Cisco IOS In Service Software Upgrade Process

First Published: March 16, 2006
Last Updated: June 4, 2007

The Cisco IOS In Service Software Upgrade (ISSU) process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.

This document also provides information about Enhanced Fast Software Upgrade (eFSU) concepts. For further information about eFSU, see *Enhanced Fast Software Upgrade on the Cisco 7600 Series Router*, Release 12.2(33)SRB1.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, refer to Table 1.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Feature History for the Cisco IOS ISSU Process

Release	Modification
12.2(28)SB	The ISSU feature was introduced.
12.2(31)SGA	Support for ISSU was introduced on the Cisco Catalyst 4500 series platform. Support for the following new features was added on the Cisco Catalyst 4500 series platform: • Dynamic Host Configuration Protocol (DHCP) snooping • EtherChannel - Port Aggregation Protocol (PagP) and Link Aggregate Control Protocol (LACP) • IEEE 802.1x protocol • IEEE 802.3 • Internet Group Management Protocol (IGMP) snooping • IP Host • Port security • Spanning-Tree Protocol (STP)
12.2(31)SB2	Support for the following new features were added to the 12.2(31)SB2 release: • ISSU - Dynamic Host Configuration Protocol (DHCP) on-demand address pool (ODAP) client/server • ISSU - DHCP proxy client • ISSU - DHCP relay on unnumbered interface • ISSU - DHCP server • ISSU - First Hop Routing Protocol (FHRP) - Gateway Load Balancing Protocol (GLBP) • ISSU - Intermediate System-to-Intermediate System (IS-IS) • ISSU - Quality of Service (QoS)
12.2(33)SRB1	Support for the following new features were added to the 12.2(33)SRB1 release: • ISSU - ARP • ISSU - ATM • ISSU - Frame Relay • ISSU - GLBP • ISSU - HDLC • ISSU - HSRP • ISSU - IS-IS • ISSU - Multitopology routing (MTR) • ISSU - PPP/MLP • ISSU - QoS • ISSU - RIB/VRF • ISSU - SNMP

Contents

Prerequisites for Performing the Cisco IOS ISSU Process

This section describes prerequisites for performing ISSU.

ISSU

- Ensure that both the active and the standby Route Processors (RPs) are available in the system.
- The new and old Cisco IOS 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. If you do not have SSO enabled, see the *Stateful Switchover* document for further information on how to enable and configure SSO.
- Nonstop Forwarding (NSF) must be configured and working properly. If you do not have NSF enabled, see the *Cisco Nonstop Forwarding* document for further information on how to enable and configure SSO.

Restrictions for Performing the Cisco IOS ISSU Process

This section describes restrictions for performing ISSU.

ISSU

General Restrictions

- Before you perform ISSU, ensure the system is configured for redundancy mode SSO and that the file system for both the active and standby RPs contains 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.
- Do not make any hardware changes while performing an ISSU process.

Cisco 10000 Series Internet Router Platform Restrictions

- ISSU is available only in Cisco IOS 12.2(28)SB software released for the and 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

Information About Performing the Cisco IOS ISSU Process

Before you perform ISSU, you should understand the following concepts:

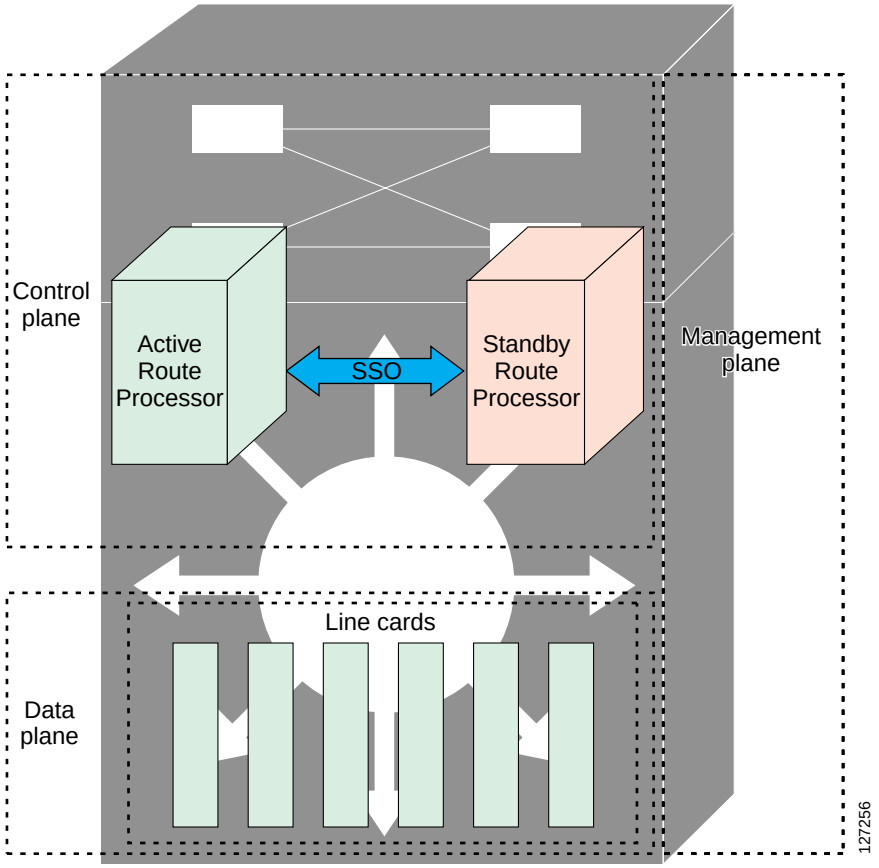
ISSU Process Overview

The ISSU process allows you to perform a Cisco IOS software upgrade or downgrade while the system continues to forward packets. Cisco IOS ISSU takes advantage of the Cisco IOS high availability infrastructure—Cisco NSF with SSO and hardware redundancy—and eliminates downtime associated with software upgrades or version changes by allowing changes while the system remains in service (see

Figure 1). Cisco IOS software 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.

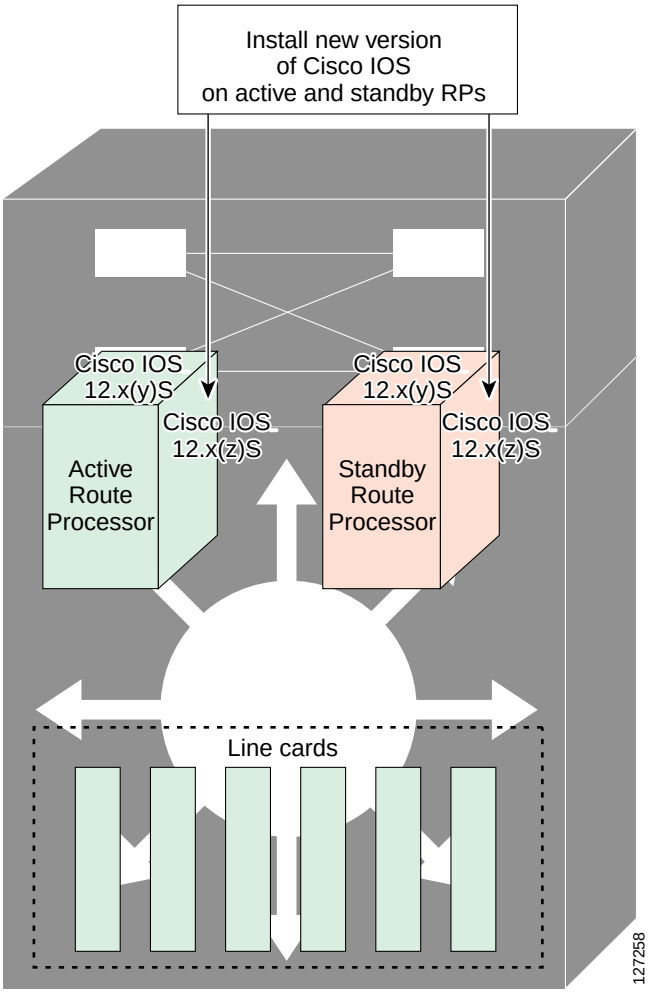
SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two RPs to be kept in synchronization although they may support different sets of commands.

Figure 1 High Availability Features and Hardware Redundancy in the ISSU Process



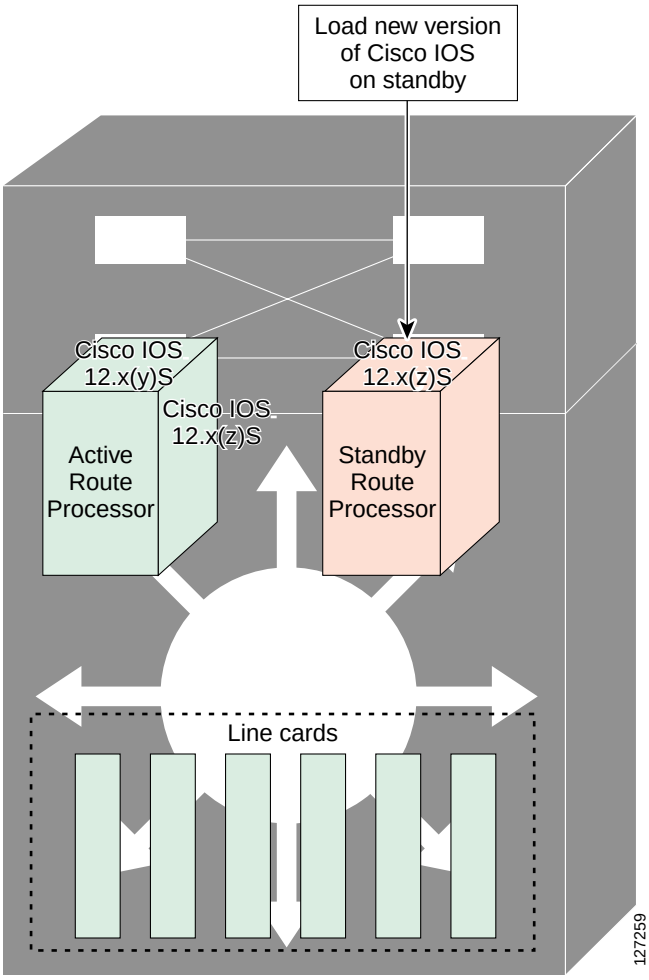
An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, copy the Cisco IOS software into the file systems of both RPs (see Figure 2).

Figure 2 How to Load New Cisco IOS Software on Both RPs



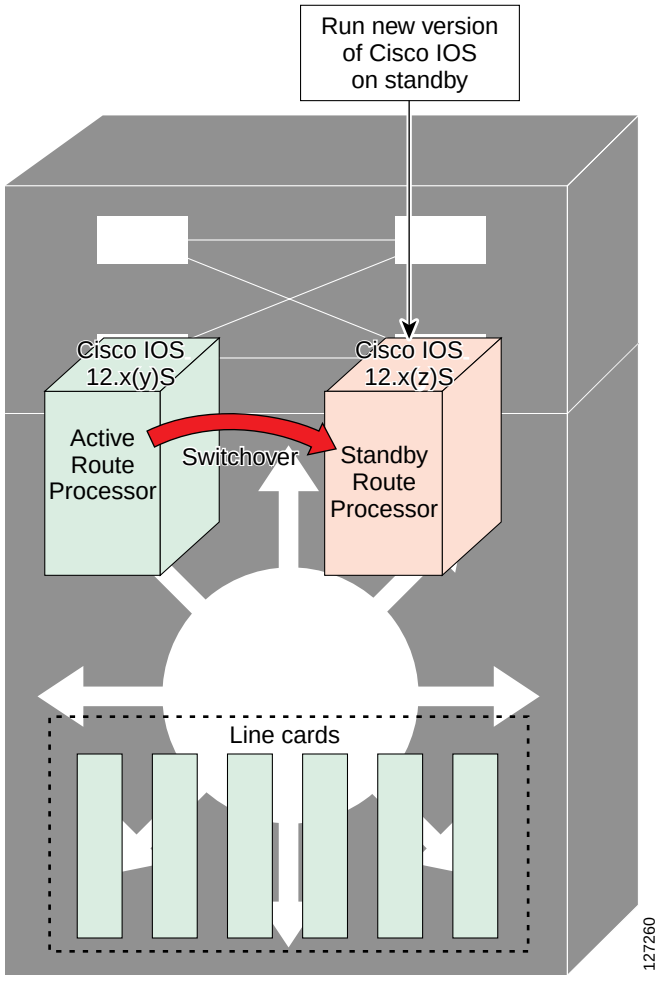
After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP (see Figure 3).

Figure 3 Load New Cisco IOS Software on the Standby RP



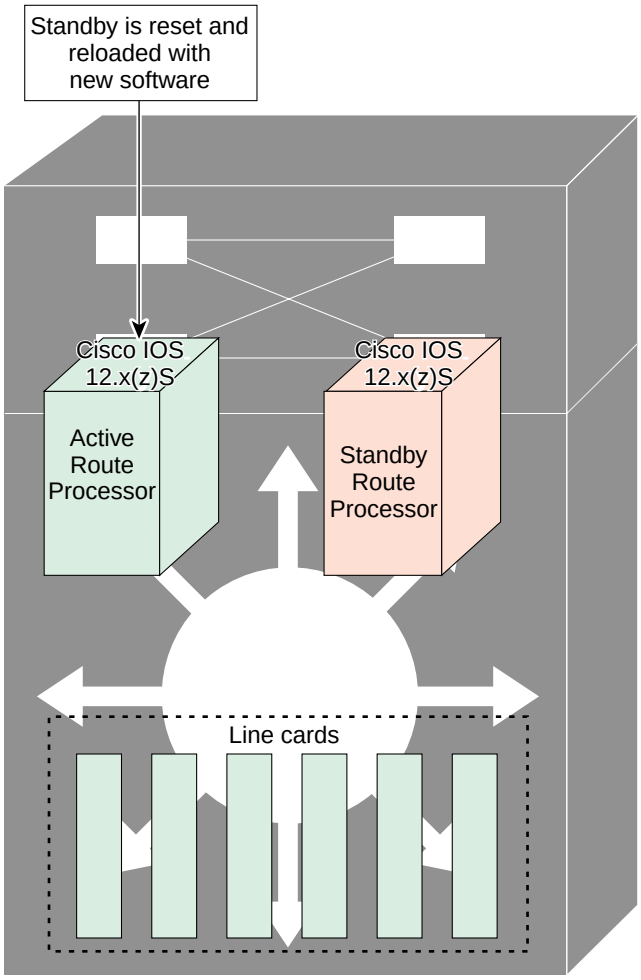
After switchover, the standby RP takes over as the new active RP (see Figure 4).

Figure 4 Switch Over to Standby RP



Then, the former active RP, which is now the new standby RP, is loaded with the new software (see Figure 5).

Figure 5 Load New Standby RP with New Cisco IOS Software

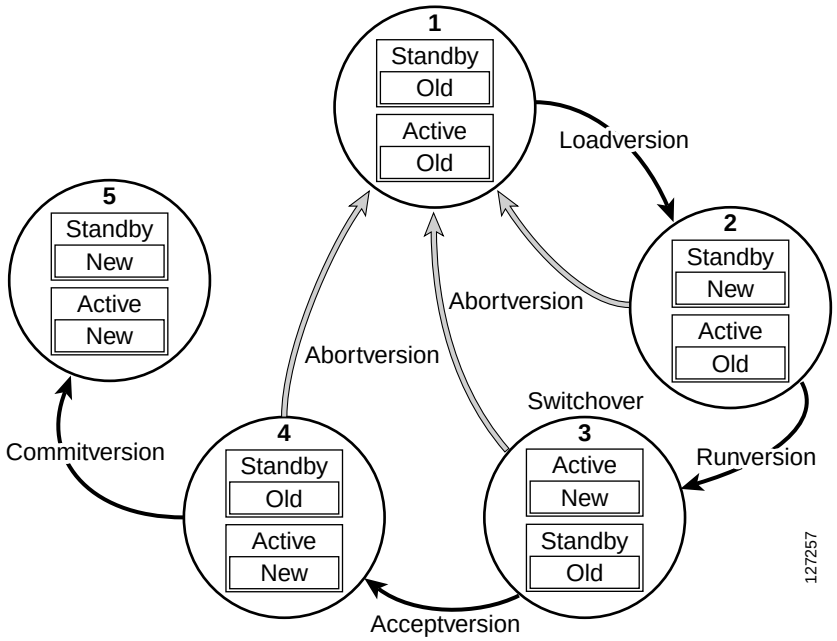


The two RPs in a system can be in one of three different states during ISSU:

- 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.

Figure 6 shows the ISSU states during the ISSU process.

Figure 6 ISSU States During the ISSU Process



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 some 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 IOS software versions. If you want to downgrade to a pre-ISSU version, you must use the manual FSU method.

Enhanced Fast Software Upgrade

eFSU is supported on eFSU is an improvement over FSU, reducing the downtime during an IOS upgrade.

The VIP MDR feature in eFSU allows users to upgrade or downgrade the VIP line cards without resetting them. With MDR, the new Cisco IOS image is downloaded to the VIP cards before the RP switchover. After the switchover, the VIP line cards quickly reinitialize the Cisco IOS software.

Stateful Switchover Overview

Development of the SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability by establishing 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.

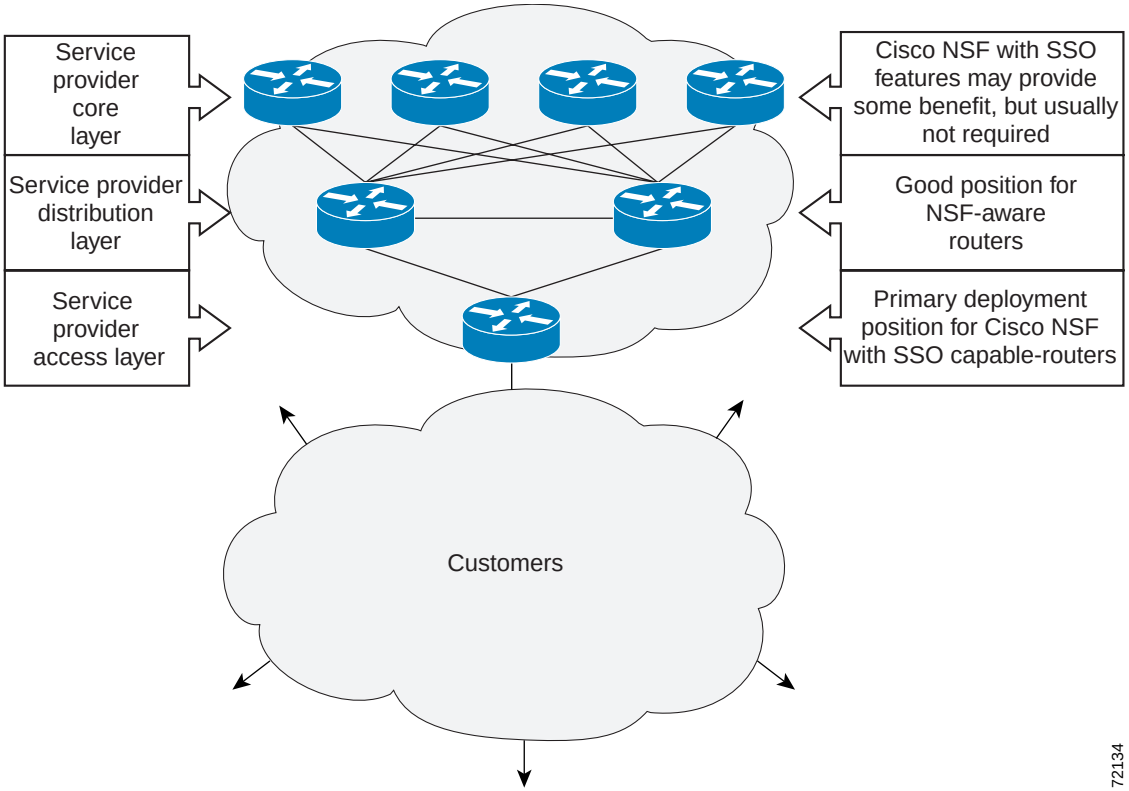
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Cisco NSF is used with SSO. 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.

Figure 7 illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is enabled 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.

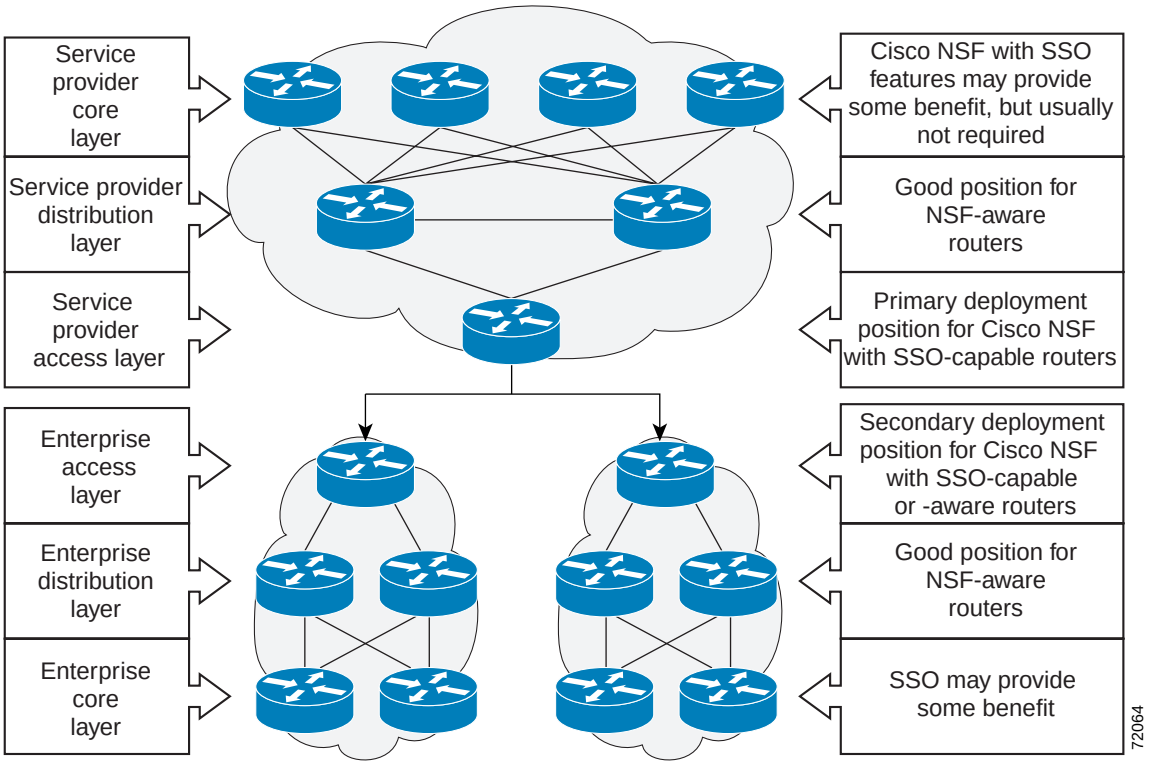
For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Depending on your objectives, you may decide to deploy Cisco NSF and SSO features at the core layer of your network. Doing this can help reduce the time to restore network capacity and service for certain failures, which leads to additional availability.

Figure 7 Cisco NSF with SSO Network Deployment: Service Provider Networks



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. Figure 8 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 8 Cisco NSF with SSO Network Deployment: Enterprise Networks



For further information on SSO, see the *Stateful Switchover* document.

NSF Overview

Cisco NSF works with the SSO feature in Cisco IOS software. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco 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. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

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 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 Cisco NSF operation.

Versioning Capability in Cisco IOS Software to Support ISSU

Before the introduction of the ISSU capability, the SSO mode of operation required each RP to be running like versions of Cisco IOS 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 the 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 IOS 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 IOS infrastructure has been internally modified and redesigned to accommodate subsystem versioning with ISSU. Cisco IOS 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 IOS 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. (For further information on operating modes, see the *Stateful Switchover* document.)

Compatibility Matrix

You can perform the ISSU process when the Cisco IOS 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 IOS 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 IOS software image has with all of the other Cisco IOS 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 IOS software image and on Cisco.com so that users can determine in advance whether an upgrade can be done using the ISSU process.

Before attempting an ISSU, you should determine the compatibility level between the Cisco IOS software versions on the active and the standby RPs. To display the compatibility matrix data between two software versions on a given system, enter the **show issu comp-matrix negotiated** command.

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 IOS 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 IOS releases are the same.

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:

- ISSU - ARP — Address Resolution Protocol (ARP) supports ISSU.
- ISSU - ATM—Asynchronous Transfer Mode (ATM) supports 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 supports ISSU.
- ISSU - DHCP proxy client—The DHCP proxy client feature supports ISSU.
- ISSU - DHCP relay on unnumbered interface—The DHCP relay on unnumbered interface feature supports ISSU.
- ISSU - DHCP server—The DHCP server feature supports ISSU.

- ISSU - DHCP snooping—DHCP snooping supports ISSU.
- ISSU - EtherChannel - PagP LACP—PagP and LACP support ISSU.
- Cisco Express Forwarding—Cisco Express Forwarding (CEF) supports ISSU.
- ISSU - FHRP/GLBP—GLBP supports ISSU.
- ISSU - FHRP/HSRP—The Hot Standby Router Protocol (HSRP) supports ISSU.
- ISSU - Frame Relay—The Frame Relay protocol supports ISSU.
- ISSU - HDLC—The High-Level Data Link Control (HDLC) protocol supports ISSU.
- ISSU - IEEE 802.1x—The IEEE 802.1x protocol supports ISSU.
- ISSU - IEEE 802.3af—IEEE 802.3af supports ISSU.
- ISSU - IGMP snooping—IGMP snooping supports ISSU.
- ISSU - IP Host—The IP host supports ISSU.
- ISSU - IS-IS—IS-IS protocol supports ISSU.
- ISSU - MTR - MTR supports ISSU.
- ISSU - MPLS L3VPN—Multiprotocol Label Switching (MPLS) supports ISSU. For information about upgrading ISSU MPLS-related applications through ISSU, see the *ISSU MPLS Clients* document.
- ISSU - Port Security—Port security supports ISSU.
- ISSU - PPP/MLP—Point-to-Point Protocol (PPP) and multilink PPP (MLP) support ISSU.
- ISSU - QoS support—The Quality of Service (QoS) feature supports ISSU.
- ISSU - Remote File System—The Remote File System (RFS) versioning feature supports ISSU.
- ISSU - SNMP—SNMP supports ISSU.
- ISSU - STP—STP supports ISSU.

How to Perform the Cisco IOS ISSU Process

Unlike SSO, which is a mode of operation for the device and a prerequisite for performing ISSU, the ISSU process is a series of steps performed while the router or switch is in operation. The steps result in the implementation of new or modified Cisco IOS software, and have a minimal impact to traffic.

- Performing the Cisco IOS ISSU Process, page 16

Restrictions for Performing the Cisco IOS ISSU Process

The following list provides basic restrictions for performing the ISSU process:

- Even with ISSU, it is recommended that upgrades be performed during a maintenance window.
- The new features should not be enabled (if they require change of configuration) during the ISSU process.
- In a downgrade scenario, if any feature is not available in the downgrade revision Cisco IOS software image, that feature should be disabled prior to initiating the ISSU process.

Performing the Cisco IOS ISSU Process

The tasks in the following sections explain how to perform the ISSU process:

- Loading Cisco IOS Software on the Standby RP, page 16 (required)
- Switching to the Standby RP, page 17 (required)
- Stopping the ISSU Rollback Timer, page 18 (required)
- Verifying the ISSU Software Installation, page 18 (required)
- Enabling the New Standby RP to Use New Cisco IOS Software Version, page 19
- Aborting a Software Upgrade Using ISSU, page 20 (optional)
- Configuring the Rollback Timer to Safeguard Against Upgrades, page 21 (optional)
- Displaying ISSU Compatibility Matrix Information, page 22 (optional)

Loading Cisco IOS Software on the Standby RP

This task describes how to use ISSU to load Cisco IOS software to the standby RP.

Prerequisites

- Ensure that both the active and the standby RPs are configured in SSO mode. Refer to the *Stateful Switchover* document for more details on how to configure SSO mode on RPs.
- Ensure that the new version of Cisco IOS software image is already loaded in the file system of both the active and standby RPs. Also ensure that appropriate boot parameters are set for the standby RP.
- Optionally, customers may want to perform additional tests and commands to determine the current state of peers and interfaces for later comparison.

SUMMARY STEPS

1. **enable**
2. **issu loadversion** *active-slot active-image standby-slot standby-image* [**force**]
3. **show issu state** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu loadversion** *active-slot active-image standby-slot standby-image* [**force**] **Example:** `Router# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830`	Starts the ISSU process. 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:** `Router# show issu state`	Displays the state of the during the ISSU process. At this point in the ISSU process, use this command to check that the standby RP is loaded and is in SSO mode. It may take several seconds after entering the **issu loadversion** command for Cisco IOS software to load onto the standby RP and the standby RP to transition to SSO mode. If you enter the **show issu state** command too soon, you may not see the information you need.

Switching to the Standby RP

This task describes how to switch to the standby RP, which is running the new Cisco IOS software image.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu runversion** *slot image* **Example:** `Router# 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.

Stopping the ISSU Rollback Timer

The following task describes how to stop the rollback timer. If the rollback timer is not stopped, the system automatically aborts the ISSU process and reverts to the original Cisco IOS software version if the next ISSU procedure is not performed prior to the rollback timer timeout. For example, the ISSU process would abort after the **issu acceptversion** command was entered only if the **issu runversion** command was not entered before rollback timeout.

SUMMARY STEPS

1. **enable**
2. **issu acceptversion** {*active slot-number* | **active slot-name** *slot-name*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu acceptversion** {*active slot-number* | **active slot-name** *slot-name*} **Example:** `Router# 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.

Verifying the ISSU Software Installation

During the ISSU process, there are three valid states: init, load version, and run version. Use the **show issu state** command to get information on each or all of these states:

- Init state—The initial state is two RPs, one active and one standby, before the ISSU process is started.
- Load version (LV) state—The standby RP is loaded with the new version of Cisco IOS software.

- Run version (RV) state—The **issu runversion** command forces the switchover of the RPs. The newly active RP now runs the new Cisco IOS software image.

You can verify the ISSU software installation by entering **show** commands that provide information on the state of the during the ISSU process.

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:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show issu state [detail]`
	
	Example:
	`Router# show issu state`
		Displays the state of the during the ISSU process.

Step 3	`show redundancy [clients | counters | debug-log | handover | history | states | inter-device]`
	
	Example:
	`Router# show redundancy`
		Displays current or historical status, mode, and related redundancy information about the device.

Enabling the New Standby RP to Use New Cisco IOS Software Version

After loading new Cisco IOS software to the standby RP, causing the standby RP to become the active RP and the former active RP to become the standby RP, you need to enable the new standby RP to use the new Cisco IOS software version. This task explains how to perform that process.

SUMMARY STEPS

1. **enable**
2. **issu commitversion** *slot active-image*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu commitversion** *slot active-image* **Example:** `Router# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830`	Allows the new Cisco IOS software image to be loaded into the standby RP.

Aborting a Software Upgrade Using ISSU

You can abort the ISSU process at any stage manually by issuing the **issu abortversion** command. The ISSU process also aborts on its own if the software detects a failure.

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

If the process is aborted after either the **issu runversion** or **issu acceptversion** command is entered, then 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.

This task describes how to abort the ISSU process before a user has committed to the process by issuing the **issu commitversion** command.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu abortversion** *slot image* **Example:** `Router# issu abortversion b disk0:c10k2-p11-mz.2.20040830`	Cancels 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

The 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.

A user may want to configure the rollback timer to fewer than 45 minutes (the default) so that the user need not wait in case the new software is not committed or the connection to the router was lost while it was in runversion mode. A user may want to 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.

Once you are satisfied that the ISSU process has been successful and you want to remain in the current state, you must indicate acceptance by issuing the **issu acceptversion** command, which stops the rollback timer. Therefore, entering the **issu acceptversion** command is extremely important to moving the ISSU process forward.

Issuing the **issu commitversion** command at this stage is equal to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for a period of time and are satisfied with the new software version.

This task explains how to configure the rollback timer.

SUMMARY STEPS

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

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	**configure issu set rollback timer** *seconds* **Example:** `Router(config)# configure issu set rollback timer 3600`	Configures the rollback timer value.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns the user to privileged EXEC mode.
Step 5	**show issu rollback timer** **Example:** `Router# show issu rollback timer`	Displays the current setting of the ISSU rollback timer.

Displaying ISSU Compatibility Matrix Information

The ISSU compatibility matrix contains information about other software images about the version in question. This compatibility matrix represents the compatibility of the two software versions, one running on the active and the other on the standby RP, and the matrix allows the system to determine the highest operating mode it can achieve. This information helps the user identify whether or not to use ISSU.

This task explains how to display information about the ISSU compatibility matrix.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show issu comp-matrix {negotiated | stored}`
	
	Example:
	`Router# show issu comp-matrix`
		Displays information regarding the ISSU compatibility matrix.

Configuration Examples for Performing ISSU

This section contains the following configuration examples:

Verifying Redundancy Mode Before Beginning the ISSU Process: Example

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 IOS software image.

```
Router# 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

Router# 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
```

Verifying the ISSU State: Example

The following example displays and verifies the ISSU state:

```
Router# 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 (or RPs) shows that the new version is present.

```
Router# 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)

Router# directory stby-disk0:

Directory of stby-disk0:/

    1  -rw-    16864340  Jul 16 2004 09:00:26 -04:00  c10k2-p11-mz.122-16.BX1.bin
    2  -rw-     2530912  Jul 16 2004 09:00:46 -04:00  c10k2-eboot-mz.122-16.BX1.bin
    3  -rw-    20172208  Aug 30 2004 16:28:44 -04:00  c10k2-p11-mz.1.20040830
    4  -rw-    20171492  Aug 31 2004 12:30:20 -04:00  c10k2-p11-mz.2.20040830

64253952 bytes total (4509696 bytes free)
```

Performing the ISSU Process: Example

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

Initiating the ISSU Process: Example

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

```
Router# 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:

```
Router# 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;

Router# 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: Example

At this point, the system is ready to switch over and run the new version of Cisco IOS 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.

```
Router# 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.

```
Router# 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

Router# 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;

Router# 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: Example

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 IOS software by switching to the standby RP.

```
Router# 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:

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

Committing the New Software to the Standby RP: Example

The following example shows how to commit the new Cisco IOS 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 IOS software and returned to STANDBY-HOT status.

```
Router# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830

Router# 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

Router# 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


Router# 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;

Router# 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 IOS software version upgrade or downgrade will require that a new ISSU process be invoked.

Aborting the ISSU Process: Example

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

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

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

Verifying Rollback Timer Information: Example

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

```
Router# show issu rollback-timer

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

Additional References

The following sections provide references related to the Cisco IOS ISSU features.

Related Documents

Related Topic	Document Title
Performing ISSU	*Cisco IOS Software: Guide to Performing In Service Software Upgrades*
Information about eFSU on Cisco 7600 series routers	*Enhanced Fast Software Upgrade on the Cisco 7600 Series Router*, Release 12.2(33)SRB1
Cisco nonstop forwarding	*Cisco Nonstop Forwarding*
Stateful switchover	*Stateful Switchover*
ISSU and MPLS clients	*ISSU MPLS Clients*
MTR	*Multi-Topology Routing*, Release 12.2(33)SRB1
High availability commands	*Cisco IOS High Availability Command Reference*, Release 12.2 SR

Standards

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

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

ISSU commands are documented in the *Cisco IOS High Availability Command Reference*, Release 12.2SR.