



High Availability Configuration Guide, Cisco IOS Release 15E

Americas Headquarters

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



CONTENTS

CHAPTER 1

Performing an In Service Software Upgrade 1

Finding Feature Information 1

Prerequisites for Performing an ISSU 1

Restrictions for Performing an ISSU 2

 General Restrictions 2

 Termination of Virtual Template Manager for ISSU Restrictions 2

 Cisco 10000 Series Internet Router Platform Restrictions 2

 Cisco Catalyst 4500 Restrictions 3

Information About Performing an ISSU 4

 ISSU Process Overview 4

 ISSU Rollback Timer 5

 Fast Software Upgrade 5

 Enhanced Fast Software Upgrade 5

 Versioning Capability in Cisco Software to Support ISSU 6

 Compatibility Matrix 6

 SNMP Support for ISSU 7

 Virtual Template Manager for ISSU 7

 Compatibility Verification Using Cisco Feature Navigator 7

 ISSU-Capable Protocols and Applications 8

How to Perform an ISSU 9

 Displaying ISSU Compatibility Matrix Information 9

 Loading Cisco IOS Software on the Standby RP 9

 Switching to the Standby RP 10

 Stopping the ISSU Rollback Timer 11

 Verifying the ISSU Software Installation 12

 Enabling the New Standby RP to Use New Software Version 12

 Aborting a Software Upgrade Using ISSU 13

 Configuring the Rollback Timer to Safeguard Against Upgrades 14

- Configuration Examples for Performing an ISSU 15
 - Example Verifying Redundancy Mode Before Beginning the ISSU Process 15
 - Example Verifying the ISSU State 16
 - Example Performing the ISSU Process 16
 - Example Aborting the ISSU Process 20
 - Example Verifying Rollback Timer Information 20
- Additional References 20
- Feature Information for Performing an ISSU 22



Performing an In Service Software Upgrade

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

- [Finding Feature Information, page 1](#)
- [Prerequisites for Performing an ISSU, page 1](#)
- [Restrictions for Performing an ISSU, page 2](#)
- [Information About Performing an ISSU, page 4](#)
- [How to Perform an ISSU, page 9](#)
- [Configuration Examples for Performing an ISSU, page 15](#)
- [Additional References, page 20](#)
- [Feature Information for Performing an ISSU, page 22](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Performing an ISSU

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

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

Restrictions for Performing an ISSU

General Restrictions

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



Note

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

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

Termination of Virtual Template Manager for ISSU Restrictions

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

Cisco 10000 Series Internet Router Platform Restrictions

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

- The following line cards support ISSU:
 - 1-port channelized OC-12/STM-4
 - 1-port Gigabit Ethernet
 - 1-port half-height Gigabit Ethernet
 - 1-port OC-12 ATM
 - 1-port OC-12 Packet over SONET (PoS)
 - 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
- The following interface cards support ISSU:
 - SPA Interface Processor (10000-SIP-600)
 - 2-port GE SPA
 - 5-port GE SPA
 - 8-port GE SPA
 - 1-port 10GE SPA

Cisco Catalyst 4500 Restrictions

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

Information About Performing an ISSU

ISSU Process Overview

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

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

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

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

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

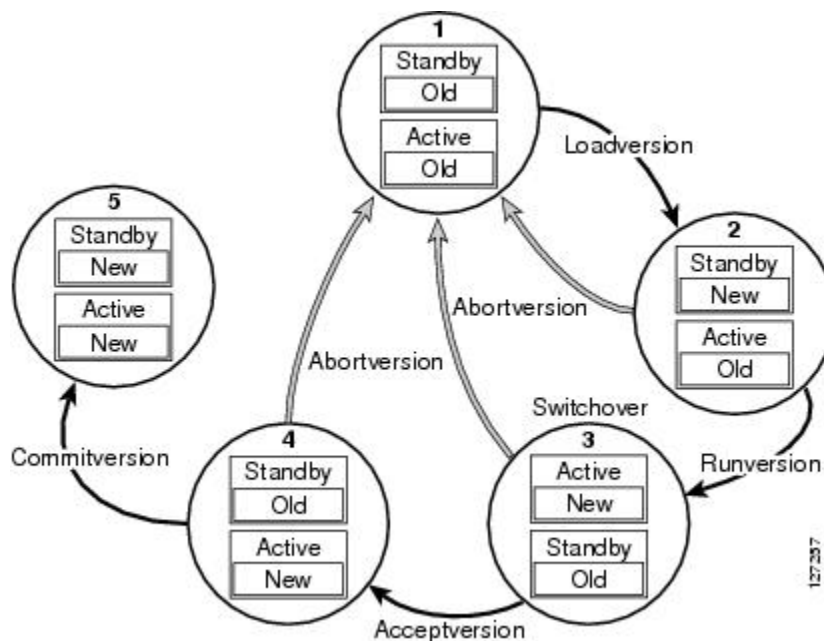
Then, the former active RP, which is now the new standby RP, is loaded with the new software.

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

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

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

Figure 1: ISSU States During the ISSU Process



ISSU Rollback Timer

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

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

Fast Software Upgrade

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

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

Enhanced Fast Software Upgrade

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

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

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

Versioning Capability in Cisco Software to Support ISSU

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

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

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

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

Compatibility Matrix

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

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

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

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

SNMP Support for ISSU

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

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

Virtual Template Manager for ISSU

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

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

Compatibility Verification Using Cisco Feature Navigator

The ISSU application on Cisco Feature Navigator allows you to:

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

ISSU-Capable Protocols and Applications

The following protocols and applications support ISSU:

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

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

How to Perform an ISSU

Displaying ISSU Compatibility Matrix Information

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>show issu comp-matrix {negotiated stored}</code></p> <p>Example:</p> <pre>Router# show issu comp-matrix negotiated</pre>	<p>Displays information about the the compatibility of the two software versions, one running on the active and the other on the standby RP.</p>

Loading Cisco IOS Software on the Standby RP

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	issu loadversion <i>image-name</i> Example: Router# issu loadversion a disk0:c10k2-p11-mz.2.20040830 b stby-disk0:c10k2-p11-mz.2.20040830	Starts the ISSU process. <p>Note The active and standby slots are optional for this command. You must provide the same image-name for both the active and standby slots. Active slot number is not available for this command.</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	show issu state [detail] Example: Router# show issu state	Displays the state of the device during the ISSU process. <ul style="list-style-type: none"> • Confirm that the standby RP is loaded and is in SSO mode.

Switching to the Standby RP

SUMMARY STEPS

1. enable
2. issu runversion

DETAILED STEPS

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

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

Stopping the ISSU Rollback Timer

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show issu rollback-timer Example: <pre>Router# show issu rollback-timer</pre>	Displays amount of time left before an automatic rollback will occur.
Step 3	issu acceptversion Example: <pre>Router# issu acceptversion b disk0:c10k2-p11-mz.2.20040830</pre>	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process. <ul style="list-style-type: none"> • You must enter this command within the time period specified by the rollback timer displayed in the previous step. • The active slot-number and slot-name parameters are optional for this command.

Verifying the ISSU Software Installation

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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 RPs 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 Software Version

SUMMARY STEPS

1. `enable`
2. `issu commitversion`

DETAILED STEPS

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

	Command or Action	Purpose
	Example: <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	issu commitversion Example: <pre>Router# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830</pre>	Allows the new Cisco IOS software image to be loaded into the standby RP. Note The <i>slot active-image</i> parameter is optional for this command.

Aborting a Software Upgrade Using ISSU

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

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

SUMMARY STEPS

- enable
- issu abortversion *slot image*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	issu abortversion <i>slot image</i> Example: <pre>Router# issu abortversion b disk0:c10k2-p11-mz.2.20040830</pre>	Aborts the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.

Configuring the Rollback Timer to Safeguard Against Upgrades

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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 <i>seconds</i> 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.

Configuration Examples for Performing an ISSU

Example Verifying Redundancy Mode Before Beginning the ISSU Process

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

```

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

```

Example Verifying the ISSU State

The following sample output 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 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:/
```

Example Performing the ISSU Process

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

Initiating the ISSU Process

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

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

```
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.2.20040830,1;disk0:c10k2-p11-mz.1.20040830,1;
Operating Mode = SSO
Primary Version = disk0:c10k2-p11-mz.2.20040830
Secondary Version = disk0:c10k2-p11-mz.1.20040830
Current Version = disk0:c10k2-p11-mz.2.20040830
Slot = A
RP State = Standby
ISSU State = Run Version
Boot Variable = disk0:c10k2-p11-mz.1.20040830,1;
Operating Mode = SSO
Primary Version = disk0:c10k2-p11-mz.2.20040830
Secondary Version = disk0:c10k2-p11-mz.1.20040830
Current Version = disk0:c10k2-p11-mz.1.20040830

```

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

Stopping the Rollback Process

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

```
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

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

```
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 software version upgrades or downgrades will require that a new ISSU process be invoked.

Example Aborting the ISSU Process

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

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

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

Example Verifying Rollback Timer Information

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

```
Router# show issu rollback-timer

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

Additional References

Related Documents

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

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Performing an ISSU

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

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

Table 1: Feature Information for Performing an In Service Software Upgrade Process

Feature Name	Releases	Feature Information
--------------	----------	---------------------

ISSU	12.2(28)SB 12.2(31)SB2 12.2(31)SGA 12.2(33)SB 12.2(33)SRB1 12.2(33)SRC 12.2(33)SRE 12.3(11)T Cisco IOS XE 3.1.0SG	<p>In Service Software Upgrade (ISSU) allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues, increasing network availability and reducing downtime caused by planned software upgrades.</p> <p>In 12.2(31)SGA, ISSU was introduced on the Cisco 7200 router.</p> <p>In 12.2(31)SGA, support for ISSU was introduced on the Cisco Catalyst 4500 series switch.</p> <p>In 12.2(33)SB, support for the following interface cards was added.</p> <ul style="list-style-type: none"> • SPA Interface Processor (10000-SIP-600) • 2-port GE SPA • 5-port GE SPA • 8-port GE SPA • 1-port 10GE SPA
ARP	12.2(33)SRB1 12.2(33)SXI	This feature is supported.
ATM	12.2(33)SRB1 12.2(33)SRE 15.0(1)S	This feature ARP is supported.
Circuit Emulation Services (CES) for TDM pseudowires	12.2(33)SRC	This feature is supported.
DHCP ODAP client/server	12.2(31)SB2 12.2(33)SRC 15.0(1)S	This feature is supported.
DHCP proxy client	12.2(31)SB2 12.2(33)SRC 15.0(1)S	This feature is supported.
DHCP relay on unnumbered interface	12.2(31)SB2 12.2(33)SRC 15.0(1)S	This feature is supported.
DHCP server	12.2(31)SB2 12.2(33)SRC 15.0(1)S	This feature is supported.

DHCP snooping	12.2(31)SGA	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
EtherChannel - PagP and LACP	12.2(31)SGA	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
FHRP - HSRP group shutdown	12.2(33)SRC	This feature is supported.
Frame Relay	12.2(33)SRB1 15.0(1)S	This feature is supported.
GLBP	12.2(31)SB2 12.2(33)SRB1	This feature is supported.
HDLC	12.2(33)SRB1	This feature is supported.
HSRP	12.2(30)S 12.2(31)SGA 12.2(33)SRB1	This feature is supported. In 12.2(31)SGA, this feature was introduced on the Cisco 7200 router. Support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
HSRP	12.2(30)S 12.2(31)SGA 12.2(33)SRB1	This feature is supported. In 12.2(31)SGA, this feature was introduced on the Cisco 7200 router. Support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
IEEE 802.1x protocol	12.2(33)SRB1 12.2(31)SGA	This feature is supported. In 12.2(31)SGA, this feature was introduced on the Cisco 7200 router. Support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
IEEE 802.3af	12.2(31)SGA	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
IGMP snooping	12.2(31)SGA	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.

IP host	12.2(31)SGA	This feature is supported.
IPv4 Multicast	12.2(33)SRE 15.0(1)S	This feature is supported.
IS-IS	12.2(31)SB2 12.2(31)SGA 12.2(33)SRB1 15.0(1)S Cisco IOS XE 3.1.0SG	This feature is supported. In 12.2(31)SGA, this feature was introduced on the Cisco 7200 router. Support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
MPLS Clients	12.2(28)SB 12.2(33)SRB1	MPLS applications can be upgrading using the In Service Software Upgrade (ISSU) process and the enhanced Fast Software Upgrade (eFSU) process. Thus, MPLS applications are considered ISSU's MPLS clients. The ISSU process allows Cisco IOS software at the router level to be updated or otherwise modified while packet forwarding continues. At the line-card level, the eFSU process minimizes line-card downtime during such upgrades to between 30 and 90 seconds, by loading the new line-card image before the ISSU switchover occurs from the active to the standby Route Processor (RP). In 12.2(28)SB, the ISSU feature was introduced. In 12.2(33)SRB-1, the LSPV Push and TE clients and the eFSU functionality were added.
MPLS VPN 6VPE and 6PE ISSU support	12.2(33)SRE 12.2(33)XNE	This feature is supported.
MTR	12.2(33)SRB1	This feature is supported.
NSF/SSO/ISSU - Virtual Private LAN Services	12.2(33)SXI4 15.0(1)S	This feature is supported.
Port security	12.2(31)SGA	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.

PPP/MLP	12.2(33)SRB1	This feature is supported.
PPPoA	12.2(31)SB2	This feature is supported.
PPPoE	12.2(31)SB2 15.0(1)S	This feature is supported.
QoS	12.2(31)SB2 12.2(33)SRB1	This feature is supported.
RIB/VRF	12.2(33)SRB1 12.2(33)SRE	This feature is supported.
SNMP	12.2(33)SB 12.2(33)SRB1	This feature is supported.
STP	12.2(31)SGA 12.2(33)SRB1	This feature was introduced on the Cisco 7200 router and support for ISSU was introduced on the Cisco Catalyst 4500 series switch.
Virtual template manager	12.2(33)SRC	This feature is supported.
VRRP	15.0(1)S	This feature is supported.