



Cisco IOS In Service Software Upgrade Process

The 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.

Feature History for ISSU

Release	Modification
12.2(28)SB	This feature was introduced.



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

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:
	<ul style="list-style-type: none"> • 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:
	<ul style="list-style-type: none"> • 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)

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Performing ISSU, page 3](#)
- [Restrictions for Performing ISSU, page 3](#)
- [Information About Performing ISSU, page 4](#)
- [How to Perform the ISSU Process, page 15](#)
- [Configuration Examples for Performing ISSU, page 23](#)
- [Additional References, page 30](#)
- [Command Reference, page 31](#)

Prerequisites for Performing 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 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)
 - 1-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 ISSU

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

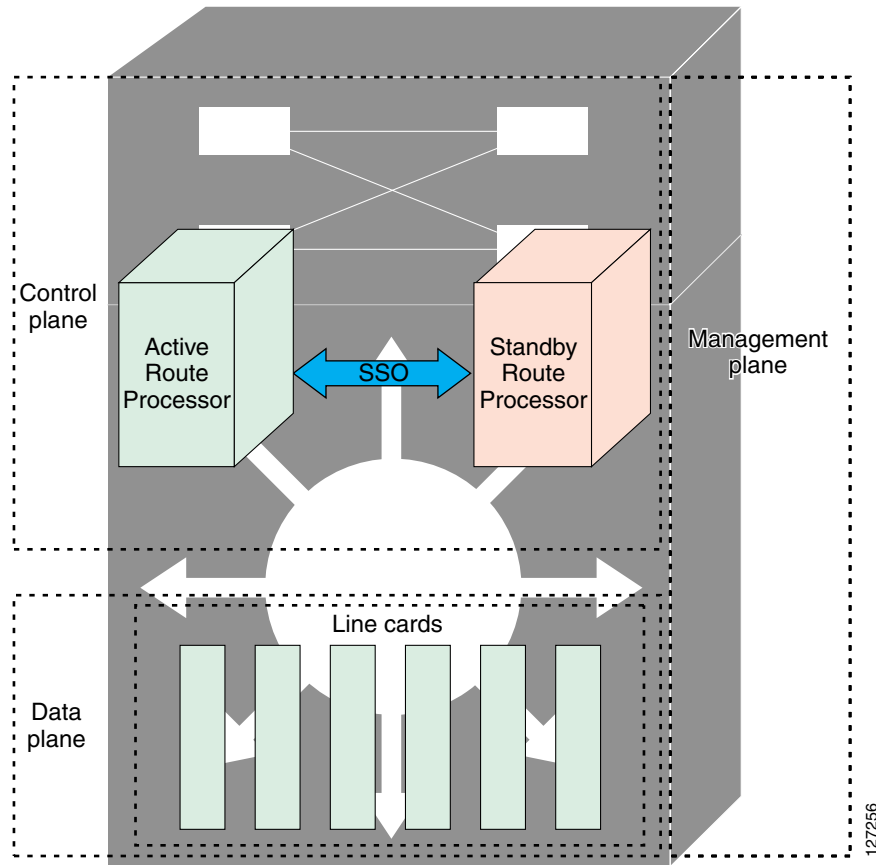
- [ISSU Process Overview, page 4](#)
- [Stateful Switchover Overview, page 10](#)
- [NSF Overview, page 12](#)
- [Versioning Capability in Cisco IOS Software to Support ISSU, page 13](#)
- [ISSU-Capable Protocols and Applications, page 14](#)
- [SNMP Support for ISSU, page 15](#)
- [Compatibility Verification Using Cisco Feature Navigator, page 15](#)

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.

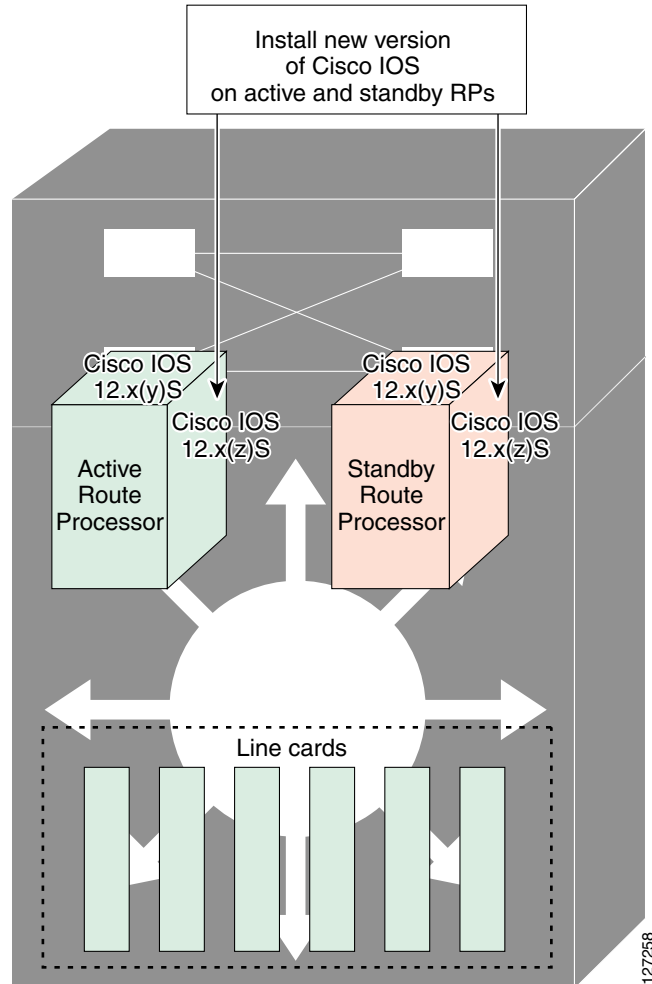
SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two RPs to be kept in synchronization although they may support different sets of commands.

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



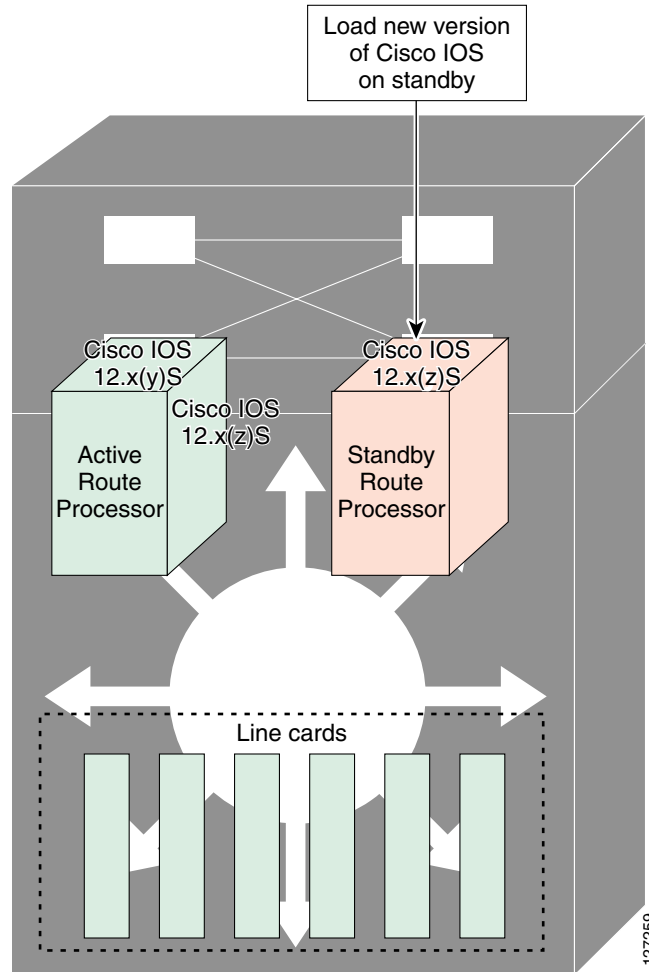
An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, copy the Cisco IOS software into the file systems of both RPs (see [Figure 2](#)).

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



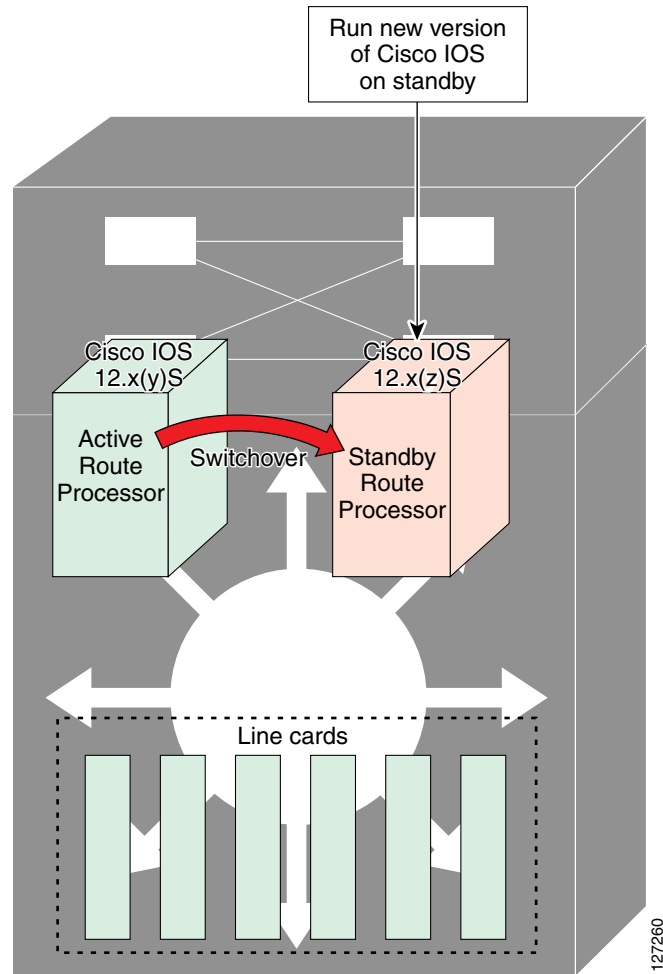
After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP (see [Figure 3](#)).

Figure 3 Load New Cisco IOS Software on the Standby RP



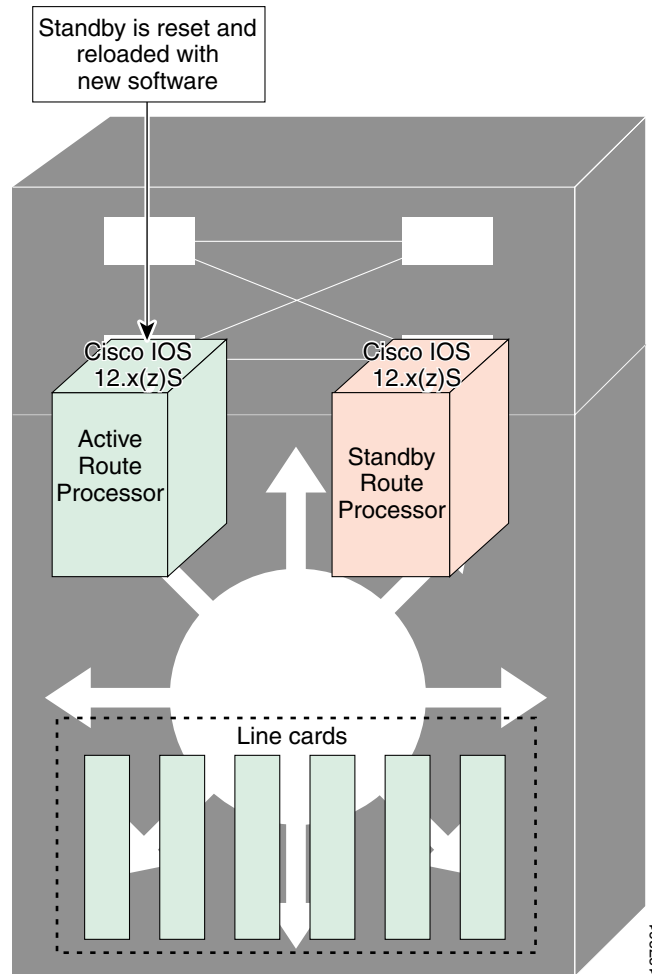
After switchover, the standby RP takes over as the new active RP (see [Figure 4](#)).

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

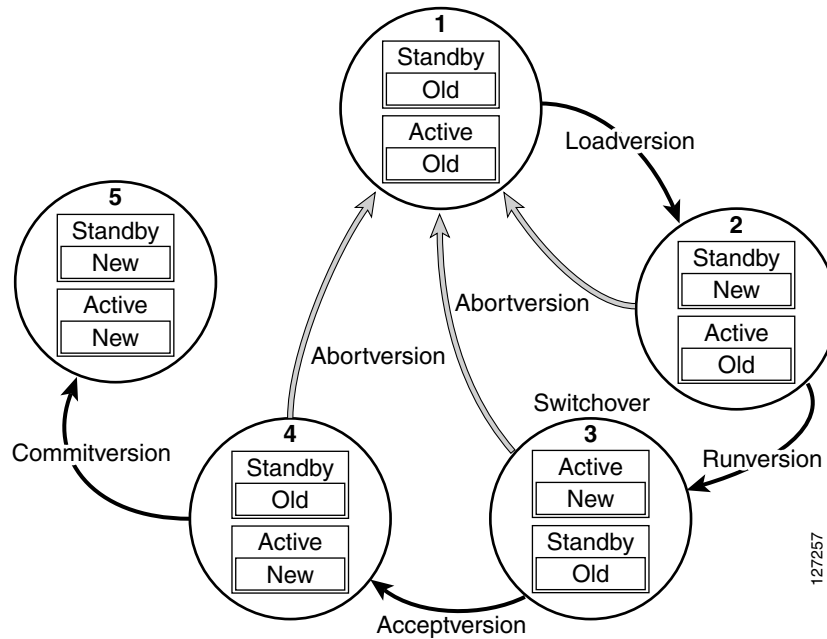


The two RPs in a system can be in one of three different states during ISSU:

- 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



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.

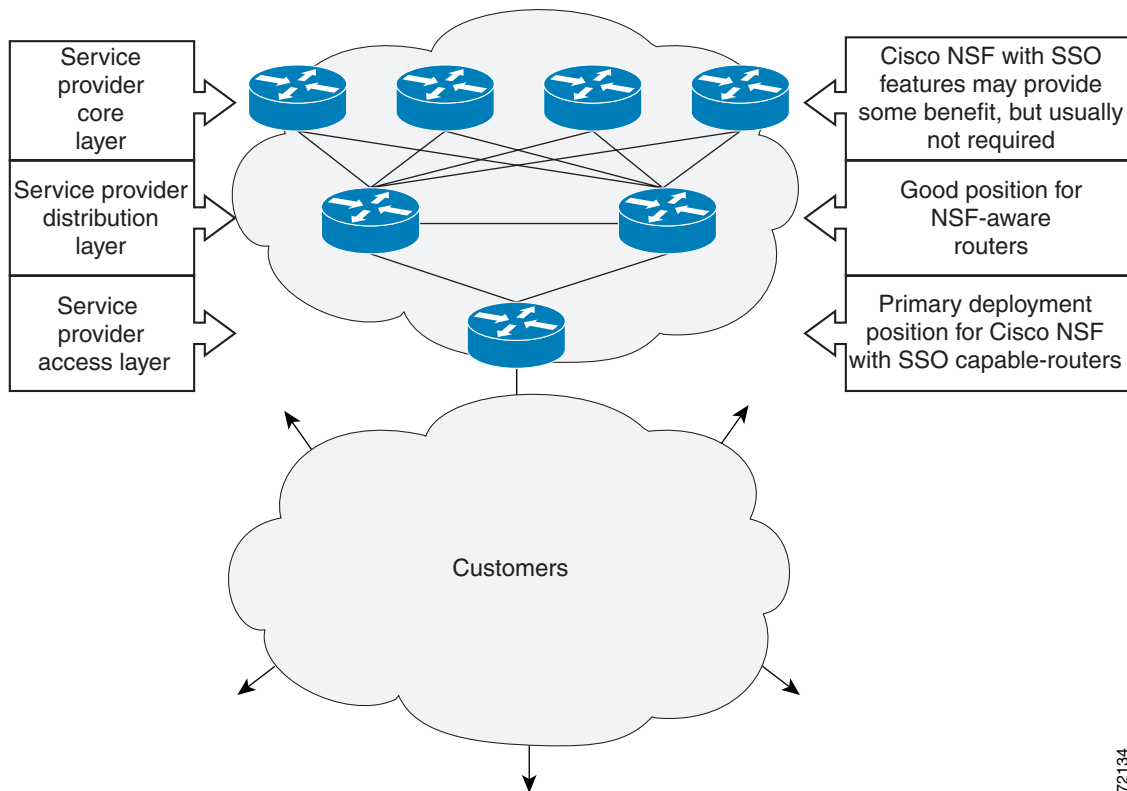
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

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.

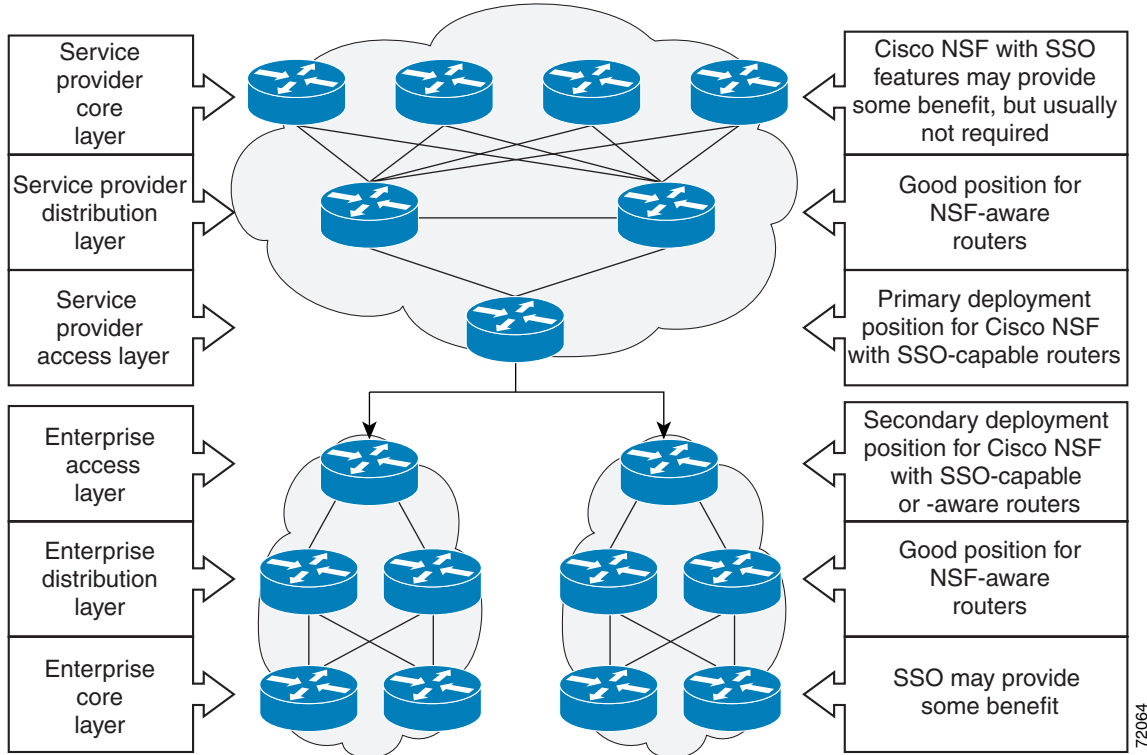
Figure 7 Cisco NSF with SSO Network Deployment: Service Provider Networks



72134

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.

ISSU-Capable Protocols and Applications

The following protocols and applications support ISSU:

- ISSU - ARP—ARP supports ISSU.
- ISSU - ATM—The ATM application 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—The Gateway Load Balancing Protocol (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 - 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—The PPP and multilink PPP (MLP) protocols 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

SNMP Support for ISSU

ISSU - SNMP for SSO provides a mechanism for synchronizing the 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

How to Perform the 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.

Restrictions for Performing the 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.

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)
- [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	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>issu loadversion <i>active-slot active-image standby-slot standby-image</i> [force]</p> <p>Example: Router# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830</p>	<p>Starts the ISSU process.</p> <p>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.</p>
Step 3	<p>show issu state [detail]</p> <p>Example: Router# show issu state</p>	<p>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.</p> <p>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.</p>

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

- enable**
- issu runversion** *slot image*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	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

- enable**
- 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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	issu acceptversion { <i>active slot-number</i> active slot-name <i>slot-name</i> }	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
	Example: Router# issu acceptversion b disk0:c10k2-p11-mz.2.20040830	

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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> 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

- enable**
- issu abortversion slot image**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	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. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	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

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show 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, page 23](#)
- [Verifying the ISSU State: Example, page 24](#)
- [Performing the ISSU Process: Example, page 25](#)
- [Aborting the ISSU Process: Example, page 29](#)
- [Verifying Rollback Timer Information: Example, page 30](#)

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 performing ISSU.

Related Documents

Related Topic	Document Title
Performing ISSU	<i>Cisco IOS Software: Guide to Performing In Service Software Upgrades</i>
Information about Cisco Nonstop Forwarding	<i>Cisco Nonstop Forwarding</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fsnsf20s.htm
Information about stateful switchover	<i>Stateful Switchover</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fssso20s.htm
ISSU and MPLS clients	<i>ISSU MPLS Clients</i>

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
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands.

- [configure issu set rollback timer](#), page 32
- [issu abortversion](#), page 33
- [issu acceptversion](#), page 35
- [issu commitversion](#), page 37
- [issu loadversion](#), page 39
- [issu runversion](#), page 41
- [show issu comp-matrix](#), page 42
- [show issu state](#), page 43
- [show redundancy](#), page 45

configure issu set rollback timer

To configure the rollback timer value, use the **configure issu set rollback timer** command in global configuration mode.

configure issu set rollback timer *seconds*

Syntax Description	<i>seconds</i>	The rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (two hours). A value of 0 seconds disables the rollback timer.
---------------------------	----------------	--

Defaults	Rollback timer value is 45 minutes.
-----------------	-------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines	Use the configure issue set rollback timer command to configure the rollback timer value. Note that you can enable this command only when the Route Processors (RPs) are in the init state.
-------------------------	--

Examples	The following example sets the rollback timer value to 3600 seconds, or 1 hour:
-----------------	---

```
configure issu set rollback timer 3600
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
	show issu rollback timer	Displays the current setting of the ISSU rollback timer.

issu abortversion

To cancel the In Service Software Upgrade (ISSU) upgrade or downgrade process in progress and restore the router to its state before the process had started, use the **issu abortversion** command in user EXEC or privileged EXEC mode.

issu abortversion *slot image*

Syntax Description	slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
	<i>image</i>	The new image to be loaded into the standby .

Defaults This command is disabled by default.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines The **issu abortversion** command allows the user to stop the ISSU process at any time before the user commits to completing the process by issuing the **issu commitversion** command. Before any action is taken, a check is performed to ensure that both RPs are either in the run version (RV) or load version (LV) state.

When the **issu abortversion** command is issued before the **issu runversion** command, the standby RP is reset and reloaded. When the **issu abortversion** command is issued after the **issu runversion** command, the network switches to the former Cisco IOS software version.

Examples In the following example, the **issu abortversion** command resets and reloads the standby RP:

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

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
	issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
	issu loadversion	Starts the ISSU process.

Command	Description
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of the during the ISSU process.

issu acceptversion

To halt the rollback timer and ensure the new Cisco IOS software image is not automatically aborted during the In Service Software Upgrade (ISSU) process, use the **issu acceptversion** command in user EXEC or privileged EXEC mode.

issu acceptversion { *active slot-number* | **active slot-name** *slot-name* }

Syntax Description

<i>active slot-number</i>	The specified active slot on your networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
active slot-name <i>slot-name</i>	Identifies a specific slot name.

Defaults

45 minutes from the time the **issu runversion** command is issued to the time the **issu acceptversion** is issued.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines

Use the **issu acceptversion** command to ensure that the active Route Processor (RP) is running the new image, that the standby RP is running the old image, and that both RPs are in the run version (RV) state. If the **issu acceptversion** command is not issued within 45 minutes from the time the **issu runversion** command is issued, the new active RP is assumed to be unreachable, and the entire ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after the user issues the **issu runversion** command.

If the rollback timer is set for a short period of time, such as 1 minute, and the standby RP is not yet in a hot standby state, you then have 15 1-minute extensions during which the router will wait for the standby state to become hot standby state. However, if the standby state becomes hot standby state within the 15-minute extension, the router will abort the ISSU process because the 1-minute rollback timer has expired. Therefore, it is not recommended to set the rollback timer shorter than the time required for the standby state to become hot standby state.

If the rollback timer is set to a long period of time, such as the default of 45 minutes, and the standby RP goes into the hot standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll back if necessary.

Use the **configure issu set rollback timer** to configure the 45-minute default value on the rollback timer.

■ **issu acceptversion****Examples**

The following example halts the rollback timer and allows the ISSU process to continue:

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

Related Commands

Command	Description
configure issu set rollback timer	Configures the rollback timer value.
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu commitversion

To allow the new Cisco IOS software image to be loaded into the standby RP, use the **issu commitversion** command in user EXEC or privileged EXEC mode.

issu commitversion *slot active-image*

Syntax Description

<i>slot</i>	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
<i>active-image</i>	The new image to be loaded into the active networking device.

Defaults

This command is disabled by default.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines

The **issu commitversion** command verifies that the standby Route Processor (RP) has the new Cisco IOS software image in its file system and that both RPs are in the run version (RV) state. If these conditions are met, then the following actions take place:

- The standby RP is reset and booted with the new version of Cisco IOS software.
- If both images are compatible, the standby RP moves into the stateful switchover (SSO) mode and is fully stateful for all clients and applications with which the standby RP is compatible.
- If both images are not compatible, the standby RP moves into Route Processor Redundancy Plus (RPR+) mode or RPR mode.
- If all conditions are correct, the RPs are moved into final state, which is the same as initial state.

Issuing the **issu commitversion** command completes the In Service Software Upgrade (ISSU) process. This process cannot be stopped or reverted to its original state without starting a new ISSU process.

Issuing the **issu commitversion** command at this stage is equivalent 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.

Examples

The following example causes the standby RP to be reset and reloaded with the new Cisco IOS software version:

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

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
	issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
	show issu state	Displays the state and current version of the RPs during the ISSU process.

issu loadversion

To start the In Service Software Upgrade (ISSU) process, use the **issu loadversion** command in user EXEC or privileged EXEC mode.

issu loadversion *active-slot active-image standby-slot standby-image* [**force**]

Syntax Description		
	<i>active-slot</i>	The active slot on the networking device.
	<i>active-image</i>	The active image on the networking device.
	<i>standby-slot</i>	The standby slot on the networking device.
	<i>standby-image</i>	The new image to be loaded into the standby networking device.
	force	(Optional) Used to override the automatic rollback when the new Cisco IOS software version is detected to be incompatible, which is the case when as user intends to perform a fast software upgrade (FSU) in Route Processor Redundancy (RPR) mode.

Defaults This command is disabled by default.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines Enabling the **issu loadversion** command causes the standby Route Processor (RP) to be reset and booted with the new Cisco IOS software image specified by the command. If both the active and standby RP images are ISSU-capable, ISSU-compatible, and have no configuration mismatches, then the standby RP moves into stateful switchover (SSO) mode, and both RPs move into the load version (LV) state. It may take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load into the standby RP and the standby RP to transition to SSO mode.

Examples The following example initiates the ISSU process by loading the active image into the active RP slot and loading the standby image into the standby RP slot:

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

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
	issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
	issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
	issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
	show issu state	Displays the state and current version of the RPs during the ISSU process.

issu runversion

To force a switchover from the active Route Processor (RP) to the standby RP and cause the newly active RP to run the new image specified in the **issu loadversion** command, use the **issu runversion** command in user EXEC or privileged EXEC mode.

issu runversion *slot image*

Syntax Description

<i>slot</i>	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
<i>image</i>	The new image to be loaded into the standby RP.

Defaults

This command is disabled by default.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines

When a user enables the **issu runversion** command, a switchover is performed, and the standby RP is booted with the old image version following the reset caused by the switchover. As soon as the standby RP moves into the standby state, the rollback timer is started.

Examples

In the following example, the **issu runversion** command is used to switch to the redundant RP with the new Cisco IOS software image:

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

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Commits the new Cisco IOS software image in the file system of the standby RP and ensures that both the active and standby RPs are in the RV state.
issu loadversion	Starts the ISSU process.
show issu state	Displays the state and current version of the RPs during the ISSU process.

show issu comp-matrix

To display information regarding the In Service Software Upgrade (ISSU) compatibility matrix, use the **show issu comp-matrix** command in user EXEC or privileged EXEC mode.

```
show issu comp-matrix { negotiated | stored }
```

Syntax Description

negotiated	Displays negotiated matrix information.
stored	Displays stored matrix information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines

Before attempting an ISSU, you should know the compatibility level between the Cisco IOS software versions on the active and the standby Route Processors (RPs). ISSU will not work if the two versions are incompatible. Use the **show issu comp-matrix** command with the **negotiated** keyword to display information on the negotiation of the compatibility matrix data between two software versions on a given system.

Compatibility matrix data is stored with each Cisco IOS software image that supports the ISSU capability. Use the **show issu comp-matrix** command with the **stored** keyword to display stored compatibility matrix information.

Examples

The following example displays stored compatibility matrix information:

```
Router# show issu comp-matrix stored
```

show issu state

To display the state and current version of the Route Processors (RPs) during the In Service Software Upgrade (ISSU) process, use the **show issu state** command in user EXEC or privileged EXEC mode.

show issu state [detail]

Syntax Description	detail	(Optional) Provides detailed information about the state of the active and standby RPs.
--------------------	--------	---

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines	Use the show issu state command to display the state and current version of each RP. It may take several seconds after the issu loadversion command is entered for Cisco IOS software to load onto the standby RP and the standby RP to transition to stateful switchover (SSO) mode. If you enter the show issu state command too soon, you may not see the information you need.
------------------	--

Examples	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
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.

show redundancy

To display current or historical status and related information on planned or logged handovers, use the **show redundancy** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode

```
show redundancy [clients | counters | debug-log | handover | history | switchover history |
states | inter-device]
```

User EXEC Mode

```
show redundancy {clients | counters | history | states | switchover}
```

Syntax	Description
clients	Displays the redundancy-aware client-application list.
counters	Displays redundancy-related operational measurements.
debug-log	(Optional) Displays up to 256 redundancy-related debug entries.
handover	(Optional) Displays details of any pending scheduled handover.
history	Displays past status and related information about logged handovers. This is the only keyword supported on the Cisco AS5800.
switchover history	Displays redundancy switchover history.
states	Displays redundancy-related states: disabled, initialization, standby, active (various substates for the latter two).
switchover	Displays the switchover counts, the uptime since active, and the total system uptime.
inter-device	(Optional) Displays redundancy interdevice operational state and statistics.

Command Modes
User EXEC Privileged EXEC

Command History	Release	Modification
	11.3(6)AA	This command was introduced in privileged EXEC mode.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5800 and Cisco AS5850 is not included in this release.
	12.2(8)MC2	This command was introduced in user EXEC mode.
	12.2(11)T	The privileged EXEC mode form of this command was implemented on the Cisco AS5800 and Cisco AS5850.
	12.2(14)SX	The user EXEC mode form of this command was introduced on the Supervisor Engine 720.
	12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
	12.2(20)S	The states , counters , clients , history , and switchover history keywords were added.

Release	Modification
12.2(17d)SXB	Support for the user EXEC mode form of this command was extended to the Supervisor Engine 2.
12.3(8)T	The inter-device keyword was added to the privileged EXEC form of the command.
12.3(11)T	The user EXEC form of this command was integrated into Cisco IOS Release 12.3(11)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.

Usage Guidelines

Cisco AS5800

Use this command from the router-shelf console to determine when failover is enabled. Use this command with the **history** keyword to log failover events.

Cisco AS5850

To use this command, the router must have two route-switch-controller (RSC) cards installed and must be connected to one of them.

Examples

The following example shows how to display information about the RF client:

```
Router# show redundancy clients

clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 25     clientSeq = 130    CHKPT RF
clientID = 5026   clientSeq = 130    CHKPT RF
clientID = 5029   clientSeq = 135    Redundancy Mode RF
clientID = 5006   clientSeq = 170    RFS client
clientID = 6      clientSeq = 180    Const OIR Client
clientID = 7      clientSeq = 190    PF Client
clientID = 5008   clientSeq = 190    PF Client
clientID = 28     clientSeq = 330    Const Startup Config
clientID = 29     clientSeq = 340    Const IDPROM Client
clientID = 65000  clientSeq = 65000  RF_LAST_CLIENT
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current RF state.

The following example shows how to display information about the RF counters:

```
Router# show redundancy counters

Redundancy Facility OMs
  comm link up = 0
  comm link down down = 0

  invalid client tx = 0
  null tx by client = 0
  tx failures = 0
  tx msg length invalid = 0
```

```

    client not rxing msgs = 0
  rx peer msg routing errors = 0
    null peer msg rx = 0
    errored peer msg rx = 0

    buffers tx = 0
  tx buffers unavailable = 0
    buffers rx = 0
  buffer release errors = 0

duplicate client registers = 0
failed to register client = 0
  Invalid client syncs = 0

```

The following example shows information about the RF history:

```

Router# show redundancy history

00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:02 client added: Const Startup Config Sync Clie(28) seq=330
00:00:02 client added: CHKPT RF(25) seq=130
00:00:02 client added: PF Client(7) seq=190
00:00:02 client added: Const OIR Client(6) seq=180
00:00:02 client added: Const IDPROM Client(29) seq=340
00:00:02 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:02 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) CHKPT RF(25) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) Const OIR Client(6) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) PF Client(7) op=0 rc=11

```

The following example shows information about the RF state:

```

Router# show redundancy states

    my state = 13 -ACTIVE
    peer state = 1 -DISABLED
      Mode = Simplex
      Unit = Primary
      Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured) = Route Processor Redundancy
  Split Mode = Disabled
  Manual Swact = Disabled Reason: Simplex mode
  Communications = Down Reason: Simplex mode

  client count = 11
  client_notification_TMR = 30000 milliseconds
    keep_alive TMR = 4000 milliseconds
    keep_alive count = 0
    keep_alive threshold = 7
    RF debug mask = 0x0

```

If you enter the **show redundancy states** command with stateful switchover (SSO) configured, the Redundancy Mode (Operational) and the Redundancy Mode (Configured) fields display stateful switchover.

The following example shows how to display the switchover counts, the uptime since active, and the total system uptime:

```

Router> show redundancy switchover

```

```

Switchovers this system has experienced      : 1
Uptime since this supervisor switched to active : 1 minute
Total system uptime from reload              : 2 hours, 47 minutes

```

Cisco AS5850 Example

The following is sample output from the **show redundancy handover** and **show redundancy states** commands on a Cisco AS5850:

```
Router# show redundancy handover
```

```

No busyout period specified
Handover pending at 23:00:00 PDT Wed May 9 2001

```

```
Router# show redundancy states
```

```

my state = 14 -ACTIVE_EXTRALOAD
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit = Preferred Primary
Unit ID = 6
Redundancy Mode = Handover-split: If one RSC fails, the peer RSC will take over the
feature boards
Maintenance Mode = Disabled
Manual Swact = Disabled Reason: Progression in progress
Communications = Up
client count = 3
client_notification_TMR = 30000 milliseconds
keep_alive TMR = 4000 milliseconds
keep_alive count = 1
keep_alive threshold = 7
RF debug mask = 0x0

```

Cisco AS5800 Example

The following is sample output from the **show redundancy** command on a Cisco AS5800:

```
Router# show redundancy
```

```

DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.

```

Cisco AS5800 with History Example

The following is sample output from the **show redundancy history** command on a Cisco AS5800:

```
Router# show redundancy history
```

```

DSC Redundancy Status Change History:

981130 18:56 Slot 12 DSC: Hub, becoming active - RS instruction
981130 19:03 Slot 12 DSC: Hub, becoming active - D13 order

```

Cisco AS5800 Router Shelves as Failover Pair Example

The following is sample output from two Cisco AS5800 router shelves configured as a failover pair. The active router shelf is initially RouterA. The **show redundancy history** and **show redundancy** commands have been issued. The **show redundancy** command shows that failover is enabled, shows the configured group number, and shows that this router shelf is the active one of the pair. Compare this output with that from the backup router shelf (RouterB) that follows.

**Note**

When RouterA is reloaded, thereby forcing a failover, new entries are shown on RouterB when a **show redundancy history** command is issued after failover has occurred.

Log from the First Router (RouterA)

```
RouterA# show redundancy history
```

```
DSC Redundancy Status Change History:
```

```
010215 18:17 Slot -1 DSC:Failover configured -> ACTIVE role by default.
010215 18:18 Slot -1 DSC:Failover -> BACKUP role.
010215 18:18 Slot 12 DSC:Failover -> ACTIVE role.
010215 18:18 Slot 12 DSC:Hub, becoming active - arb timeout
```

```
RouterA# show redundancy
```

```
failover mode enabled, failover group = 32
Currently ACTIVE role.
DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
No connection to slot 13
```

```
RouterA# reload
```

```
Proceed with reload? [confirm] y
*Feb 15 20:19:11.059:%SYS-5-RELOAD:Reload requested
System Bootstrap, Version xxx
Copyright xxx by cisco Systems, Inc.
C7200 processor with 131072 Kbytes of main memory
```

Log from the Second Router (RouterB)

```
RouterB# show redundancy
```

```
failover mode enabled, failover group = 32
Currently BACKUP role.
No connection to slot 12
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.
```

```
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Switching to DSC 13
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Failover:changing to active mode
*Feb 16 03:24:54.931:%DIAL13-3-MSG:
02:32:06:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:24:55.491:%OIR-6-INSCARD:Card inserted in slot 12, interfaces administratively
shut down
*Feb 16 03:24:58.455:%DIAL13-3-MSG:
02:32:09:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:25:04.939:%DIAL13-0-MSG:
```

```
RouterB# show redundancy
```

```
failover mode enabled, failover group = 32
Currently ACTIVE role.
No connection to slot 12
DSC in slot 13:
Hub is in 'active' state.
Clock is in 'backup' state.
```

```
RouterB# show redundancy history
```

show redundancy

DSC Redundancy Status Change History:

```
010216 03:09 Slot -1 DSC:Failover configured -> BACKUP role.
010216 03:24 Slot 13 DSC:Failover -> ACTIVE role.
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
```

```
*Feb 16 03:26:14.079:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 1 Succeeded
*Feb 16 03:26:14.255:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 3 Succeeded
*Feb 16 03:26:14.979:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 10 Succeeded
```

Privileged EXEC Mode Example

The following is sample output generated by this command in privileged EXEC mode on router platforms that support no keywords for the privileged EXEC mode form of the command:

```
RouterB# show redundancy
```

```
MWR1900 is the Active Router
Previous States with most recent at bottom
```

```
INITL_INITL      Dec 31 19:00:00.000
LISTN_INITL      Feb 28 19:00:15.568
LISTN_LISTN      Feb 28 19:00:15.568
SPEAK_LISTN      Feb 28 19:00:18.568
SPEAK_SPEAK      Feb 28 19:00:18.568
STDBY_SPEAK      Mar 19 08:54:26.191
ACTIV_SPEAK      Mar 19 08:54:26.191
ACTIV_STDBY      Mar 19 08:54:26.191
ACTIV_ACTIV      Mar 19 08:54:26.191
INITL_ACTIV      Mar 19 08:56:22.700
INITL_INITL      Mar 19 08:56:22.700
INITL_LISTN      Mar 19 08:56:28.544
LISTN_LISTN      Mar 19 08:56:28.652
LISTN_SPEAK      Mar 19 08:56:31.544
SPEAK_SPEAK      Mar 19 08:56:31.652
SPEAK_STDBY      Mar 19 08:56:34.544
SPEAK_ACTIV      Mar 19 08:56:34.544
STDBY_ACTIV      Mar 19 08:56:34.652
ACTIV_ACTIV      Mar 19 08:56:34.652
INITL_ACTIV      Mar 19 10:20:41.455
INITL_INITL      Mar 19 10:20:41.455
INITL_LISTN      Mar 19 10:20:49.243
LISTN_LISTN      Mar 19 10:20:49.299
LISTN_SPEAK      Mar 19 10:20:52.244
SPEAK_SPEAK      Mar 19 10:20:52.300
SPEAK_STDBY      Mar 19 10:20:55.244
STDBY_STDBY      Mar 19 10:20:55.300
ACTIV_STDBY      Mar 19 10:21:01.692
ACTIV_ACTIV      Mar 19 10:21:01.692
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) router shelves (Cisco AS5800) or RSCs (Cisco AS5850).
hw-module	Enables the router shelf to stop a DSC or to restart a stopped DSC.
mode	Sets the redundancy mode.
mode y-cable	Invokes y-cable mode.
redundancy	Enters redundancy configuration mode.

Command	Description
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
show chassis	Displays, for a router with two RSCs, information about mode (handover-split or classic-split), RSC configuration, and slot ownership.
show standby	Displays the standby configuration.
standalone	Specifies whether the MWR 1941-DC router is used in a redundant or standalone configuration.
standby	Sets HSRP attributes.

