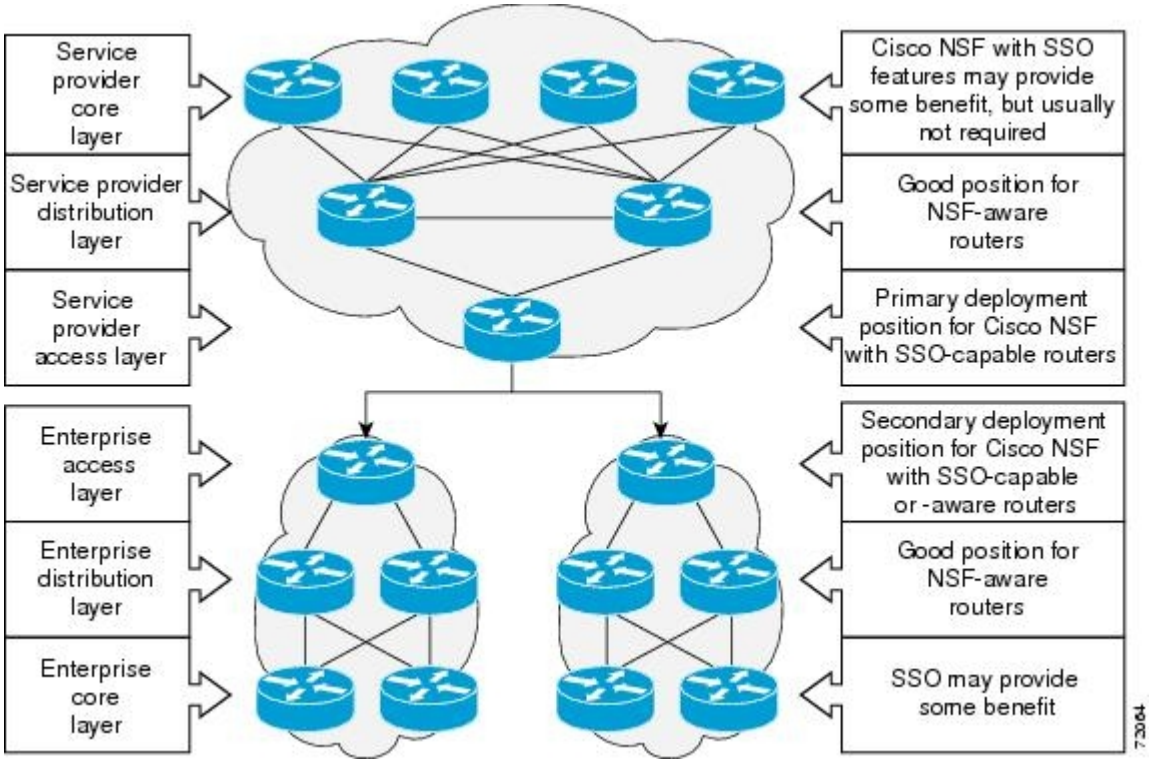


For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF and SSO features at the core layer 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

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

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

Redundancy Mode Support in Cisco IOS Releases


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

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

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 coredump, 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

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

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

Protocol	Platform	12.2 (28)SB	12.2(31)SB2
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.

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.

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

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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy tftp** {**slot**	**disk**}*device-number* **:** *filename* **Example:** `Router# copy tftp slot0:image1`	Copies a Cisco software image onto the flash device of the active RP.
Step 3	**copy tftp** {**slave**	**stby-**}{**slot**	**disk**}*device-number* **:** *filename* **Example:** `Router# copy tftp stby-slot0:image1`	Copies a Cisco software image onto the flash device of the standby RP.
Step 4	**exit** **Example:** `Router# exit`	Exits to user EXEC mode.

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*] | **ftp***filename* [*ip-address*]}
5. **boot system** {**flash** [*flash-fs***:**][*partition-number***:**][*filename*] | **tftp***filename* [*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. • 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** [*flash-fs***:**][*partition-number***:**][*filename*] | **ftp***filename* [*ip-address*]}	(Optional) Clears any existing system flash or TFTP boot image specification.

	Command or Action	Purpose
	Example: `Router(config)# no boot system flash`	
Step 5	**boot system** {**flash** [*flash-fs***:**][*partition-number***:**][*filename*] | **tftp***filename* [*ip-address*]} **Example:** **Example:** `Router(config)# boot system flash`	Specifies the filename of stored image in flash memory or, for Cisco 10000, on a TFTP server.
Step 6	**config-register** *value* **Example:** `Router(config)# config-register 0x2102`	Modifies the existing configuration register setting to reflect the way in which you want to load a system image.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 8	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the configuration changes to the startup configuration file.
Step 9	**reload** **Example:** `Router# reload`	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.

Before You Begin

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hw-module slot** *slot-number* **image** *file-spec* **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. • 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. **Note** After configuring SSO mode, the standby RP will automatically reset.

	Command or Action	Purpose
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. • 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. • Enter your password if prompted.
Step 2	**show redundancy** [**clients** | **counters** | **history** | **switchover history** | **states**] **Example:** `Router# show redundancy`	Displays SSO configuration information.
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. • Enter your password if prompted.
Step 2	**copy tftp** {**slot** | **disk**}*device-number*:*filename* **Example:** `Router# copy tftp slot0:image1`	Copies a Cisco software image onto the flash device of the active RP.
Step 3	**copy tftp** {**slave** | **stby-**}{**slot** | **disk }** *device-number* **:** *filename* **Example:** `Router# copy tftp stby-slot0:image1` **Example:**	Copies a Cisco software image onto the flash device of the standby RP.
Step 4	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 5	**no hw-module slot** *slot-number* **image** *file-spec* **Example:** `Router(config)# no hw-module slot 6 image slot0:rsp-pv-mz`	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. • Repeat this step for both the active and standby RSPs.
Step 6	**hw-module slot** *slot-number* **image** *file-spec* **Example:** `Router(config)# hw-module slot 6 image slot0:image1`	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. • Repeat this step for both the active and standby RSPs.
Step 7	**no boot system flash** [*flash-fs***:**][*partition-number***:**][*filename*] **Example:** `Router(config)# no boot system flash`	Clears the current boot image filename from the configuration file.
Step 8	**boot system flash** [*flash-fs***:**][*partition-number***:**][*filename*] **Example:** `Router(config)#` **boot system flash**	Specifies the filename of a boot image stored in flash memory.
Step 9	**config-register** *value* **Example:** `Router(config)# config-register 0x2102`	Modifies the existing configuration register setting to reflect the way in which you want to load a system image.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 11	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the configuration changes to your startup configuration in NVRAM so that the router will boot with the configuration you have entered.
Step 12	**hw-module standby-cpu reset** **Example:** `Router# hw-module standby-cpu reset`	Resets and reloads the standby processor with the specified Cisco software image, and executes the image.

	Command or Action	Purpose
Step 13	**reload standby-cpu** **Example:** `Router# reload standby-cpu`	(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	**redundancy force-switchover** [**main-cpu**] **Example:** `Router# redundancy force-switchover`	Forces a switchover to the standby RP. • 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.
- 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.

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 ppp redundancy** [**detailed** | **event**]
7. **debug redundancy** {**all** | **ui** | **clk** | **hub**}
8. **show diag** [*slot-number* | **chassis** | **subslot** *slot* / *subslot*] [**details** | **summary**]
9. **show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **switchover history** | **states** | **inter-device**]
10. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crashdump-timeout** [*mm* | *hh* **:** *mm*] **Example:** `router(config-red)# crashdump-timeout`	Set the longest time that the newly active RP will wait before reloading the formerly active RP.
Step 3	**debug atm ha-error** **Example:** `Router# debug atm ha-error`	Debugs ATM HA errors on the networking device.
Step 4	**debug atm ha-events** **Example:** `Router# debug atm ha-events`	Debugs ATM HA events on the networking device.
Step 5	**debug atm ha-state** **Example:** `Router# debug atm ha-state`	Debugs ATM high-availability state information on the networking device.

	Command or Action	Purpose
Step 6	**debug ppp redundancy** [**detailed** | **event**] **Example:** `Router# debug ppp redundancy`	Debugs PPP redundancy on the networking device.
Step 7	**debug redundancy** {**all** | **ui** | **clk** | **hub**} **Example:** `Router# debug redundancy all`	Debugs redundancy on the networking device.
Step 8	**show diag** [*slot-number* | **chassis** | **subslot** *slot / subslot*] [**details** | **summary**] **Example:** `Router# show diag`	Displays hardware information for the router.
Step 9	**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 10	**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

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 Routere

```
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      DHCPC
 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	*Cisco IOS High Availability Command Reference*
DHCP proxy client	ISSU and SSO--DHCP High Availability Features module in the *Cisco IOS IP Addressing Services Configuration Guide*

Related Topic	Document Title
MPLS high availability	MPLS High Availability: Overview module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO - 802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO - Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO - E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
SSO - BFD (Admin Down)	Bidirectional Forwarding Detection module in the *Cisco IOS IP Routing: BFD Configuration Guide*
SSO GLBP	GLBP SSO module in the *Cisco IOS IP Application Services Configuration Guide*
SSO HSRP	Configuring HSRP module in the *Cisco IOS IP Application Services Configuration Guide*
• MFIB: IPv4 SSO/ISSU • NSF/SSO - IPv4 Multicast • SSO - IPv4 MFIB	Monitoring and Maintaining Multicast HA Operations (NSF/SSO and ISSU) module in the *Cisco IOS IP Multicast Configuration Guide*
SSO and RPR on the Cisco ASR 1000 series routers	*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*
SSO VRRP	Configuring VRRP module in the *Cisco IOS IP Application Services Configuration Guide*
Basic IPv6 configuration	Implementing IPv6 Addressing and Basic Connectivity module in the *Cisco IOS IPv6 Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

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 . An account on Cisco.com is not required.

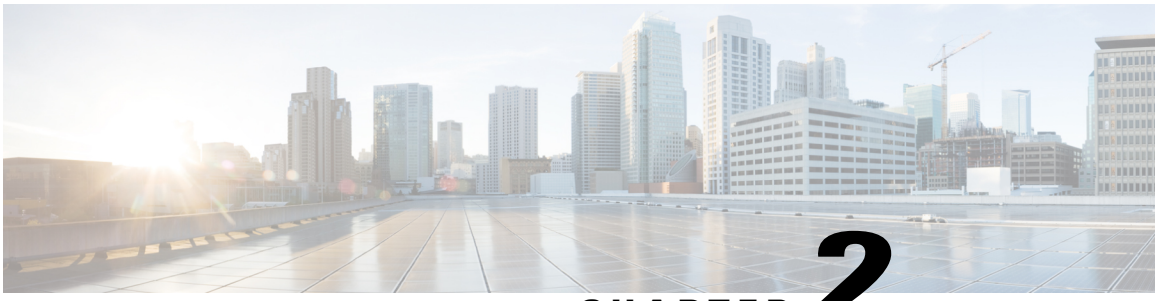
Table 11: Feature Information for Cisco Stateful Switchover

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	

Feature Name	Releases	Feature Information
		This feature was introduced: In 12.0(23)S, support was added for 1xGE and 3xGE line cards on the Cisco 12000 series Internet router. In 12.0(24)S, support was added for the following line cards on the Cisco 12000 series Internet router: • Engine 1 • 2-port OC-12/STM-4c DPT • Engine 2 • 1-port OC-48/STM-16c DPT • 8-port OC-3/STM-1c ATM • IP Service Engine (ISE) • 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

Feature Name	Releases	Feature Information
		In 12.0(26)S, support was added for the following line cards on the Cisco 12000 series Internet router: • 4-port OC-12c/STM-4c DPT ISE In 12.2(20)S, support was added for the Cisco 7304 router.
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.
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.

Feature Name	Releases	Feature Information
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.



CHAPTER 2

Configuring Nonstop Forwarding

This module describes how to configure Nonstop Forwarding (NSF) in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. NSF is supported by the BGP, EIGRP, IPv6, IS-IS, and OSPF protocols for routing and by CEF for forwarding.

The following terms are used throughout this document:

- NSF-aware device--A device that is running NSF-compatible software
- NSF-capable device--A device that is configured to support NSF. NSF-capable devices can rebuild routing information from either NSF-aware or NSF-capable neighboring devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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

Prerequisites for Nonstop Forwarding

- The networking device that is to be configured for NSF must first be configured for SSO. For information, see the Configuring Stateful Switchover section.
- For Border Gateway Protocol (BGP) NSF, all neighboring devices must be NSF-aware and must be configured for BGP graceful restart.
- For Enhanced Interior Gateway Routing Protocol (EIGRP) NSF:
  - All neighboring devices must be NSF-capable or NSF-aware.
  - An NSF-aware device must be completely converged with the network before it can assist an NSF-capable device in an NSF restart operation.
- For Internet Engineering Task Force (IETF) Intermediate System to Intermediate System (IS-IS), all neighboring devices must be NSF-aware.
- For Open Shortest Path First (OSPF) NSF, all networking devices on the same network segment must be NSF-aware.
- For IPv6 NSF, IPv6 must be enabled on your networking device.
- On platforms supporting the Route Switch Processor (RSP), and where the Cisco Express Forwarding (CEF) switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command.

Restrictions for Nonstop Forwarding

General Restrictions

NSF capability is not enabled by default for OSPF, ISIS, or BGP. NSF capability is enabled by default for EIGRP only.

BGP NSF Restrictions

- BGP support in NSF requires that neighbor networking devices be NSF-aware. If an NSF-capable device discovers that a particular BGP neighbor does not have graceful restart capability, it will not establish an NSF-capable session with that neighbor. All other neighbors that have graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device.
- All devices must be configured with the same type of NSF helper mode, either IETF graceful restart or Cisco NSF.

EIGRP NSF Restrictions

- An NSF-aware device cannot support two NSF-capable peers performing an NSF restart operation at the same time. However, both neighbors will reestablish peering sessions after the NSF restart operation is complete.
- Distributed platforms that run a supporting version of Cisco software can support full NSF capabilities. These devices can perform a restart operation and can support other NSF capable peers.
- Single processor platforms that run a supporting version of Cisco software support only NSF awareness. These devices maintain adjacency and hold known routes for the NSF-capable neighbor until it signals that it is ready for the NSF-aware device to send its topology table or the route-hold timer expires.

OSPF NSF Restrictions

- OSPF NSF for virtual links is not supported.
- OSPF NSF for sham links is not supported.
- OSPF NSF supports NSF/SSO for IPv4 traffic only.
- OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.
- All neighbor networking devices must be NSF-aware. If an NSF-capable device discovers that it has non-NSF-aware neighbors on a particular network segment, it will disable NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware devices will continue to provide NSF capabilities.
- You can configure strict link state advertisement (LSA) checking on both NSF-aware and NSF-capable devices; however, it is effective only when the device is in helper mode.

Cisco7200SeriesRouterRestrictions

- The Cisco 7200 series router has a single CPU and cannot support the stateful switchover in the event of a network processor engine (NPE) fault.
- The Cisco 7206 supports NSF and can operate in a peer role with a Cisco 7500, 10000, or 12000 series router running Cisco IOS Release 12.0(23)S or a later release. With NSF enabled, an RP switchover on the Cisco 7500, 10000, or 12000 series router peer should not cause a loss of PPP, ATM, high-level data link control (HDLC), or Frame Relay sessions, or a loss of any OSPF, BGP, or IS-IS adjacencies established between the Cisco 7200 and the peer.

Information About Nonstop Forwarding

Nonstop Forwarding

Note In the following content, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

NSF works with the SSO feature in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following an RP switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This 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. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

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 NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

The NSF feature provides the following benefits:

- Improved network availability—NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.
- Overall network stability—Network stability may be improved with the reduction in the number of route flaps that had been created when devices in the network failed and lost their routing tables.
- Neighboring devices do not detect link flapping—Because the interfaces remain up across a switchover, neighboring devices do not detect a link flap (that is, the link does not go down and come back up).
- Prevention of routing flaps—Because SSO continues forwarding network traffic in the event of a switchover, routing flaps are avoided.
- No loss of user sessions—User sessions established prior to the switchover are maintained.

NSF always runs together with SSO. SSO supported protocols and applications must be high-availability (HA)-aware. A feature or protocol is HA-aware if it maintains, either partially or completely, undisturbed operation during an RP switchover. For some HA-aware protocols and applications, state information is synchronized from the active to the standby processor.

Cisco NSF Routing and Forwarding

Cisco NSF is supported by the BGP, EIGRP, IPv6, IS-IS, and OSPF protocols for routing and by CEF for forwarding. Of the routing protocols, BGP, EIGRP, IPv6, IS-IS, and OSPF have been enhanced with

NSF-capability and awareness, which means that devices running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol can be configured to use state information that has been synchronized between the active and the standby RP to recover route information following a switchover instead of information received from peer devices.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

Routing Protocols and CEF Support in Cisco NSF

The table below lists the routing protocol and CEF support in Cisco NSF.

Table 12: Routing Protocol and CEF Support in Cisco NSF

Protocol	Platform	NSF Support in Cisco IOS Software Release					
12.0(22)S	12.0(23)S	12.0(24)S	12.2(18)S	12.2(28)SB	12.2(33)SRA		
BGP	Cisco 7200	Yes[2]	Yes	Yes	No[3]	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	Yes	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
OSPF	Cisco 7200	Yes	Yes	Yes	No	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	No	No
	Cisco 12000	Yes	Yes	Yes	No	No	No

Protocol	Platform	NSF Support in Cisco IOS Software Release					
IS-IS	Cisco 7200	Yes	Yes	Yes	No	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	Yes	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
CEF	Cisco 7200[4]	--	--	--	--	--	--
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	No	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
EIGRP	Cisco 7200	No	No	No	Yes	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	No	No	No	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	No	No	No	No	No	No
	Cisco 12000	No	No	No	No	No	No

2 The Cisco 7200 is a single-route processor system and cannot maintain its forwarding table in the event of a route processor failure. It cannot perform nonstop forwarding of packets. However, it supports the NSF protocol extensions for BGP, EIGRP, OSPF, and IS-IS. Therefore, it can peer with NSF-capable routers and facilitate the resynchronization of routing information with such routers.

3 The Cisco 7200 is NSF-aware in Cisco IOS Release 12.2(18)S.

4 The Cisco 7200 is a single-processor device and does not support SSO; therefore, CEF support for NSF does not apply.

Cisco Express Forwarding and NSF

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF 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 reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates to CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The routing protocols run only on the active RP, and they receive routing updates from their neighbor devices. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables. Alternately, the IS-IS protocol can be configured to synchronize state information from the active to the standby RP to help rebuild the routing table on the NSF-capable device in environments where neighbor devices are not NSF-aware.

For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information. The CEF NSF feature operates by default while the networking device is running in SSO mode. No configuration is necessary.

BGP NSF Operations

When a NSF-capable device begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the NSF-capable device has “graceful restart capability.” Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable device and its BGP peers need to exchange the graceful restart capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable device as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable device reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable device as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful-restart capability in an OPEN message but will establish a BGP session with the NSF-capable device. This function will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart-capable.

BGP support in NSF requires that neighbor networking devices be NSF-aware; that is, the devices must have the graceful restart capability and advertise that capability in their OPEN message during session establishment. If an NSF-capable device discovers that a particular BGP neighbor does not have graceful restart capability, it will not establish an NSF-capable session with that neighbor. All other neighbors that have graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device.

EIGRP NSF Operations

Cisco NSF is supported by the EIGRP protocol for routing and by CEF for forwarding. EIGRP depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. The NSF-capable device notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware device receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, the NSF-capable and NSF-aware devices immediately exchange their topology tables. The NSF-aware device sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware device then performs the following actions to assist the NSF-capable device:

- The EIGRP hello hold timer is expired to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware device to reply to the NSF-capable device more quickly reducing the amount of time required for the NSF-capable device to rediscover neighbors and rebuild the topology table.
- The route-hold timer is started. This timer is used to set the period of time that the NSF-aware device will hold known routes for the NSF-capable neighbor.
- The NSF-aware device notes in the peer list that the NSF-capable neighbor is restarting, maintains adjacency, and holds known routes for the NSF-capable neighbor until the neighbor signals that it is ready for the NSF-aware device to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware device, the NSF-aware device will discard held routes and treat the NSF-capable device as a new device joining the network and reestablishing adjacency accordingly.
- The NSF-aware device will continue to send queries to the NSF-capable device that is still converging after switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.

When the switchover operation is complete, the NSF-capable device notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting devices. The NSF-capable device then returns to normal operation. The NSF-aware device will look for alternate paths (go

active) for any routes that are not refreshed by the NSF-capable (restarting device). The NSF-aware device will then return to normal operation. If all paths are refreshed by the NSF-capable device, the NSF-aware device will immediately return to normal operation.

NSF-aware devices are completely compatible with non-NSF-aware or non-NSF-capable neighbors in an EIGRP network. A non-NSF-aware neighbor will ignore NSF capabilities and reset adjacencies and otherwise maintain the peering sessions normally.

IPv6 support for NSF Operations

Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family

The graceful restart capability is supported for IPv6 BGP unicast, multicast, and VPNv6 address families, enabling Cisco NSF functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state.

NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover. Forwarding is maintained by synchronizing the FIB between the active and standby RP. On switchover, forwarding is maintained using the FIB. The RIB is not kept synchronized; therefore, the RIB is empty on switchover. The RIB is repopulated by the routing protocols and subsequently informs the FIB about RIB convergence by using the NSF_RIB_CONVERGED registry call. The FIB tables are updated from the RIB, removing any stale entries. The RIB starts a fail-safe timer during RP switchover, in case the routing protocols fail to notify the RIB of convergence.

The Cisco BGP address family identifier (AFI) model is modular and scalable, and supports multiple AFIs and subsequent address family identifier (SAFI) configurations.

Nonstop Forwarding for IPv6 RIP

RIP registers as an IPv6 NSF client. Doing so has the benefit of using RIP routes installed in the Cisco Express Forwarding table until RIP has converged on the standby.

Nonstop Forwarding for Static Routes

Cisco NSF supports IPv6 static routes.

IS-IS NSF Operations

When an IS-IS NSF-capable device performs an RP switchover, it must perform two tasks in order to resynchronize its Link State Database with its IS-IS neighbors. First, it must relearn the available IS-IS neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the Link State Database for the network.

The IS-IS NSF feature offers two options when configuring NSF:

- IETF IS-IS
- Cisco IS-IS

If neighbor devices on a network segment are NSF-aware, meaning that neighbor devices are running a software version that supports the IETF Internet draft for device restartability, they will assist an IETF NSF device that is restarting. With IETF, neighbor devices provide adjacency and link-state information to help rebuild the routing information following a switchover. A benefit of IETF IS-IS configuration is operation between peer devices based on a proposed standard.

If you configure IETF on the networking device, but neighbor devices are not IETF-compatible, NSF will abort following a switchover.

If the neighbor devices on a network segment are not NSF-aware, you must use the Cisco configuration option. The Cisco IS-IS configuration transfers both protocol adjacency and link-state information from the active to the standby RP. A benefit of Cisco configuration is that it does not rely on NSF-aware neighbors.

IETF IS-IS Configuration

With the IETF IS-IS configuration, the NSF-capable device sends IS-IS NSF restart requests to neighboring NSF-aware devices as quickly as possible after an RP switchover. Neighbor networking devices recognize this restart request as a cue that the neighbor relationship with this device should not be reset, but that they should initiate database resynchronization with the restarting device. As the restarting device receives restart request responses from devices on the network, it can begin to rebuild its neighbor list.

Once this exchange is complete, the NSF-capable device uses the link-state information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. IS-IS is then fully converged.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. The IS-IS NSF operation waits for a specified interval to ensure that connections are stable before attempting another restart of IS-IS NSF. This functionality prevents IS-IS from attempting back-to-back NSF restarts with stale information.

Cisco IS-IS Configuration

With the Cisco configuration option, full adjacency and link-state packet (LSP) information is saved, or “checkpointed,” to the standby RP. Following a switchover, the newly active RP maintains its adjacencies using the checkpointed data, and can quickly rebuild its routing tables.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. Once this synchronization is completed, IS-IS adjacency and LSP data is checkpointed to the standby RP; however, a new NSF restart will not be attempted by IS-IS until the interval time expires. This functionality prevents IS-IS from attempting back-to-back NSF restarts. IS-IS NSF provides a command to extend the wait time for interfaces that, for whatever reason, do not come up in a timely fashion.

Following a switchover, Cisco IS-IS NSF has complete neighbor adjacency and LSP information; however, it must wait for all interfaces that had adjacencies prior to the switchover to come up. If an interface does not come up within the allocated interface wait time, the routes learned from these neighbor devices are not considered in routing table recalculation.

NSF-OSPF Operations

For Cisco Nonstop Forwarding (NSF), the Open Shortest Path First (OSPF) routing protocol has been enhanced to support high availability (HA) features in Stateful Switchover (SSO). Before an OSPF NSF-capable device can perform a Route Processor (RP) switchover, the device must be aware of the available OSPF neighbors on the network without resetting the neighbor relationship, and the device must acquire the contents of the link state database for the network. The NSF-capable device sends an OSPF NSF signal to neighboring NSF-aware devices to notify the devices that the neighbor relationship with the sending device must not be reset. The NSF-capable device uses the signals that it receives from other devices on the network to rebuild its neighbor list.

The NSF-capable device synchronizes its database with all the NSF-aware neighbors on its neighbor list. After all neighbors exchange routing information, the NSF-capable device uses the routing information to remove stale routes and update the routing information base (RIB) and the forwarding information base (FIB) with the new forwarding information. The OSPF protocols are then fully converged.

Prior to RFC 3623, Cisco implemented the proprietary Cisco NSF. The RFC 3623 Graceful OSPF Restart feature supports IETF NSF for OSPF processes in multivendor networks. The following are NSF device modes of operation common to Cisco and IETF NSF implementations:

- Restarting mode—In this mode, the OSPF device performs nonstop forwarding recovery because of an RP switchover.
- Helper mode—Also known as NSF-awareness mode. In this mode, the neighboring device is in the restarting state and helps in NSF recovery.

The strict link state advertisement (LSA) checking feature allows a helper device to terminate the graceful restart process if the device detects a changed LSA that would cause flooding during the graceful restart process. Strict LSA checking is disabled by default. You can enable strict LSA checking when there is a change to an LSA that would be flooded to the restarting device.

How to Configure Nonstop Forwarding

Configuring and Verifying BGP NSF

Repeat this procedure on each peer device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*]
5. **end**
6. **show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy**[**detail**]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 120`	Enables a BGP routing process, and enters router configuration mode.
Step 4	**bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] **Example:** `Router(config-router)# bgp graceful-restart`	Enables the BGP graceful restart capability, which starts NSF for BGP.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 6	**show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy**[**detail**]]] **Example:** `Router# show ip bgp neighbors`	Displays information about BGP and TCP connections to neighbors.

Configuring and Verifying EIGRP NSF

Repeat this procedure on each peer device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **nsf**
5. **timers nsf converge** *seconds*
6. **timers nsf signal** *seconds*
7. **timers nsf route-hold** *seconds*
8. **timers graceful-restart purge-time** *seconds*
9. **end**
10. **show ip protocols**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 109`	Enables an EIGRP routing process, and enters router configuration mode.
Step 4	**nsf** **Example:** `Router(config)# no nsf`	(Optional) Enables NSF capabilities. • This command is enabled by default.
Step 5	**timers nsf converge** *seconds* **Example:** `Router(config-router)# timers nsf converge 120`	(Optional) Adjusts the maximum time that the restarting device will wait for the EOT notification from an NSF-capable or NSF-aware peer. • Enter this command on NSF-capable devices only.
Step 6	**timers nsf signal** *seconds*	(Optional) Adjusts the maximum time for the initial restart period.

	Command or Action	Purpose
	Example: `Router(config-router)# timers nsf signal 20`	• Enter this command on NSF-capable devices only.
Step 7	**timers nsf route-hold** *seconds* **Example:** `Router(config-router)# timers nsf route-hold 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer. • This command is suported in releases before Cisco IOS 12.2(33)SRE.
Step 8	**timers graceful-restart purge-time** *seconds* **Example:** `Router(config-router)# timers graceful-restart purge-time 240`	(Optional) Sets the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer. • This command is supported in Cisco IOS Release 12.2(33)SRE and later releases.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 10	**show ip protocols** **Example:** `Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process.

Configuring NSF-OSPF

Perform only one of the following tasks:

Configuring Cisco NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf cisco** [**enforce global**]
5. **nsf cisco helper** [**disable**]
6. **nsf ietf helper** [**disable** | **strict-lsa-checking**]
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf cisco** [**enforce global**] **Example:** `Device(config-router)# nsf cisco`	Enables Cisco Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in NSF helper mode.
Step 5	**nsf cisco helper** [**disable**] **Example:** `Device(config-router)# nsf cisco helper`	Enables Cisco NSF helper support. • This command shows how to enable Cisco NSF helper mode.

	Command or Action	Purpose
Step 6	**nsf ietf helper** [**disable** | **strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper disable`	(Optional) Disables IETF NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Configuring IETF NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf ietf** [**restart-interval** *seconds*]
5. **nsf ietf helper** [**disable** | **strict-lsa-checking**]
6. **nsf cisco helper disable**
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf ietf** [**restart-interval** *seconds*] **Example:** `Device(config-router)# nsf ietf restart-interval 180`	Enables IETF Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in helper mode.
Step 5	**nsf ietf helper** [**disable** | **strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper strict-lsa-checking`	(Optional) Configures IETF NSF helper mode on neighbor devices that operate in helper mode.
Step 6	**nsf cisco helper disable** **Example:** `Device(config-router)# nsf cisco helper disable`	(Optional) Disables Cisco NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Configuring and Verifying IS-IS NSF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **nsf** [**cisco** | **ietf**]
5. **nsf interval** *minutes*
6. **nsf t3** {**manual** *seconds* | **adjacency**}
7. **nsf interface wait** *seconds*
8. **end**
9. **show isis nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis cisco1`	Enables the IS-IS routing protocol to specify an IS-IS process and enters router configuration mode.
Step 4	**nsf** [**cisco**	**ietf**] **Example:** `Router(config-router)# nsf ietf`	Enables IS-IS NSF operations.
Step 5	**nsf interval** *minutes* **Example:** `Router(config-router)# nsf interval 2`	(Optional) Configures the minimum time between NSF restart attempts.

	Command or Action	Purpose
Step 6	**nsf t3** {**manual** *seconds* | **adjacency**} **Example:** `Router(config-router)# nsf t3 manual 40`	(Optional) Specifies the methodology used to determine how long IETF NSF will wait for the link-state packet (LSP) database to synchronize before generating overloaded link-state information. • This command is supported for IETF NSF only.
Step 7	**nsf interface wait** *seconds* **Example:** `Router(config-router)# nsf interface wait 15`	(Optional) Specifies how long a Cisco NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart. • This command is supported for Cisco NSF only.
Step 8	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.
Step 9	**show isis nsf** **Example:** `Router# show isis nsf`	Displays current state information regarding IS-IS NSF.

Troubleshooting Nonstop Forwarding

SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug ip eigrp notifications**
4. **debug isis nsf** [**detail**]
5. **debug ospf nsf** [**detail**]
6. **show cef nsf**
7. **show cef state**
8. **show clns neighbors**
9. **show ip bgp**
10. **show ip bgp neighbor**
11. **show ip cef**
12. **show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**]
13. **show ip ospf**
14. **show ip ospf neighbor** [**detail**]
15. **show ip protocols**
16. **show isis database** [**detail**]
17. **show isis nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eigrp nsf** **Example:** `Device# debug eigrp nsf`	Displays notifications and information about NSF events for an EIGRP routing process.
Step 3	**debug ip eigrp notifications** **Example:** `Device# debug ip eigrp notifications`	Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.

	Command or Action	Purpose
Step 4	**debug isis nsf** [**detail**] **Example:** `Device# debug isis nsf [detail]`	Displays information about the IS-IS state during a Cisco NSF restart.
Step 5	**debug ospf nsf** [**detail**] **Example:** `Device# debug ospf nsf [detail]`	Displays debugging messages related to OSPF Cisco NSF commands.
Step 6	**show cef nsf** **Example:** `Device# show cef nsf`	Displays the current NSF state of CEF on both the active and standby RPs.
Step 7	**show cef state** **Example:** `Device# show cef state`	Displays the CEF state on a networking device.
Step 8	**show clns neighbors** **Example:** `Device# show clns neighbors`	Displays both end system and intermediate system neighbors.
Step 9	**show ip bgp** **Example:** `Device# show ip bgp`	Displays entries in the BGP routing table.
Step 10	**show ip bgp neighbor** **Example:** `Device# show ip bgp neighbor`	Displays information about the TCP and BGP connections to neighbor devices.
Step 11	**show ip cef** **Example:** `Device# show ip cef`	Displays entries in the FIB that are unresolved, or displays FIB summary.

	Command or Action	Purpose
Step 12	**show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**] **Example:** `Device# show ip eigrp neighbors detail`	Displays displayed information about neighbors discovered by EIGRP.
Step 13	**show ip ospf** **Example:** `Device# show ip ospf`	Displays general information about OSPF routing processes.
Step 14	**show ip ospf neighbor** [**detail**] **Example:** `Device# show ip ospf neighbor [detail]`	Displays OSPF-neighbor information on a per-interface basis.
Step 15	**show ip protocols** **Example:** `Device# show ip protocols`	Displays the parameters and current state of the active routing protocol process. • The status of EIGRP NSF configuration and support is displayed in the output.
Step 16	**show isis database** [**detail**] **Example:** `Device# show isis database [detail]`	Displays the IS-IS link-state database.
Step 17	**show isis nsf** **Example:** `Device# show isis nsf`	Displays the current state information regarding IS-IS NSF.

Configuration Examples for Nonstop Forwarding

Example NSF-Capable CEF

The CEF NSF feature operates by default while the networking device is running in SSO mode. No configuration is necessary. The following sample output shows that CEF is NSF capable:

```
Router# show cef state
CEF Status [RP]
```

```
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:      yes
Default CEF switching:     yes
Default dCEF switching:    yes
Update HWIDB counters:     no
Drop multicast packets:    no
CEF NSF capable:           yes
IPC delayed func on SSO:   no
RRP state:
I am standby RRP:          no
My logical slot:           0
RF PeerComm:               no
```

Example BGP NSF

The following partial output shows the BGP configuration on the SSO-enabled device:

```
Router# show running-config
router bgp 120
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
```

The following sample output shows that the graceful restart function is both advertised and received and that the address families have the graceful restart capability. If no address families were listed, then BGP NSF will not occur.

```
Router# show ip bgp neighbors
 192.168.2.2
BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
Address family IPv4 Unicast:advertised and received
    Address family IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

Example: EIGRP NSF

The following sample output shows that EIGRP NSF support is present in the installed software image.

- “EIGRP NSF-aware route hold timer is . . .” is displayed in the output for either NSF-aware or NSF-capable devices, and the default or user-defined value for the route-hold timer is displayed.
- “EIGRP NSF enabled” or “EIGRP NSF disabled” appears in the output only when the NSF capability is supported by the device.

```
Device# show ip protocols

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
```

```
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

Example: Configuring Cisco NSF-OSPF

The following example shows how to enable Cisco Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 400
Device(config-router)# nsf cisco helper
Device(config-router)# nsf ietf helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 400. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, IETF helper mode is disabled for process 400.

```
Device> show ip ospf nsf

Routing Process "ospf 400"
Non-Stop Forwarding enabled
IETF NSF helper support disabled
Cisco NSF helper support enabled
  OSPF restart state is NO_RESTART
  Handle 2162698, Router ID 192.168.2.155, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example: Configuring IETF NSF-OSPF

The following example shows how to enable IETF Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 500
Device(config-router)# nsf ietf helper strict-lsa-checking
Device(config-router)# nsf cisco helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 500. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, Cisco helper mode is disabled.

```
Device> show ip ospf nsf
```

```
Routing Process "ospf 500"
Non-Stop Forwarding enabled
IETF NSF helper support enabled
Cisco NSF helper support disabled
  OSPF restart state is NO_RESTART
  Handle 1786466333, Router ID 10.1.1.1, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example IS-ISNSF

The following partial output shows that this device uses the Cisco implementation of IS-IS NSF. The display will show either Cisco IS-IS or IETF IS-IS configuration.

```
Router# show running-config
router isis
nsf cisco
```

In a Cisco NSF configuration, the display output is different on the active and the standby RPs.

The following sample output on the active RP shows that Cisco NSF is enabled on the device:

```
Router# show isis nsf
NSF is ENABLED, mode 'cisco'
RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

The following sample output on the standby RP shows that NSF is enabled on the device (NSF restart enabled):

```
Router# show isis nsf
NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

The following sample output shows that IETF NSF is configured for the IS-IS networking device:

```
Router# show isis nsf
NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
```

```
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco debug commands	*Cisco IOS Debug Command Reference*
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*
BGP support for NSF	BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) module in the *Cisco IOS IP Routing: BGP Configuration Guide*
EIGRP NSF awareness	EIGRP Nonstop Awareness module in the *Cisco IOS IP Routing: EIGRP Configuration Guide*
IPv6 BGP graceful restart	Implementing Multiprotocol BGP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
IPv6 RIP	Implementing RIP for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
IPv6 static routes	Implementing Static Routes for IPv6 module in the *Cisco IOS IPv6 Configuration Guide*
• MFIB: IPv4 SSO/ISSU • NSF/SSO--IPv4 Multicast	Monitoring and Maintaining Multicast HA Operations (NSF/SSO and ISSU) module in the *Cisco IOS IP Multicast Configuration Guide*
NSF/SSO--802.3ah OAM Support	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*

Related Topic	Document Title
NSF/SSO--Any Transport over MPLS (AToM)	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
NSF/SSO--E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
NSF/SSO--MPLS VPN	Configuring NSF/SSO--MPLS VPN module in the *MPLS Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

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
RFC 3623	*Graceful OSPF Restart*
RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
RFC 4781	*Graceful Restart Mechanism for BGP*

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 Nonstop Forwarding

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 . An account on Cisco.com is not required.

Table 13: Feature Information for Nonstop Forwarding

Feature Name	Releases	Feature Information
EIGRP Nonstop Forwarding (NSF) Awareness	12.2(18)S	NSF support for EIGRP allows an NSF-aware device that is running EIGRP to forward packets along routes known to a device performing a switchover operation or in a well-known failure condition. The following commands were introduced or modified: **debug eigrp nsf**, **debug ip eigrp notifications**, **show ip eigrp neighbors**, **show ip protocols**, **timers graceful-restart purge-time**, **timers nsf route-hold**.
MFIB: IPv4 SSO/ISSU	12.2(33)SRE	This feature was introduced.

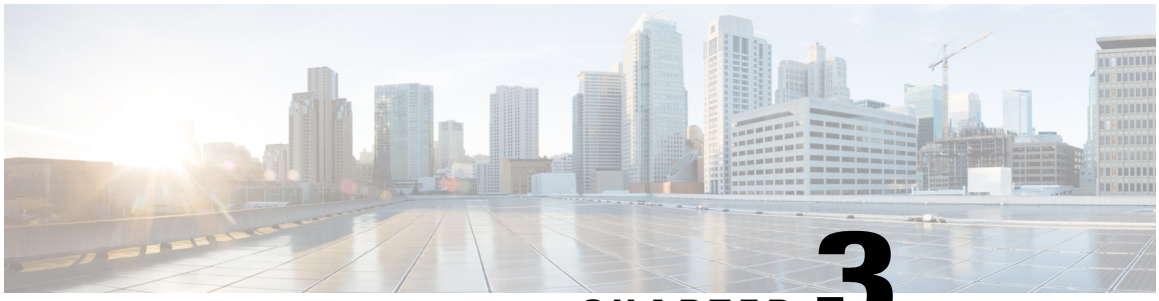
Feature Name	Releases	Feature Information
Nonstop Forwarding Support for EIGRP	12.2(18)S 12.2(28)SB	NSF support for EIGRP allows an NSF-aware device that is running EIGRP to forward packets along routes known to a device performing a switchover operation or in a well-known failure condition. The following commands were introduced or modified: **nsf**(EIGRP), **router eigrp**, **timers nsf converge**, **timers nsf signal.**
NSF Awareness--OSPF	12.2(31)SB2 15.0(1)S	Allows customer premises equipment (CPE) devices to participate in the upstream device's NSF recovery process. The following commands were introduced or modified: **debug ospf nsf**, **nsf** (OSPF), **nsf cisco**, **nsf ietf**, **show ip ospf neighbor**, **show ip ospf nsf**.
NSF--OSPF (RFC 3623 OSPF Graceful Restart)	12.0(32)S 12.2(33)SRA 12.2(31)SB2 12.2(33)SXH	NSF for OSPFv2 in Cisco IOS software, using the IETF standardized graceful restart functionality as described in RFC 3623, was introduced. The following commands were introduced or modified: **nsf cisco**, **nsf ietf**, **nsf (OSPF).**
NSF--Graceful Restart (GR) and Non Stop Routing (NSR) for IS-IS Road/FIT	15.0(1)S	This feature is supported.

Feature Name	Releases	Feature Information
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	12.0(22)S 12.0(23)S 12.0(24)S 12.2(20)S 15.0(1)S	

Feature Name	Releases	Feature Information

		This feature was introduced.
		In Cisco IOS Release 12.0(23)S, support was added for 1xGE and 3xGE line cards on the Cisco 12000 series Internet router.
		In Cisco IOS Release 12.0(24)S, support was added for the following line cards on the Cisco 12000 series Internet router.
		• Engine 1
		  • 2-port OC-12/STM-4c DPT
		• Engine 2
		  • 1-port OC-48/STM-16c DPT
		  • 8-port OC-3/STM-1c ATM
		• IP Service Engine (ISE)
		  • 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

Feature Name	Releases	Feature Information
		The following commands were introduced or modified: **bgp graceful-restart**, **debug isis nsf**, **ip cef distributed**, **nsf**(IS-IS), **nsf interface wait**, **nsf interval**, **nsf t3**, **router bgp**, **router isis**, **router ospf**, **show cef nsf**, **show cef state**, **show clns neighbors**, **show ip bgp**, **show ip bgp neighbors**, **show ip cef**, **show ip eigrp neighbors**, **show ip protocols**, **show isis database**, **show isis nsf**.
NSF/SSO--MPLS VPN	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature allows a provider edge (PE) router or Autonomous System Border Router (ASBR) (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor restarts. In 12.2(25)S, this feature was introduced on the Cisco 7500 series router. In 12.2(28)SB, support was added for the Cisco 10000 series routers. In 12.2(33)SRA, support was added for the Cisco 7600 series routers.
NSF/SSO--Virtual Private LAN Services	12.2(33)SXI4 15.0(1)S	This feature was introduced.
NSF/SSO--IPv4 Multicast	12.2(33)SRE 15.0(1)S	This feature was introduced.
NSF/SSO--IPv6 Multicast	12.2(33)SRE	This feature was introduced.



CHAPTER 3

Performing an In Service Software Upgrade

This module describes how to perform an In Service Software Upgrade (ISSU) process.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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

Prerequisites for Performing an ISSU

- Both the active and standby route processors (RPs) must be available in the system.
- The new and old Cisco software images must be loaded into the file systems of both the active and standby RPs before you begin the ISSU process.
- Stateful switchover (SSO) must be configured and working properly.
- Nonstop forwarding (NSF) must be configured and working properly.

- Before you perform ISSU, the file system for both the active and standby RPs must contain the new ISSU-compatible image. The current version running in the system must also support ISSU. You can issue various commands to determine RP versioning and compatibility, or you can use the ISSU application on Cisco Feature Navigator.

Restrictions for Performing an ISSU

General Restrictions

- Do not make hardware changes while performing an ISSU process.
- Perform upgrades only during a maintenance window. (Recommended)
- Do not enable new features that require configuration changes during the ISSU process.
- If a feature is not available in a downgrade of a Cisco software image, disable that feature before you initiate the ISSU process.
- A permanent "ISSU barrier" exists between pre-IOS XE 3.6.0E and IOS XE 3.6.0 releases: ISSU is supported between versions on the same side of the barrier but it is not supported between versions on opposite sides.

Note This restriction applies to Catalyst 4500X in a VSS, as well as to Supervisor Engine 7E, Supervisor Engine 7LE, and Supervisor Engine 8E in a VSS or in a redundant chassis. Four scenarios will illustrate the restriction:

- If you are running a release prior to IOS XE 3.6.0E (3.5.1E, for example), you cannot perform an ISSU upgrade to IOS XE 3.6.0E.
- If you are running IOS XE 3.6.0E, you cannot perform an ISSU downgrade to IOS XE 3.5.0E.
- If you are running IOS XE 3.6.0E, you can perform an ISSU upgrade to IOS XE 3.6.1E (when released).
- If you are running a release after IOS XE 3.6.0E (for example, 3.7.0, when released), you cannot perform an ISSU downgrade to IOS XE 3.5.0E.

Termination of Virtual Template Manager for ISSU Restrictions

The Virtual Template Manager for ISSU is not supported in Cisco IOS Releases 12.2(31)SB and 12.2(33)SB.

Cisco 10000 Series Internet Router Platform Restrictions

- ISSU is available only in Cisco IOS 12.2(28)SB software released for theand later.

- The following line cards support ISSU:
  - 1-port channelized OC-12/STM-4
  - 1-port Gigabit Ethernet
  - 1-port half-height Gigabit Ethernet
  - 1-port OC-12 ATM
  - 1-port OC-12 Packet over SONET (PoS)
  - l-port OC-48 PoS
  - 4-port channelized OC-3/STM-1
  - 4-port OC-3 ATM IR
  - 4-port OC-3 ATM LR
  - 4-port half-height channelized T3
  - 6-port channelized T3
  - 6-port OC-3 PoS
  - 8-port ATM E3/DS3
  - 8-port E3/DS3
  - 8-port half-height Fast Ethernet
  - 24-port channelized E1/T1
- The following interface cards support ISSU:
  - SPA Interface Processor (10000-SIP-600)
  - 2-port GE SPA
  - 5-port GE SPA
  - 8-port GE SPA
  - 1-port 10GE SPA

Cisco Catalyst 4500 Restrictions

- The single-step complete upgrade process cycle is available on the Cisco Catalyst 4500 series switch in Cisco IOS Release 12.2(47)SG.
- An ISSU upgrade process available on the Cisco Catalyst 4500 series switch from any previous releases to Cisco IOS XE Release 3.6E is not supported. Installer uses compatibility meta data prior to performing ISSU, and upgrade to non-compatible image is terminated.

Information About Performing an ISSU

ISSU Process Overview

ISSU allows Cisco software to be upgraded or downgraded, at a router level, while the system continues to forward packets. ISSU takes advantage of the Cisco high availability infrastructure--Cisco NSF with SSO and hardware redundancy--and eliminates downtime associated with software upgrades or version changes by allowing updates while the system remains in service. Cisco high availability features combine to lower the impact that planned maintenance activities have on network service availability, with the results of less downtime and better access to critical systems.

SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two Route Processors (RPs) to remain synchronized although they may support different sets of commands.

An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, you must copy the Cisco IOS software into the file systems of both RPs

After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP.

After switchover, the standby RP takes over as the new active RP.

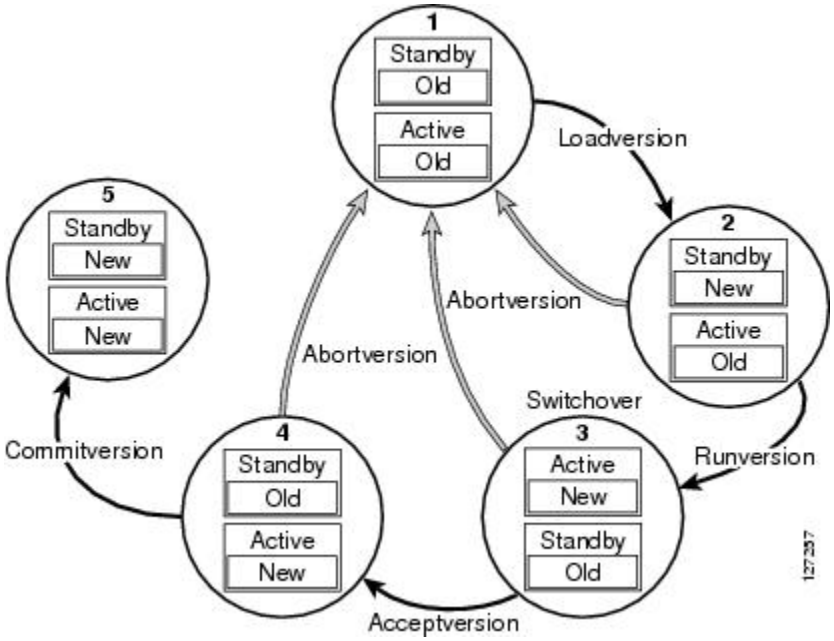
Then, the former active RP, which is now the new standby RP, is loaded with the new software.

The two RPs in a system can be in one of three different states during ISSU:

- Active--One RP is actively forwarding packets with old software. After the ISSU process is performed, the original active RP becomes the standby RP.
- Standby--Perform ISSU on the standby RP, loading it with new software. After the ISSU process is performed, the original standby RP is the new active RP.
- Hot standby--After the original standby RP becomes the new active RP, load the new software image into the new standby RP. Doing so makes the standby RP a hot standby RP.

The figure below shows the ISSU states during the ISSU process.

Figure 3: ISSU States During the ISSU Process



ISSU Rollback Timer

Cisco IOS software maintains an ISSU rollback timer. The rollback timer provides a safeguard against an upgrade that may leave the new active RP in a state in which communication with the RP is severed.

Configuring the rollback timer to fewer than 45 minutes (the default) eliminates waiting in case the new software is not committed or the connection to the router is lost while it is in runversion mode. Configure the rollback timer to more than 45 minutes in order to have enough time to verify the operation of the new Cisco IOS software before committing the new image.

Fast Software Upgrade

When Cisco IOS software versions are not compatible and ISSU is not possible, the FSU procedure can be performed within the ISSU command context. Through the use of optional parameters in ISSU commands, the system reverts to RPR mode rather than the SSO mode required for ISSU.

FSU using the ISSU command context works only with ISSU-aware Cisco software versions. If you want to downgrade to a pre-ISSU version, you must use the manual FSU method.

Enhanced Fast Software Upgrade

Enhanced Fast Software Upgrade (eFSU) is an improvement over FSU, reducing the downtime during a Cisco software upgrade.

At the linecard level, an enhanced Fast Software Upgrade (eFSU) process minimizes linecard downtime during upgrades to between 30 and 90 seconds, by pre-loading the new linecard image before the ISSU switchover occurs from the active to the standby Route Processor.

See the Enhanced Fast Software Upgrade on the Cisco 7600 Series Routers for more information.

Versioning Capability in Cisco Software to Support ISSU

Before the introduction of the ISSU capability, the SSO mode of operation required each RP to be running the same versions of Cisco software. The operating mode of the system in a redundant HA configuration is determined by exchanging version strings when the standby RP registers with the active RP.

The system entered SSO mode only if the versions running on both RPs were the same. If not, the redundancy mode was reduced to ensure compatibility. With ISSU capability, the implementation allows two different but compatible release levels of Cisco software images to interoperate in SSO mode and enables software upgrades while packet forwarding continues. Version checking done before ISSU capability was introduced is no longer sufficient to allow the system to determine the operating mode.

ISSU requires additional information to determine compatibility between software versions. Therefore, a compatibility matrix is defined that contains information about other images with respect to the one in question. This compatibility matrix represents the compatibility of two software versions, one running on the active and the other on the standby RP, and to allow the system to determine the highest operating mode it can achieve. Incompatible versions will not be able to progress to SSO operational mode.

The Cisco software infrastructure has been internally modified and redesigned to accommodate subsystem versioning with ISSU. Cisco software subsystems correspond to feature sets and software component groupings. Features or subsystems that maintain state information across RPs are HA-aware or SSO clients. A mechanism called ISSU Framework, or ISSU protocol, allows subsystems within Cisco software to communicate RP to RP and to negotiate the message version for communication between RPs. Internally, all NSF- and SSO-compliant applications or subsystems that are HA-aware must follow this protocol to establish communication with their peer across different versions of software.

Compatibility Matrix

You can perform the ISSU process when the Cisco software on both the active and the standby RP is capable of ISSU and the old and new images are compatible. The compatibility matrix information stores the compatibility among releases as follows:

- Compatible--The base-level system infrastructure and all optional HA-aware subsystems are compatible. An in-service upgrade or downgrade between these versions will succeed with minimal service impact. The matrix entry designates the images to be compatible (C).
- Base-level compatible--One or more of the optional HA-aware subsystems is not compatible. An in-service upgrade or downgrade between these versions will succeed; however, some subsystems will not be able to maintain state during the transition. The matrix entry designates the images to be base-level compatible (B).
- Incompatible--A core set of system infrastructure exists that must be able to interoperate in a stateful manner for SSO to function correctly. If any of these required features or protocols is not interoperable, then the two versions of the Cisco software images are declared to be incompatible. An in-service upgrade or downgrade between these versions is not possible. The matrix entry designates the images to be incompatible (I).

If you attempt to perform ISSU with a peer that does not support ISSU, the system automatically uses Fast Software Upgrade (FSU) instead.

The compatibility matrix represents the compatibility relationship a Cisco software image has with all of the other Cisco software versions within the designated support window (for example, all of those software versions the image "knows" about) and is populated and released with every image. The matrix stores compatibility information between its own release and prior releases. It is always the newest release that contains the latest information about compatibility with existing releases in the field. The compatibility matrix is available within the Cisco software image and on Cisco.com so that users can determine in advance whether an upgrade can be done using the ISSU process.

SNMP Support for ISSU

ISSU - SNMP for SSO provides a mechanism for synchronizing the Simple Network Management Protocol (SNMP) configurations and the MIBs that support SSO from the active RP to the standby RP, assuming that both RPs are running the same version of Cisco software. This assumption is not valid for ISSU.

ISSU - SNMP provides an SNMP client that can handle ISSU transformations for the MIBs. An SNMP client (SIC) handles ISSU for all MIBs and handles the transmit and receive functions required for ISSU. During SNMP, a MIB is completely synchronized from the active RP to the standby RP only if the versions of the MIB on both Cisco software releases are the same.

Virtual Template Manager for ISSU

The virtual template manager feature for ISSU 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 virtual access interfaces 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.

Compatibility Verification Using Cisco Feature Navigator

The ISSU application on Cisco Feature Navigator allows you to:

- Select an ISSU-capable image
- Identify which images are compatible with that image
- Compare two images and understand the compatibility level of the images (that is, compatible, base-level compatible, and incompatible)
- Compare two images and see the client compatibility for each ISSU client
- Provide links to release notes for the image

ISSU-Capable Protocols and Applications

The following protocols and applications support ISSU:

- FHRP - HSRP Group Shutdown--FHRP - HSRP group shutdown is supported in ISSU.
- ISSU - ARP--Address Resolution Protocol (ARP) is supported in ISSU.
- ISSU - ATM--Asynchronous Transfer Mode (ATM) is supported in ISSU. The application requirements for ISSU are as follows:
  - Identify the ATM client as nonbase
  - Support message versioning of ATM HA event synchronous messages
  - Provide capability exchange between peers
- ISSU - Dynamic Host Configuration Protocol (DHCP) on-demand address pool (ODAP) client/server--This feature is supported in ISSU.
- ISSU - DHCP proxy client--The DHCP proxy client feature is supported in ISSU.
- ISSU - DHCP relay on unnumbered interface--The DHCP relay on unnumbered interface feature is supported in ISSU.
- ISSU - DHCP server--The DHCP server feature is supported in ISSU.
- ISSU - DHCP snooping--DHCP snooping is supported in ISSU.
- ISSU - EtherChannel - Port Aggregation Protocol (PagP) and Link Aggregate Control Protocol (LACP) support ISSU.
- ISSU - First Hop Routing Protocol (FHRP) - Gateway Load Balancing Protocol (GLBP) is supported in ISSU.
- ISSU - FHRP/HSRP--The Hot Standby Router Protocol (HSRP) is supported in ISSU.
- ISSU - Frame Relay--The Frame Relay protocol is supported in ISSU.
- ISSU - HDLC--The High-Level Data Link Control (HDLC) protocol is supported in ISSU.
- ISSU - IEEE 802.1x--The IEEE 802.1x protocol is supported in ISSU.
- ISSU - IEEE 802.3af--IEEE 802.3af is supported in ISSU.
- ISSU - Internet Group Management Protocol (IGMP) snooping--IGMP snooping is supported in ISSU.
- ISSU - IP host--The IP host is supported in ISSU.
- ISSU - IPv4 Multicast - IPv4 multicast is supported in ISSU.
- ISSU - IS-IS--The Intermediate System-to-Intermediate System (IS-IS) protocol is supported in ISSU.
- ISSU - MTR--Multitopology routing (MTR) is supported in ISSU.
- ISSU - MPLS L3VPN--Multiprotocol Label Switching (MPLS) is supported in ISSU. For information about upgrading ISSU MPLS-related applications through ISSUt.
- ISSU - Port security--Port security is supported in ISSU.
- ISSU - PPP/MLP--multilink PPP (MLP) support ISSU.

- ISSU - PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) support ISSU.
- ISSU - QoS support--The quality of service (QoS) feature is supported in ISSU.
- ISSU - RIB/VRF - The RIB/VRF feature is supported in ISSU.
- ISSU - SNMP--SNMP is supported in ISSU.
- ISSU - Spanning-Tree Protocol (STP)--STP is supported in ISSU.

How to Perform an ISSU

Displaying ISSU Compatibility Matrix Information

SUMMARY STEPS

1. **enable**
2. **show issu comp-matrix** {**negotiated** | **stored**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu comp-matrix** {**negotiated**	**stored**} **Example:** `Device# show issu comp-matrix negotiated`	Displays information about the the compatibility of the two software versions, one running on the active and the other on the standby RP.

Loading Cisco IOS Software on the Standby RP

SUMMARY STEPS

1. **enable**
2. **issu loadversion** *image-name*
3. **show issu state** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu loadversion** *image-name* **Example:** `Device# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830`	Starts the ISSU process. **Note** The active and standby slots are optional for this command. You must provide the same image-name for both the active and standby slots. Active slot number is not available for this command. It may take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load onto the standby RP and for the standby RP to transition to SSO mode.
Step 3	**show issu state** [**detail**] **Example:** `Device# show issu state`	Displays the state of the device during the ISSU process. • Confirm that the standby RP is loaded and is in SSO mode.

Switching to the Standby RP

SUMMARY STEPS

1. **enable**
2. **issu runversion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**issu runversion** **Example:** `Device# issu runversion b stby-disk0:c10k2-p11-mz.2.20040830`	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image. **Note** The *slot image* parameter is optional for this command.

Stopping the ISSU Rollback Timer

SUMMARY STEPS

1. **enable**
2. **show issu rollback-timer**
3. **issu acceptversion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu rollback-timer** **Example:** `Device# show issu rollback-timer`	Displays amount of time left before an automatic rollback will occur.
Step 3	**issu acceptversion** **Example:** `Device# issu acceptversion b disk0:c10k2-p11-mz.2.20040830`	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process. • You must enter this command within the time period specified by the rollback timer displayed in the previous step. • The active slot-number and slot-name parameters are optional for this command.

Verifying the ISSU Software Installation

SUMMARY STEPS

1. **enable**
2. **show issu state** [**detail**]
3. **show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **states** | **inter-device**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu state** [**detail**] **Example:** `Device# show issu state`	Displays the state of the RPs during the ISSU process.
Step 3	**show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **states** | **inter-device**] **Example:** `Device# show redundancy`	Displays current or historical status, mode, and related redundancy information about the device.

Enabling the New Standby RP to Use New Software Version

SUMMARY STEPS

1. **enable**
2. **issu commitversion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**issu commitversion** **Example:** `Device# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830`	Allows the new Cisco IOS software image to be loaded into the standby RP. **Note** The *slot active-image* parameter is optional for this command.

Aborting a Software Upgrade Using ISSU

If you abort the process after you load a new version on the standby RP and before switching to the standby RP, the standby RP is reset and reloaded with the original software.

If you abort the process after switching to the standby RP or stopping an automatic rollback, a second switchover is performed to the new standby RP that is still running the original software version. The RP that had been running the new software is reset and reloaded with the original software version.

SUMMARY STEPS

1. **enable**
2. **issu abortversion** *slot image*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu abortversion** *slot image* **Example:** `Device# issu abortversion b disk0:c10k2-p11-mz.2.20040830`	Aborts the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.

Configuring the Rollback Timer to Safeguard Against Upgrades

Before You Begin

The Route Processors (RPs) must be in the init state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configure issu set rollback timer** *seconds*
4. **exit**
5. **show issu rollback timer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**configure issu set rollback timer** *seconds* **Example:** `Device(config)# configure issu set rollback timer 3600`	Configures the rollback timer value.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns the user to privileged EXEC mode.
Step 5	**show issu rollback timer** **Example:** `Device# show issu rollback timer`	Displays the current setting of the ISSU rollback timer.

Configuration Examples for Performing an ISSU

Example Verifying Redundancy Mode Before Beginning the ISSU Process

Before you begin the ISSU process, verify the redundancy mode for the system. NSF and SSO must be configured before attempting an ISSU. The following example displays verification that the system is in SSO mode and that slot A--RP A is the active R, and slot B--RP B is the standby RP. Both RPs are running the same Cisco software image.

```
Device# show redundancy states
        my state = 13 -ACTIVE
      peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 0
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 31
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
Device# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 9 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 A
        Current Software state = ACTIVE
       Uptime in current state = 9 minutes
Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M), Experimental Version
12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 102] Copyright (c) 1986-2004 by Cisco
Systems, Inc. Compiled Mon 30-Aug-04 10:29 by wgrupp
                          BOOT = disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                       BOOTLDR =
       Configuration register = 0x102
Peer Processor Information :
----------------------------
              Standby Location = slot B
        Current Software state = STANDBY HOT
       Uptime in current state = 8 minutes
                  Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M),
Experimental Version 12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 102] Copyright (c)
1986-2004 by Cisco Systems, Inc. Compiled Mon 30-Aug-04 10:29 by wgrupp
                          BOOT = disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                       BOOTLDR =
       Configuration register = 0x102
```

Example Verifying the ISSU State

The following sample output displays and verifies the ISSU state:

```
Device# show issu state detail

                        Slot = A
                   RP State = Active
                  ISSU State = Init
                Boot Variable = N/A
               Operating Mode = SSO
              Primary Version = N/A
            Secondary Version = N/A
              Current Version = disk0:c10k2-p11-mz.1.20040830
                        Slot = B
                   RP State = Standby
                  ISSU State = Init
                Boot Variable = N/A
               Operating Mode = SSO
              Primary Version = N/A
            Secondary Version = N/A
              Current Version = disk0:c10k2-p11-mz.1.20040830
```

The new version of the Cisco IOS software must be present on both of the RPs. The directory information displayed for each of the RPs shows that the new version is present.

```
Device# directory disk0:
Directory of disk0:/
    1  -rw-    16864340  Jul 16 2004 01:59:42 -04:00  c10k2-p11-mz.122-16.BX1.bin
    2  -rw-     2530912  Jul 16 2004 02:00:04 -04:00  c10k2-eboot-mz.122-16.BX1.bin
    3  -rw-    20172208  Aug 30 2004 16:25:56 -04:00  c10k2-p11-mz.1.20040830
    4  -rw-    20171492  Aug 31 2004 12:25:34 -04:00  c10k2-p11-mz.2.20040830
64253952 bytes total (4509696 bytes free)
Device# directory stby-disk0:
Directory of stby-disk0:/
```

Example Performing the ISSU Process

The following examples show how to verify the ISSU software installation by entering **show** commands that provide information on the state of theduring the ISSU process.

Initiating the ISSU Process

To initiate the ISSU process, enter the **issu loadversion** command as shown in the following example:

```
Device# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830
```

The following two examples display the ISSU state and redundancy state after ISSU process initiation:

```
Device# show issu state
                        Slot = A
                   RP State = Active
                  ISSU State = Load Version
                Boot Variable = disk0:c10k2-p11-mz.1.20040830,1;
                        Slot = B
                   RP State = Standby
                  ISSU State = Load Version
                Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
Device# show redundancy state
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
```

```
           Mode = Duplex
           Unit = Primary
        Unit ID = 0
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 31
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

Forcing a Switchover from the Active RP to the Standby RP

At this point, the system is ready to switch over and run the new version of Cisco software that has been loaded onto the standby RP. When you enter the **issu runversion** command, an SSO switchover will be performed, and NSF procedures will be invoked if so configured.

```
Device# issu runversion b stby-disk0:c10k2-p11-mz.2.20040830
```

Once the ISSU process has been completed, the system will be running the new version of software and the previously active RP will now become the standby RP. The standby will be reset and reloaded, but it will remain on the previous version of software and come back online in STANDBY-HOT status. The following example shows how to connect to the newly active RP and verify these conditions.

```
Device# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 24 minutes
Switchovers system experienced = 1
             Standby failures = 0
        Last switchover reason = user initiated
                 Hardware Mode = Duplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up
Current Processor Information :
-------------------------------
               Active Location = slot B
        Current Software state = ACTIVE
       Uptime in current state = 8 minutes
                 Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M),
Experimental Version 12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 103] Copyright (c)
1986-2004 by Cisco Systems, Inc. Compiled Mon 30-Aug-04 11:50 by wgrupp
                          BOOT =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x102
Peer Processor Information :
----------------------------
              Standby Location = slot A
        Current Software state = STANDBY HOT
       Uptime in current state = 6 minutes
                 Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M),
Experimental Version 12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 102] Copyright (c)
1986-2004 by Cisco Systems, Inc. Compiled Mon 30-Aug-04 10:29 by wgrupp
                          BOOT = disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x102
Device# show issu state
                          Slot = B
                     RP State = Active
                    ISSU State = Run Version
                  Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                          Slot = A
```

```
                    RP State = Standby
                  ISSU State = Run Version
                Boot Variable = disk0:c10k2-p11-mz.1.20040830,1;
Device# show issu state detail
                           Slot = B
                    RP State = Active
                  ISSU State = Run Version
                Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
               Operating Mode = SSO
             Primary Version = disk0:c10k2-p11-mz.2.20040830
           Secondary Version = disk0:c10k2-p11-mz.1.20040830
             Current Version = disk0:c10k2-p11-mz.2.20040830
                           Slot = A
                    RP State = Standby
                  ISSU State = Run Version
                Boot Variable = disk0:c10k2-p11-mz.1.20040830,1;
               Operating Mode = SSO
             Primary Version = disk0:c10k2-p11-mz.2.20040830
           Secondary Version = disk0:c10k2-p11-mz.1.20040830
             Current Version = disk0:c10k2-p11-mz.1.20040830
```

The new active RP is now running the new version of software, and the standby RP is running the old version of software and is in the STANDBY-HOT state.

Stopping the Rollback Process

In the following example, the "Automatic Rollback Time" information indicates the amount of time left before an automatic rollback will occur. Enter the **issu acceptversion** command within the time period specified by the rollback timer to acknowledge that the RP has achieved connectivity to the outside world; otherwise, the ISSU process is terminated, and the system reverts to the previous version of Cisco software by switching to the standby RP.

```
Device# show issu rollback-timer

Rollback Process State = In progress
Configured Rollback Time = 45:00
Automatic Rollback Time = 29:03
```

Entering the **issu acceptversion** command stops the rollback timer:

```
Device# issu acceptversion b disk0:c10k2-p11-mz.2.20040830
```

Committing the New Software to the Standby RP

The following example shows how to commit the new Cisco software image in the file system of the standby RP and ensure that both the active and the standby RPs are in the run version (RV) state. The standby RP is reset and reloaded with the new Cisco software and returned to STANDBY-HOT status.

```
Device# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830
Device# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Secondary
        Unit ID = 1
Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured)  = SSO
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 31
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
Device# show redundancy
Redundant System Information :
------------------------------
```

```
       Available system uptime = 35 minutes
Switchovers system experienced = 1
             Standby failures = 1
        Last switchover reason = user initiated
                 Hardware Mode = Duplex
Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up
Current Processor Information :
-------------------------------
               Active Location = slot B
        Current Software state = ACTIVE
       Uptime in current state = 18 minutes
                 Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M),
Experimental Version 12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 103] Copyright (c)
1986-2004 by Cisco Systems, Inc. Compiled Mon 30-Aug-04 11:50 by wgrupp
                        BOOT =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x102
Peer Processor Information :
----------------------------
              Standby Location = slot A
        Current Software state = STANDBY HOT
       Uptime in current state = 4 minutes
                 Image Version = Cisco IOS Software, 10000 Software (C10K2-P11-M),
Experimental Version 12.2(20040825:224856) [wgrupp-c10k_bba_122s_work 103] Copyright (c)
1986-2004 by Cisco Systems, Inc. Compiled Mon 30-Aug-04 11:50 by wgrupp
                        BOOT =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                   CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x102
Device# show issu state
                           Slot = B
                      RP State = Active
                     ISSU State = Init
                  Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                           Slot = A
                      RP State = Standby
                     ISSU State = Init
                  Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
Device# show issu state detail
                           Slot = B
                      RP State = Active
                     ISSU State = Init
                  Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                 Operating Mode = SSO
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = disk0:c10k2-p11-mz.2.20040830
                           Slot = A
                      RP State = Standby
                     ISSU State = Init
                  Boot Variable =
disk0:c10k2-p11-mz.2.20040830,12;disk0:c10k2-p11-mz.1.20040830,1;
                 Operating Mode = SSO
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = disk0:c10k2-p11-mz.2.20040830
```

The ISSU process has been completed. At this stage, any further Cisco software version upgrades or downgrades will require that a new ISSU process be invoked.

Example Aborting the ISSU Process

The following example shows how to abort the ISSU process manually:

```
Device# issu abortversion
 b disk0:c10k2-p11-mz.2.20040830
```

If you abort the process after you have entered the **issu loadversion** command, the standby RP is reset and is reloaded with the original software version.

Example Verifying Rollback Timer Information

To display rollback timer information, enter the **show issu rollback-timer**command:

```
Device# show issu rollback-timer

        Rollback Process State = In progress
      Configured Rollback Time = 45:00
       Automatic Rollback Time = 29:03
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS master command list	Cisco IOS Master Command List , All Releases
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*
DHCP ODAP client/server	ISSU - DHCP ODAP Client and Server module in the *Cisco IOS IP Addressing Services Configuration Guide*
DHCP proxy client	ISSU - DHCP Proxy Client module in the *Cisco IOS IP Addressing Services Configuration Guide*
DHCP relay on unnumbered interface	ISSU - DHCP Relay on Unnumbered Interface module in the *Cisco IOS IP Addressing Services Configuration Guide*
DHCP server	ISSU - DHCP Server module in the *Cisco IOS IP Addressing Services Configuration Guide*
Enhanced Fast Software Upgrade (eFSU)	Enhanced Fast Software Upgrade on the Cisco 7600 Series Router
FHRP and HSRP group shutdown	FHRP - HSRP Group Shutdown module in the *Cisco IOS IP Application Services Configuration Guide*

Related Topic	Document Title
ISSU - 802.3ah OAM	Using Ethernet Operations, Administration, and Maintenance module in the *Cisco IOS Carrier Ethernet Configuration Guide*
ISSU - AToM ATM Attachment Circuit	Any Transport over MPLS and AToM Graceful Restart module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
ISSU and eFSU on Cisco 7600 series routers	ISSU and eFSU on Cisco 7600 Series Routers module in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*
ISSU- E-LMI Support	Configuring Ethernet Local Management Interface at a Provider Edge module in the *Cisco IOS Carrier Ethernet Configuration Guide*
ISSU - IPv4 multicast	Monitoring and Maintaining Multicast HA Operations (NSF/SSO and ISSU) module in the *Cisco IOS IP Multicast Configuration Guide*
ISSU - PPoE	Cisco IOS Broadband High Availability In Service Software Upgrade module in the *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
ISSU - VRRP	Configuring VRRP module in the *Cisco IOS IP Application Services Configuration Guide*
MPLS clients	ISSU MPLS Clients module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*
MTR	*Cisco IOS Multi-Topology Routing Configuration Guide*
Virtual Private LAN Services	NSF/SSO/ISSU Support for VPLS module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

Standards

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

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, and support for existing RFCs has not been modified.	--

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 Performing an ISSU

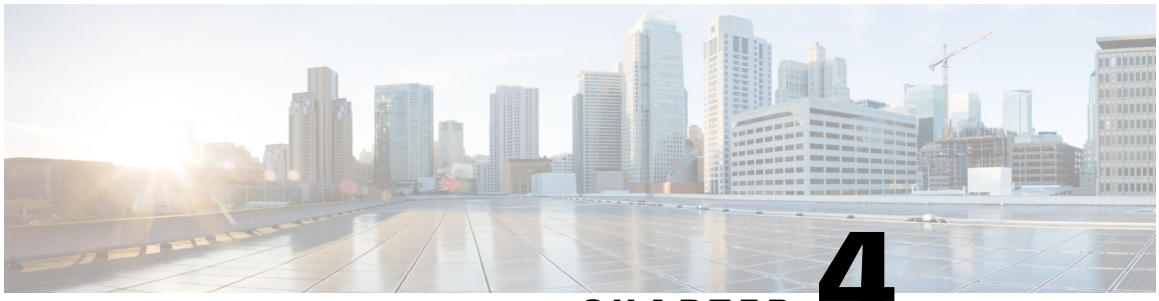
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 . An account on Cisco.com is not required.

Table 14: Feature Information for Performing an In Service Software Upgrade Process

Feature Name	Releases	Feature Information

ISSU		In Service Software Upgrade (ISSU) allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues, increasing network availability and reducing downtime caused by planned software upgrades.



CHAPTER 4

Configuring NSF-OSPF

This module describes how to configure Nonstop Forwarding (NSF) in Cisco software to minimize the duration for which a network is unavailable to its users after a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. NSF is supported by the Open Shortest Path First (OSPF) protocol for routing. A device that is running NSF-compatible software is known as an NSF-aware device and a device that is configured to support NSF is called an NSF-capable device. NSF-capable devices can rebuild routing information from either NSF-aware or NSF-capable neighboring devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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

Prerequisites for NSF-OSPF

For Nonstop Forwarding (NSF) Open Shortest Path First (OSPF), all networking devices on the network segment must be NSF-aware.

Restrictions for NSF-OSPF

- Nonstop Forwarding (NSF) capability is not enabled by default for the Open Shortest Path First (OSPF) configurations.
- NSF OSPF for virtual links is not supported.
- NSF OSPF for sham links is not supported.
- NSF OSPF supports NSF/Stateful Switchover (SSO) for IPv4 traffic only.
- OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.
- If an NSF-capable device discovers that it has non-NSF-aware neighbors on a particular network segment, the device will disable NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware devices will continue to provide NSF capabilities.
- You can configure strict link state advertisement (LSA) checking on both NSF-aware and NSF-capable devices. However, configuring an LSA is effective only when the device is in helper mode.

Information About NSF-OSPF

NSF-OSPF Operations

For Cisco Nonstop Forwarding (NSF), the Open Shortest Path First (OSPF) routing protocol has been enhanced to support high availability (HA) features in Stateful Switchover (SSO). Before an OSPF NSF-capable device can perform a Route Processor (RP) switchover, the device must be aware of the available OSPF neighbors on the network without resetting the neighbor relationship, and the device must acquire the contents of the link state database for the network. The NSF-capable device sends an OSPF NSF signal to neighboring NSF-aware devices to notify the devices that the neighbor relationship with the sending device must not be reset. The NSF-capable device uses the signals that it receives from other devices on the network to rebuild its neighbor list.

The NSF-capable device synchronizes its database with all the NSF-aware neighbors on its neighbor list. After all neighbors exchange routing information, the NSF-capable device uses the routing information to remove stale routes and update the routing information base (RIB) and the forwarding information base (FIB) with the new forwarding information. The OSPF protocols are then fully converged.

Prior to RFC 3623, Cisco implemented the proprietary Cisco NSF. The RFC 3623 Graceful OSPF Restart feature supports IETF NSF for OSPF processes in multivendor networks. The following are NSF device modes of operation common to Cisco and IETF NSF implementations:

- Restarting mode—In this mode, the OSPF device performs nonstop forwarding recovery because of an RP switchover.

- Helper mode—Also known as NSF-awareness mode. In this mode, the neighboring device is in the restarting state and helps in NSF recovery.

The strict link state advertisement (LSA) checking feature allows a helper device to terminate the graceful restart process if the device detects a changed LSA that would cause flooding during the graceful restart process. Strict LSA checking is disabled by default. You can enable strict LSA checking when there is a change to an LSA that would be flooded to the restarting device.

How to Configure NSF-OSPF

Configuring NSF-OSPF

Perform only one of the following tasks:

Configuring Cisco NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf cisco** [**enforce global**]
5. **nsf cisco helper** [**disable**]
6. **nsf ietf helper** [**disable** | **strict-lsa-checking**]
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf cisco** [**enforce global**] **Example:** `Device(config-router)# nsf cisco`	Enables Cisco Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in NSF helper mode.
Step 5	**nsf cisco helper** [**disable**] **Example:** `Device(config-router)# nsf cisco helper`	Enables Cisco NSF helper support. • This command shows how to enable Cisco NSF helper mode.
Step 6	**nsf ietf helper** [**disable** | **strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper disable`	(Optional) Disables IETF NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Configuring IETF NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf ietf** [**restart-interval** *seconds*]
5. **nsf ietf helper** [**disable** | **strict-lsa-checking**]
6. **nsf cisco helper disable**
7. **end**
8. **show ip ospf nsf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 12`	Enables Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf ietf** [**restart-interval** *seconds*] **Example:** `Device(config-router)# nsf ietf restart-interval 180`	Enables IETF Nonstop Forwarding (NSF) restarting mode. • This command is not required on devices that operate only in helper mode.
Step 5	**nsf ietf helper** [**disable**	**strict-lsa-checking**] **Example:** `Device(config-router)# nsf ietf helper strict-lsa-checking`	(Optional) Configures IETF NSF helper mode on neighbor devices that operate in helper mode.

	Command or Action	Purpose
Step 6	**nsf cisco helper disable** **Example:** `Device(config-router)# nsf cisco helper disable`	(Optional) Disables Cisco NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** `Device# show ip ospf nsf`	Displays OSPF NSF state information.

Verifying NSF-OSPF

SUMMARY STEPS

1. **enable**
2. **show ip ospf**
3. **show ip ospf neighbor** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf** **Example:** `Device# show ip ospf`	Displays general information about Open Shortest Path First (OSPF) routing processes.

	Command or Action	Purpose
Step 3	**show ip ospf neighbor** [**detail**] **Example:** `Device# show ip ospf neighbor detail`	Displays OSPF-neighbor information on a per-interface basis.

Configuration Examples for NSF-OSPF

Example: Configuring Cisco NSF-OSPF

The following example shows how to enable Cisco Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 400
Device(config-router)# nsf cisco helper
Device(config-router)# nsf ietf helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 400. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, IETF helper mode is disabled for process 400.

```
Device> show ip ospf nsf

Routing Process "ospf 400"
Non-Stop Forwarding enabled
IETF NSF helper support disabled
Cisco NSF helper support enabled
  OSPF restart state is NO_RESTART
  Handle 2162698, Router ID 192.168.2.155, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Example: Configuring IETF NSF-OSPF

The following example shows how to enable IETF Nonstop Forwarding (NSF) helper support in the router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 500
Device(config-router)# nsf ietf helper strict-lsa-checking
Device(config-router)# nsf cisco helper disable
Device(config-router)# end
```

The following sample output from the **show ip ospf nsf** command shows that NSF is enabled for Open Shortest Path First (OSPF) process 500. NSF helper mode is enabled by default on devices running NSF-compatible software. In this configuration, Cisco helper mode is disabled.

```
Device> show ip ospf nsf

Routing Process "ospf 500"
Non-Stop Forwarding enabled
IETF NSF helper support enabled
Cisco NSF helper support disabled
  OSPF restart state is NO_RESTART
  Handle 1786466333, Router ID 10.1.1.1, checkpoint Router ID 0.0.0.0
  Config wait timer interval 10, timer not running
  Dbase wait timer interval 120, timer not running
```

Additional References for Configuring NSF-OSPF

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Debug commands	• Cisco IOS Debug Command Reference - Commands A through D • Cisco IOS Debug Command Reference - Commands E through H • Cisco IOS Debug Command Reference - Commands I through L • Cisco IOS Debug Command Reference - Commands M through R • Cisco IOS Debug Command Reference - Commands S through Z
High Availability commands	Cisco IOS High Availability Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 3623	*Graceful OSPF Restart*

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 Configuring NSF-OSPF

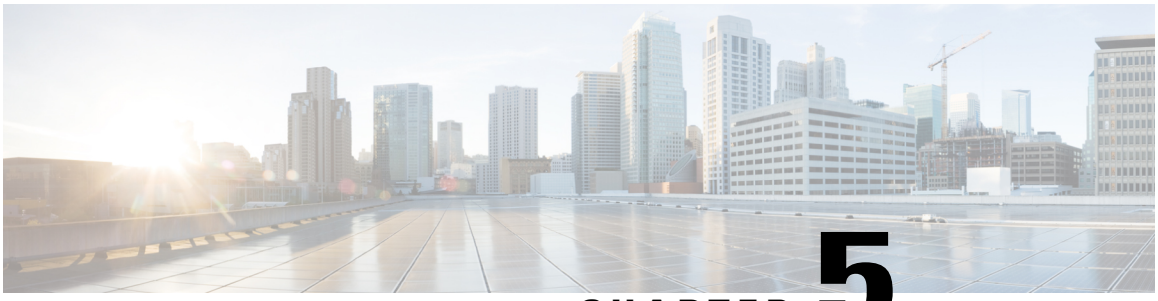
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 . An account on Cisco.com is not required.

Table 15: Feature Information for Configuring NSF-OSPF

Feature Name	Releases	Feature Information
NSF Awareness–OSPF		The Nonstop Forwarding (NSF) Awareness-Open Shortest Path First (OSPF) allows customer premises equipment (CPE) devices to participate in the upstream device's NSF recovery process. The following commands were introduced or modified: **debug ospf nsf**, **nsf (OSPF)**, **nsf cisco**, **nsf ietf**, **show ip ospf neighbor**, **show ip ospf nsf**.

Feature Name	Releases	Feature Information
NSF–OSPF (RFC 3623 OSPF Graceful Restart)		The NSF-OSPFv2 feature was introduced in Cisco software. The feature uses the IETF standardized graceful restart functionality as described in RFC 3623. The following commands were introduced or modified: **nsf cisco**, **nsf ietf**, **nsf (OSPF)**.



CHAPTER 5

Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSes) on a device, you must ensure that the following conditions are met:

- You must assign a DS to the device. Refer to the “Diagnostic Signature Downloading” section for more information on how to assign DSes to devices.

- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Information About Diagnostic Signatures

Diagnostic Signatures Overview

Diagnostic signatures (DS) for the call-home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DSes provides the ability to define more types of events and trigger types to perform the required actions than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify its integrity, reliability, and security.

The structure of a DS file can be one of the following formats:

- Metadata-based simple signature that specifies event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI . The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats mentioned above.

The following basic information is contained in a DS file:

- ID (unique string): unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription): unique description of the DS file that can be used in lists for selection.
- Description: long description about the signature.
- Revision: version number, which increments when the DS content is updated.
- Event & Action: defines the event to be detected and the action to be performed after the event happens.

Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download.

Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Workflow

The Diagnostic Signature feature is enabled by default on the Cisco software. The following is the workflow for using diagnostic signatures:

1. Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
2. The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded.
4. The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.
5. The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature Events and Actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed

after the event happens, such as collecting **show** command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature Event Detection

Event detection in DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and call-home are the supported event types, where "immediate" indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two or more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an evnt occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS file that are used to customize the files.

DS actions are categorized into the following five types:

- call-home
- command
- emailto
- script
- message

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses "diagnostic-signature" as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

DS action type message defines action to generate message to notify or remind user certain important information. The message could be broadcasted to all TTY lines or generated as a syslog entry.

Diagnostic Signature Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment***variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring Call Home Service for Diagnostic Signatures

Configure the call home service feature to set attributes such as the contact email address where notifications regarding diagnostic signature (DS) downloads are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and we recommend using it. If used, you only need to change the destination transport-method to the http setting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service call-home**
4. **call-home**
5. **contact-email-addr** *email-address*
6. **mail-server** {*ipv4-addr* | *ipv6-addr* | *name*} **priority** *number*
7. **profile** *profile-name*
8. **destination transport-method** {**email** | **http**}
9. **destination address** {**email** *address* | **http** *url*}
10. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service call-home** **Example:** `Device(config)# service call-home`	Enables Call-Home service on a device.
Step 4	**call-home** **Example:** `Device(config)# call-home`	Enters Call-Home configuration mode for the configuration of Call-Home settings.
Step 5	**contact-email-addr** *email-address* **Example:** `Device(cfg-call-home)# contact-email-addr userid@example.com`	Assigns an email address to be used for Call-Home customer contact.
Step 6	**mail-server** {*ipv4-addr* | *ipv6-addr* | *name*} **priority** *number* **Example:** `Device(cfg-call-home)# mail-server 10.1.1.1 priority 4`	Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call-Home.

	Command or Action	Purpose
Step 7	**profile** *profile-name* **Example:** `Device(cfg-call-home)# profile user1`	Configures a destination profile for Call-Home and enters Call-Home profile configuration mode.
Step 8	**destination transport-method** {**email** | **http**} **Example:** `Device(cfg-call-home-profile)# destination transport-method http`	Specifies a transport method for a destination profile in the Call-Home.
Step 9	**destination address** {**email** *address* | **http** *url*} **Example:** `Device(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Configures the address type and location to which Call-Home messages are sent. **Note** To configure diagnostic signature, you must use the http option.
Step 10	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}] **Example:** `Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Configures a destination profile to receive messages for the Inventory alert group for Call-Home. • This command is used only for the periodic downloading of DS files.
Step 11	**exit** **Example:** `Device(cfg-call-home-profile)# exit`	Exits Call-Home profile configuration mode and returns to Call-Home configuration mode.

What to Do Next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configuring Diagnostic Signatures

Before You Begin

Configure the Call Home Service feature to set attributes for the Call Home profile as described in the "Configuring Call Home Service for Diagnostic Signatures" section. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

SUMMARY STEPS

1. **call-home**
2. **diagnostic-signature**
3. **profile** *ds-profile-name*
4. **environment ds_** *env-varname ds-env-varvalue*
5. **end**
6. **call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*}
7. **show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **postrequisite** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home** **Example:** `Device(config)# call-home`	Enters call-home configuration mode for the configuration of Call Home settings.
Step 2	**diagnostic-signature** **Example:** `Device(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 3	**profile** *ds-profile-name* **Example:** `Device(cfg-call-home-diag-sign)# profile user1`	Specifies the destination profile on a device that DS uses.
Step 4	**environment ds_** *env-varname ds-env-varvalue* **Example:** `Device(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.
Step 5	**end** **Example:** `Device(cfg-call-home-diag-sign)# end`	Exits call-home diagnostic signature mode and returns to privileged EXEC mode.
Step 6	**call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*} **Example:** `Device# call-home diagnostic-signature download 6030`	Downloads, installs, and uninstalls diagnostic signature files on a device.
Step 7	**show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **postrequisite** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]	Displays the call-home diagnostic signature information.

	Command or Action	Purpose
	Example: `Device# show call-home diagnostic-signature actions`	

Configuration Examples for Diagnostic Signatures

Examples: Configuring Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Device> enable
Device# configure terminal
Device(config)# service call-home
Device(config)# call-home
Device(cfg-call-home)# contact-email-addr userid@example.com
Device(cfg-call-home)# mail-server 10.1.1.1 priority 4
Device(cfg-call-home)# profile user-1
Device(cfg-call-home-profile)# destination transport-method http
Device(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Device(cfg-call-home-profile)# exit
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# profile user1
Device(cfg-call-home-diag-sign)# environment ds_env1 envarval
Device(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

```
Device# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                         Revision Status     Last Update (GMT+00:00)
-------- ------------------------------- -------- ---------- -------------------
6015     CronInterval                    1.0      registered 2013-01-16 04:49:52
6030     ActCH                           1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                     1.0      registered 2013-01-16 06:10:37
6033     PureTCL                         1.0      registered 2013-01-16 06:11:48
```

Additional References for Diagnostic Signatures

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Debug commands	Cisco IOS Debug Command Reference - Commands A through D Cisco IOS Debug Command Reference - Commands E through H Cisco IOS Debug Command Reference - Commands I through L Cisco IOS Debug Command Reference - Commands M through R Cisco IOS Debug Command Reference - Commands S through Z
High Availability commands	Cisco IOS High Availability Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configuring Diagnostic Signatures

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 . An account on Cisco.com is not required.

Table 16: Feature Information for Configuring Diagnostic Signatures

Feature Name	Releases	Feature Information
Diagnostic Signatures		The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks. The following commands were introduced or modified: **active** (diagnostic signature), **call-home diagnostic-signature**, **clear call-home diagnostic-signature statistics**, **debug call-home diagnostic-signature**, **diagnostic-signature**, **environment** (diagnostic signature), **profile** (diagnostic signature), and **show call-home diagnostic-signature**.