Cisco IOS In-Service Software Upgrade Process

First Published: December 17, 2008

Last Updated: July 11, 2012

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 topics and describes the steps taken to perform ISSU in a system.

Finding Feature Information

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

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

Contents

Prerequisites for Performing ISSU

General Prerequisites

- 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 exist in the file systems of both the active and standby RPs, and they both must have the same running image path, before you begin the ISSU process.
- ISSU is supported within a Cisco IOS Release. Upgrading between two different Cisco IOS Releases using ISSU process is not supported. For example, upgrading from Cisco IOS Release 12.2(33)SCG to Cisco IOS Release 12.2(33)SCH using ISSU is not supported.
- 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. NSF must be configured on routers that are connected to the uBR broadband routers.

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 1: ISSU Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [1]

1 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Note Line card HA is supported for Cisco uBR-MC3GX60V line cards from 12.2(33)SCE1 onwards. ISSU is supported between rebuilds in the same release train. For example: ISSU is supported when upgrading from Cisco IOS Release 12.2(33)SCH FCS to Cisco IOS Release 2.2(33)SCH1.

Cisco uBR10012 Universal Broadband Router Platform Prerequisites

- The following WAN line card supports ISSU-uBR10K:
  - 1-Port Half-Height Gigabit Ethernet
- For the RLC ISSU process to run on cable line cards, the cable line cards must be configured for N+1 line card redundancy.

For more information about configuring N+1 redundancy, see N+1 Redundancy for the Cisco CMTS Routers .

Note If a cable line card is not configured for N+1 line card redundancy, it will be reloaded upon execution of the RP **issu linecard reloadversion** command. This will cause interruption of data service.

- The following jacket cards and SPA support Minimum Disruptive Restart (MDR):
  - Cisco 10000-SIP-600 Jacket card
  - SPA-24XDS-SFP (Wideband DOCSIS SPA)

Please see MDR Support for ISSU, on page 22 for more details.

- Before running any ISSU process, determine the compatibility level between the Cisco IOS software versions on the active and the standby RPs.
- The Dynamic Image Version Compatibility (DIVC) feature is not supported by the ISSU-uBR10K feature. The bundled compatibility matrix in the released image checks for the image compatibility. For more information, see the How to Perform the RP ISSU Process, on page 23.
- The ISSU process shall be performed under normal PRE CPU utilization and line card CPU utilization conditions. The ISSU process is not recommended when the PRE processor module CPU utilization is constantly higher than 80% or line card CPU utilization is higher than 90%.

High CPU consumption processes (such as SNMP polling) should be avoided during the ISSU process.

The following commands are used to check the PRE processor module CPU utilization and line card CPU utilization respectively prior to start of the ISSU process:

- **show processes cpu**
- **show controllers cable [proc-cpu]**

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.
- ISSU requires that there are no error conditions in the chassis. A Cisco UBR-MC20X20V cable interface line card in maintenance mode is considered an error condition. Upgrade the line card to a valid license or remove the maintenance mode line card from the system before performing ISSU.

Note ISSU supports only software upgrade on routers with the same PRE hardware. ISSU can be performed either on routers with dual PRE2 hardware or dual PRE4 hardware. ISSU does not support hardware upgrade of PRE2 to PRE4 or vice versa.

- ISSU operations utilize large amounts of system resources to perform reliable upgrades. Therefore, it is recommended that any unnecessary activities, such as excessive diagnostic activities like debugs, are ceased during all ISSU operations. However, the following debug commands do not adversely affect ISSU operations:
  - debug issu process
  - debug issu rlc-issu
  - debug cable preso
  - debug hccp timing
  - debug ipc issu

Note Usage of any other debug command during ISSU operations, apart from the ones specified above, may produce unexpected performance or results.

Cisco uBR10012 Universal Broadband Router Platform Restrictions

- ISSU-uBR10K process is available only in Cisco IOS Release 12.2(5th)SB and later on the Cisco uBR10012 Universal Broadband Router for the Performance Routing Engines- PRE-2 and PRE-4.
- The Cisco uBR10012 router supports ISSU processes at both the route processor (RP) level (for the PRE-2 cards), and at the line card (LC) level, with the following restrictions:
  - The RP ISSU process performs Minimal Disruptive Restart (MDR) functions for the supported WAN line cards, which supports a restart of the line card software with its associated upgraded or downgraded image, with minimum interruption of traffic flow.

Note The following WAN line cards support MDR for ISSU-uBR10K: 1-Port Half-Height Gigabit Ethernet and 10000-SIP-600 (4 bay Cisco 10000 SPA Jacket Card).

  - The redundant LC (RLC) ISSU process does not run automatically as part of the RP ISSU process for cable line cards. The RLC ISSU process must be initiated manually for supported cable line cards.
  - The RP ISSU process must be run prior to initiating the RLC ISSU process for the cable line cards. The RP must remain in the Run Version state until the RLC ISSU process completes while the standby RP must also be in hot standby, and ISSU accept version must have been run.
  - If a cable line card is not configured for N+1 line card redundancy, you need to upgrade via a sequential reload, using the issu linecard reloadversion command. This will cause interruption of data service for the cable line card.

- The Dynamic Image Version Compatibility (DIVC) feature is not supported by the ISSU-uBR10K feature.
- While performing ISSU within a Cisco IOS Release (for example, Cisco IOS Release 12.2(33)SCH to Cisco IOS Release 12.2(33)SCH1), MIBs like CISCO-PROCESS-MIB cannot be accessed during the period between ISSU run version and accept version.

Information About Performing ISSU

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

ISSU-uBR10K Process Overview

The ISSU-uBR10K feature enhances the set of High Availability (HA) features on the Cisco uBR10012 Universal Broadband Router by providing software upgrade or downgrade services for Cisco IOS software images and line card images on redundant Cisco uBR10012 router hardware, with minimal interruption of service. ISSU-uBR10K includes RP ISSU support between Performance Routing Engines and MDR support for certain WAN line cards, and extends the ISSU process to cable line cards.

On the Cisco uBR10012 router, the ISSU-uBR10K process consists of two phases:

1. RP ISSU phase—In this first phase, the RP ISSU process upgrades the image on the standby PREs and upgrades images for any supported WAN line cards with minimal network interruption.
2. RLC ISSU phase—(Supported only on the Cisco uBR10012 router) Once the RP ISSU process has been run and the RP is in the runversion state, this second ISSU phase can be initiated to upgrade images on redundant cable line cards. The other conditions to run the RP ISSU are standby RP has to be in hot standby mode and rollback timer has to be stopped using the issu acceptversion command.

If a cable line card is not configured for N+1 line card redundancy, you need to upgrade via a sequential reload, using the issu linecard reloadversion command.This will cause interruption of data service for the cable line card.

Switchovers during both the RP and RLC ISSU processes ensure that there are no cable modem drops (CMs do not go offline) and no PacketCable voice call drops.

RPU-only ISSU Process Overview

Existing Upgrade Process

The existing upgrade bundle consists two phases:

1. RP ISSU Upgrade: The RP ISSU upgrade is initiated. When the process reaches the issu runversion state, the RP rollback timer is stopped with **issu acceptversion** command.
2. Redundant LC ISSU Upgrade: The second phase is where the line cards connect to th new RPs and ISSU image negotiation begins. At this point, the **issu linecard** commands are executed one by one upto the **issu linecard runversion** command stage. The **issu commitversion** command is commonly executed for both RPs and line cards.

The RP-only ISSU Solution

This solution provides for upgrade of only the RP images without upgrading the line card images.

The RP-only ISSU process skips the Redundant LC ISSU Upgrade phase if the line card images matches the previous or old line card image bundled into the upgrade image. The Redundant LC ISSU Upgrade process is optional if the new upgrade image is an RP-only ISSU image.

1. The upgrade bundle must bundle the old LC image.
2. At present this process is supported only for Cisco uBR-MC20X20V and Cisco uBR-MC3GX60V line cards.

RP-only ISSU process uses the same commands that are used in the existing ISSU Upgrade process. The process consists the following steps:

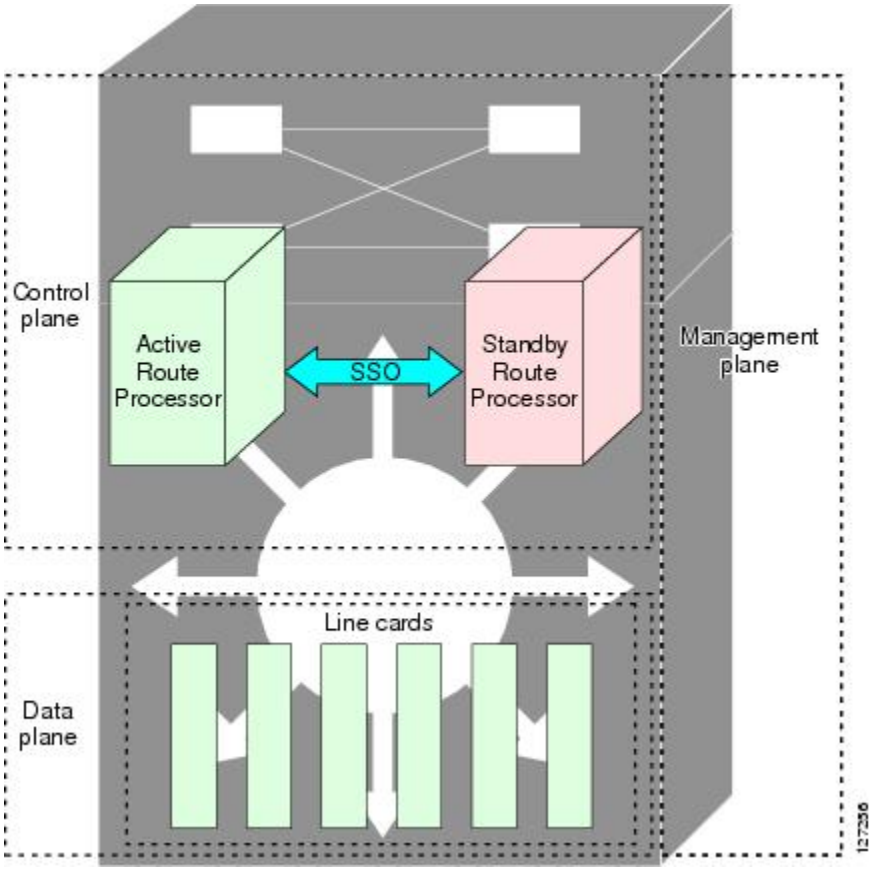
1. The RP-only ISSU Upgrade may be done using the ISSU Multi-Step Upgrade Process, page 24 or the ISSU Single-Step Upgrade Process, page 29.
2. 2.If the Multi-Step Upgrade process is used, the Redudndant LC ISSU process may be performed using the Running the RLC ISSU Process Automatically, page 36. The RLC ISSU upgrade process may be ignored if it is ensured that the upgrade image used for the ISSU Upgrade process is an RP-only ISSU image.
3. The upgrade must be completed using the t_Finishing_the_ISSU_Process_to_Enable_the_New_Cisco_IOS_Software_Version_on_the_RP_and_Cable_Line_Cards_1093719.xml#task_1093719.

RP ISSU Process Overview

The RP 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 below). 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.

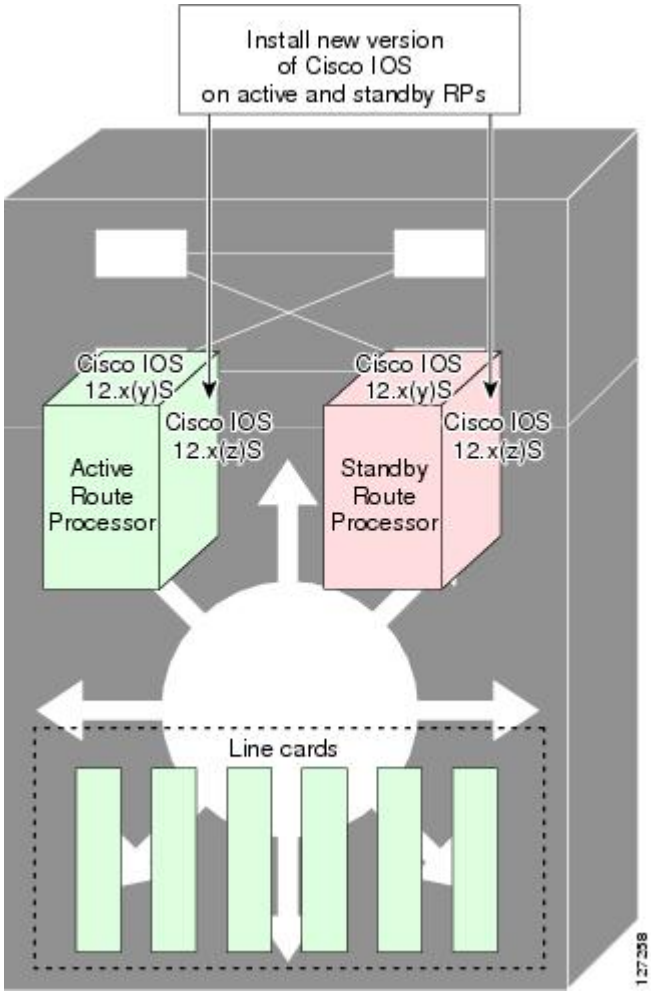
SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two RPs to be kept in synchronization although they may support different sets of commands.

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



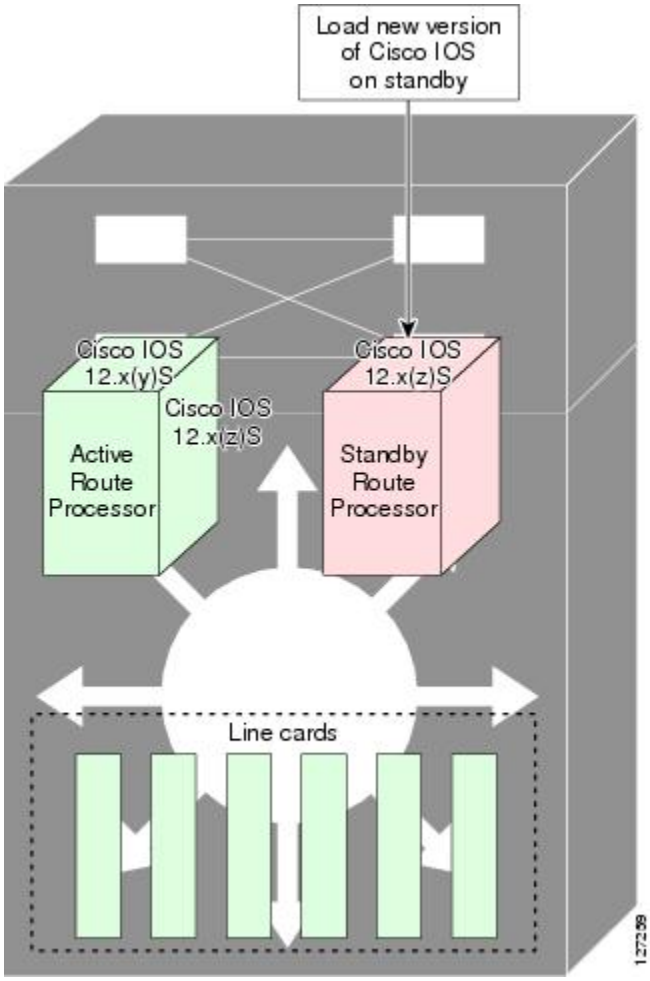
An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, copy the Cisco IOS software into the file systems of both RPs (see Figure below).

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



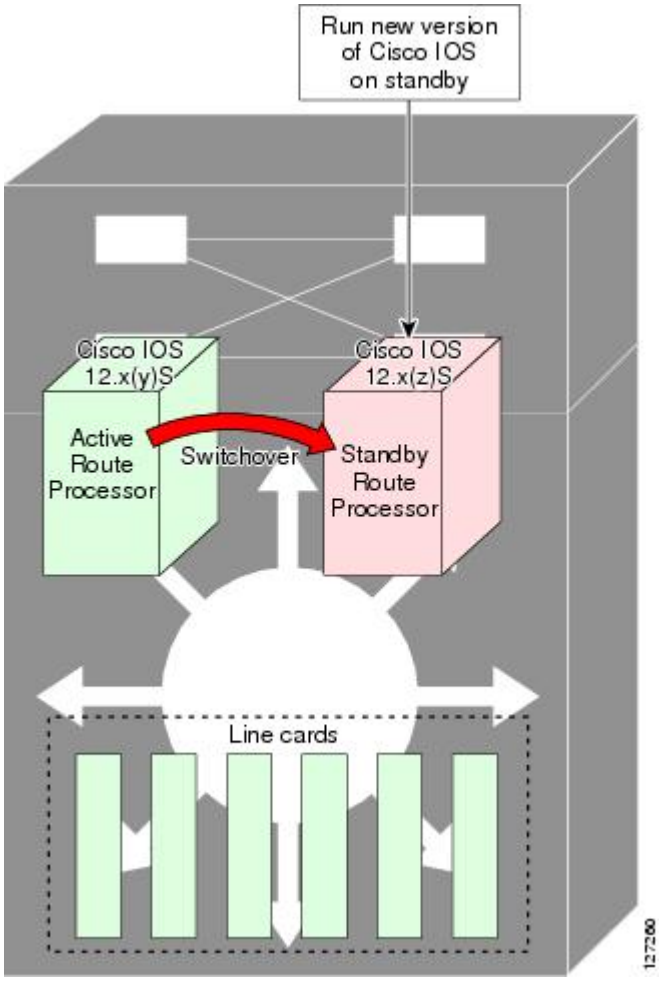
After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP (see Figure below).

Figure 3: Load New Cisco IOS Software on the Standby RP



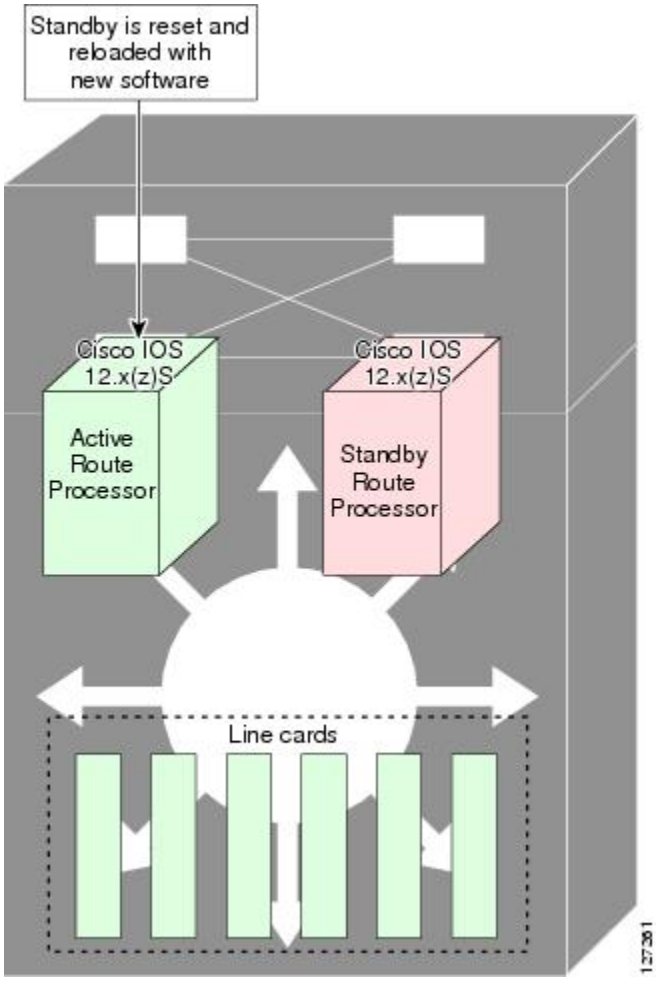
After switchover, the standby RP takes over as the new active RP (see Figure below).

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 below).

Figure 5: Load New Standby RP with New Cisco IOS Software

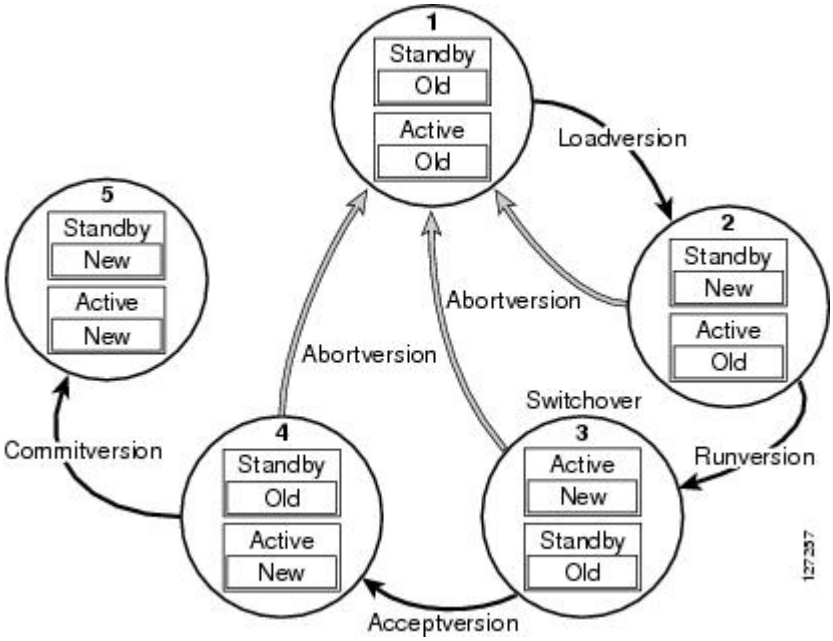


The two RPs in a system can be in one of three different states during ISSU:

- 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 below 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.

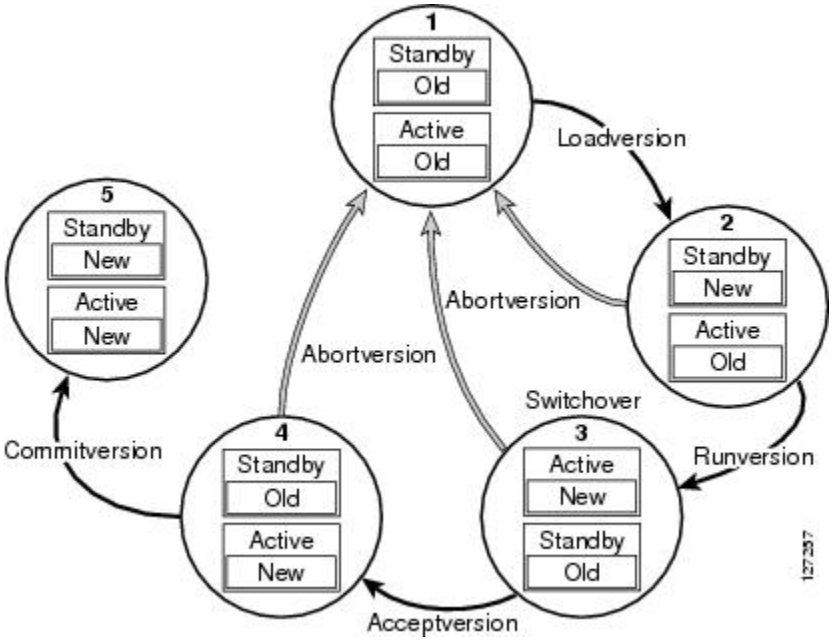
Cisco NSF is used with SSO. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, thereby reducing loss of service outages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

Figure below illustrates how SSO is typically deployed in service provider networks. In this example, Cisco NSF with SSO is enabled at the access layer (edge) of the service provider network. A fault at this point could result in loss of service for enterprise customers requiring access to the service provider network.

For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Depending on your objectives,

you may decide to deploy Cisco NSF and SSO features at the core layer of your network. Doing this can help reduce the time to restore network capacity and service for certain failures, which leads to additional availability.

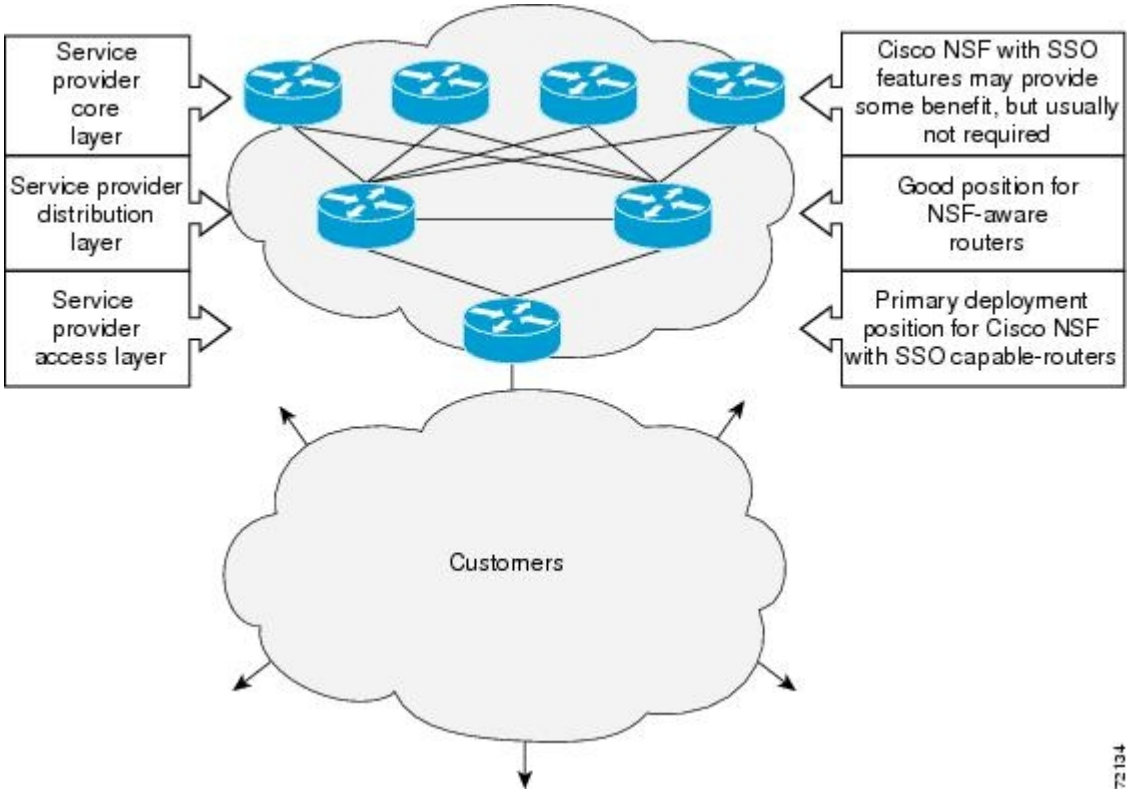
Figure 7: Cisco NSF with SSO Network Deployment: Service Provider Networks



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

enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Figure 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.

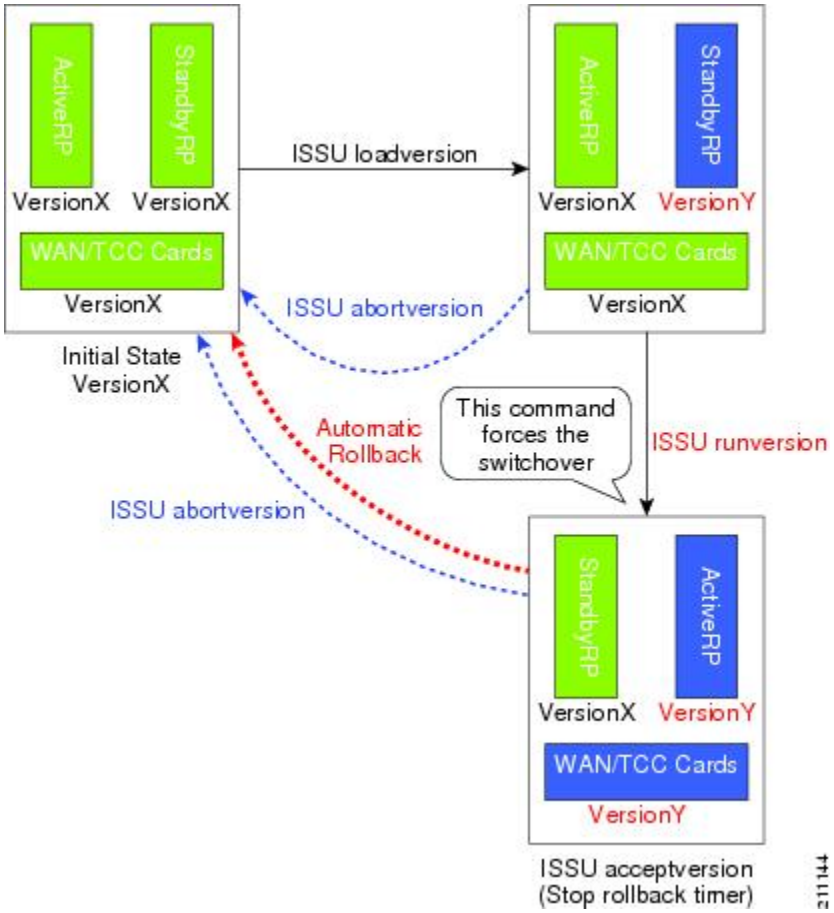
Redundant LC ISSU Process Overview

Note Effective with Cisco IOS Release 12.2(33)SCH2, in the RP-only ISSU process, the Redundant LC ISSU Upgrade process is optional.

The redundant LC (RLC) ISSU process is introduced in Cisco IOS Release 12.2(5th)SB on the Cisco uBR10012 Universal Broadband Router to support software upgrades without service interruption on supported, redundantly-configured cable line cards. The RLC ISSU process is the second phase of ISSU support in the ISSU-uBR10K feature and is supported only on the Cisco uBR10-MC5X20S/U/H cable line cards on the Cisco uBR10012 router. The dual TCC+ or DTCC+ cards are sequentially reloaded after running the issu runversion command.

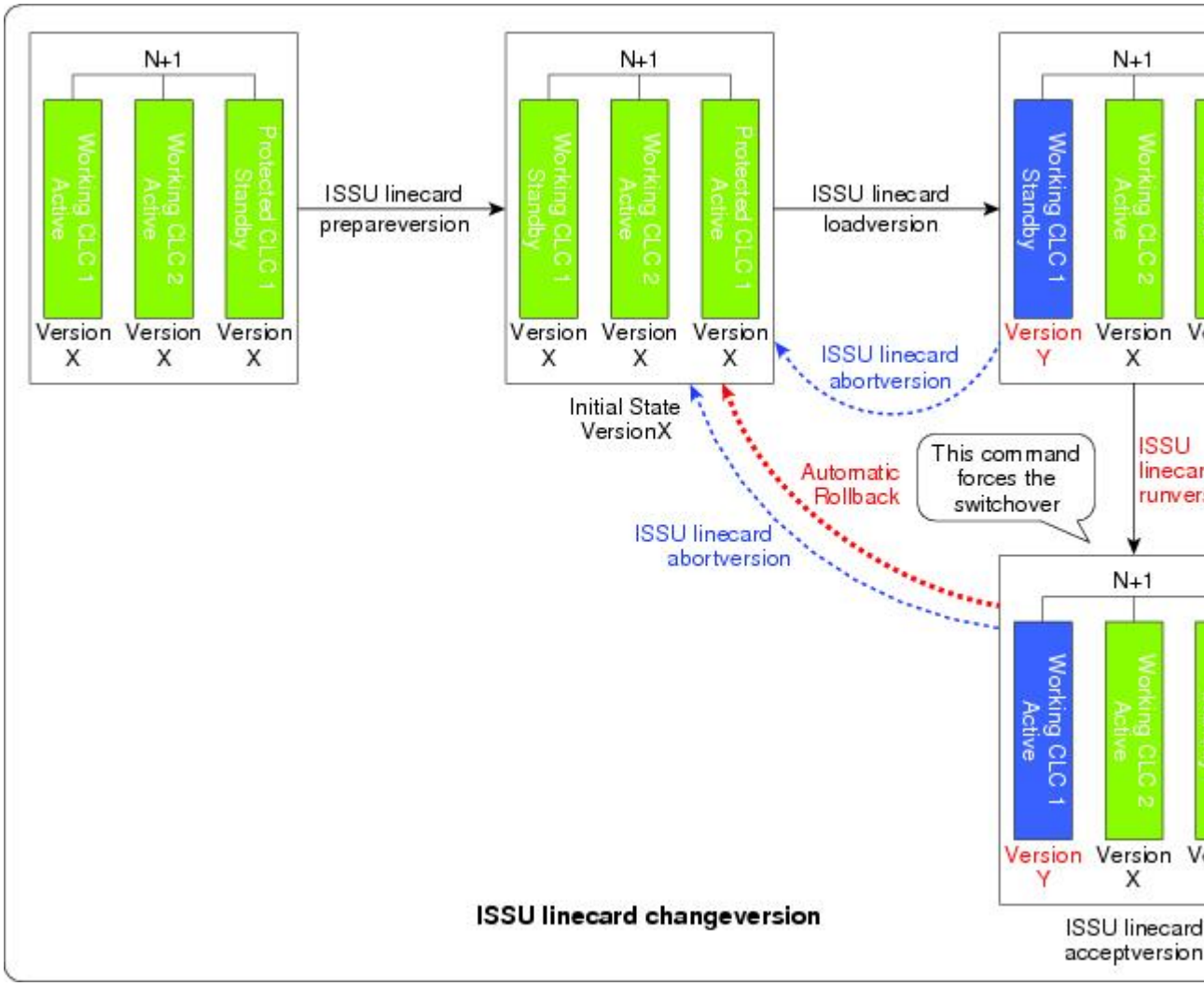
The RLC ISSU process has some dependencies with the RP ISSU process. First, the RLC ISSU process can be started only when the RP ISSU process reaches the Run Version (RV) state. In the RV state, the RP rollback timer is stopped (via the **issu acceptversion** command) and the active RP is running the new version of the software image. Each of the cable line cards have reconnected to the new RP and ISSU image negotiation has occurred between the RP and the cable line cards (See Figure below).

Figure 9: RP ISSU Process Stages With WAN Line Card MDR



At this point in the RP ISSU process, the stages of the RLC ISSU process can be executed. The stages of the RLC ISSU process are comparable to the stages that occur in the RP ISSU process. The RLC ISSU process itself can be initiated to run manually or automatically. In the manual method, the Prepare Version (only in RLC ISSU process), Load Version, Run Version, and Accept Version stages are executed in step-by-step fashion by running the corresponding **issu linecard** command for each stage of the process. In the automatic method, a single command (**issu linecard changeversion**) is executed to run each of these stages back-to-back and automatically as each stage completes (Figure below).

Figure 10: RLC ISSU Process Stages

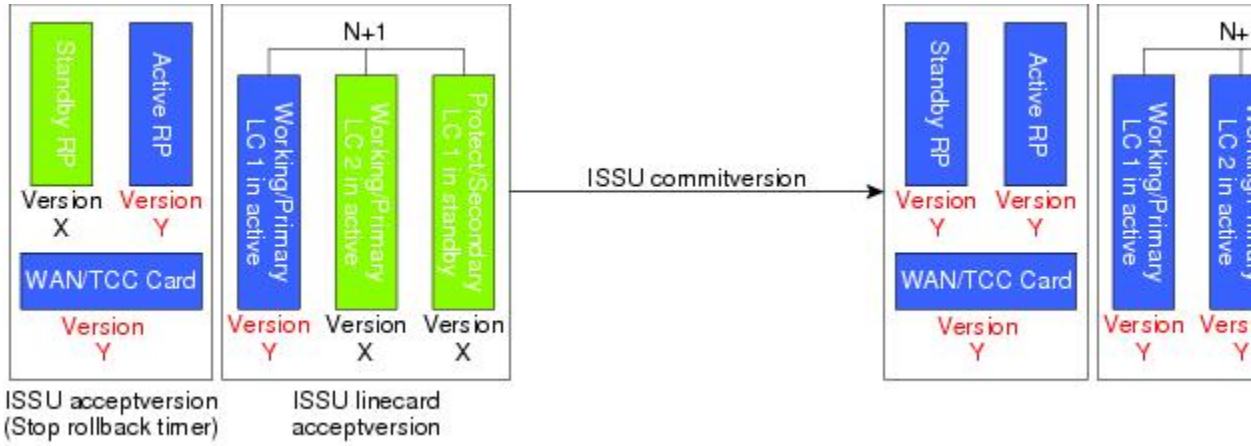


The RLC ISSU process runs serially for each targeted cable line card. A subsequent cable line card may start the process when the previous cable line card's RLC ISSU process is complete. This process is different from the ISSU process for other line cards supporting MDR, which reloads simultaneously during the Run Version stage of the RP ISSU process.

Finally, when the RLC ISSU process is complete for all redundant cable line cards, a condition is set such that the RP ISSU Commit Version stage can be executed. The RP and RLC ISSU processes share the Commit

Version stage such that the **issu commitversion** command confirms both the RP and RLC images at the same time (Figure below).

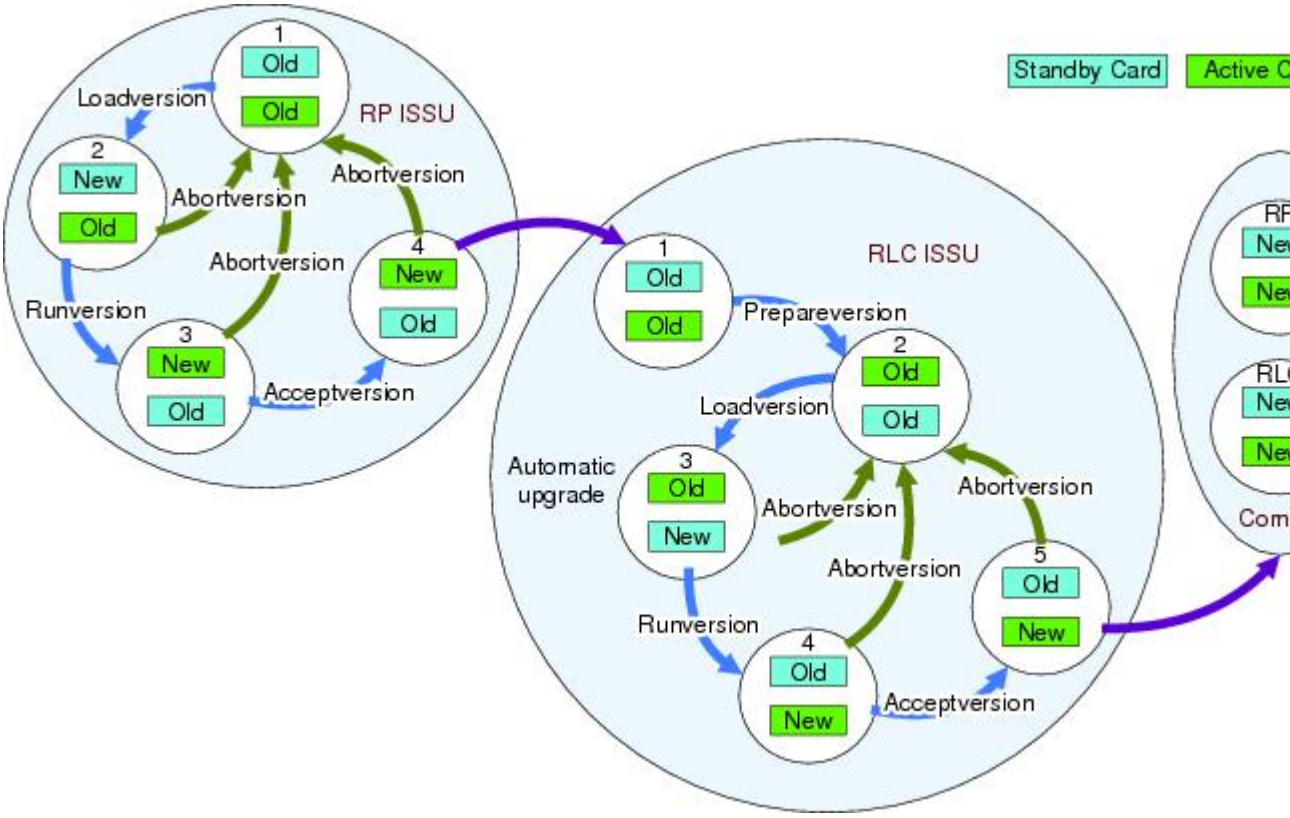
Figure 11: Combined RP and RLC ISSU Commit Version Stage



While the RLC ISSU process also supports the functions of aborting a version upgrade as the RP ISSU process does, it has the additional functions of stopping an automatic RLC ISSU process, stopping other RLC ISSU processes in the middle of execution, and reloading a version. The Reload Version function is intended to support cable line cards that are not configured for redundancy and that do not support the MDR function of the RP ISSU process.

Figure below provides a graphical overview of these RP and RLC ISSU processes.

Figure 12: RP and RLC ISSU Process Summary View



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).

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.

Compatibility Information for ISSU-uBR10K on the Cisco uBR10012 Universal Broadband Router

The **show issu comp-matrix negotiated** command provides information about the compatibility for the Cisco IOS software images on the active and standby PRE-2 cards. Compatibility information between the RP images and LC images, or LC to LC images is not explicitly reported in this output.

However, if the **show issu comp-matrix negotiated** command indicates compatibility between RP images, then RP to LC, and LC to LC image compatibility is also supported.

The following example shows sample output from the **show issu comp-matrix negotiated** command on the Cisco uBR10012 Universal Broadband Router:

```
Router# show issu comp-matrix negotiated
CardType: uBR10000(107), Uid: 2,  Image Ver: 12.2(20070219:204203)145
Image Name: UBR10K2-K9P6U2-M
```

```
Cid     Eid     Sid     pSid    pUid      Compatibility
=========================================================
2       1       65538   65542   15        COMPATIBLE
2       1       65543   65542   11        COMPATIBLE
2       1       65549   65543   17        COMPATIBLE
2       1       65579   4       1         COMPATIBLE
3       1       65577   6       1         COMPATIBLE
4       1       65567   13      1         COMPATIBLE
5       1       65547   27      1         COMPATIBLE
7       1       65570   5       1         COMPATIBLE
8       1       65572   11      1         COMPATIBLE
9       1       65540   0       2         COMPATIBLE
9       1       65541   0       2         COMPATIBLE
9       1       65545   0       2         COMPATIBLE
9       1       65563   0       2         COMPATIBLE
9       1       65569   2       1         COMPATIBLE
9       1       65573   0       2         COMPATIBLE
9       1       65575   0       2         COMPATIBLE
10      1       60      0       2         COMPATIBLE
```

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

Restrictions for ISSU-Capable Protocols and Applications With ISSU-uBR10K

The following protocols and applications are not supported with ISSU-uBR10K:

- ISSU - ATM
- ISSU - FHRP/GLBP
- ISSU - FHRP/HSRP
- ISSU - Frame Relay
- ISSU - HDLC
- ISSU - IEEE 802.1x
- ISSU - IEEE 802.3af
- ISSU - IGMP snooping
- ISSU - Port Security
- ISSU - PPP/MLP
- ISSU - STP

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.

MDR Support for ISSU

Minimum Disruptive Restart (MDR) is a feature that allows line cards to be restarted to minimize the disruption of traffic passing through the system. It prevents line protocol flaps and minimizes traffic disruption across a restart or reload of software. The uBR10K platform supports MDR of the Cisco 10000-SIP-600 jacket card and the SPA-24XDS-SFP (Wideband DOCSIS SPA). ISSU prevents network outage whenever the 10000-SIP-600 card or the Wideband SPA card reloads.

The advantages of the MDR feature in ISSU are:

- Reduces the time for a line card to pass data traffic after the card's reload.
- Maintains data and configuration during the software restart or reload.
- Retains the status of the line card after MDR.

Note MDR supports only minor changes in software, while the line cards reload in case of a major change in software or firmware.

MDR and FPGA Upgrade

Most often when performing MDR ISSU upgrade for the Cisco 10000-SIP-600 jacket card and the SPA-24XDS-SFP, only the firmware is upgraded - the FPGA will remain intact. However, there might be some rare cases where the FPGA will need to be upgraded. In these cases, the MDR ISSU process will become FPGA upgrade process. Unlike MDR ISSU, FPGA Upgrade will cause all traffic passing through the Cisco 10000-SIP-600 jacket card to be completely disrupted. During this FPGA upgrade process, the new FPGA will be downloaded to each SPA. It takes approximately 12 minutes to download the new FPGA to each SPA.

The FPGA upgrade process is an independent process from the system ISSU process. The system ISSU process triggers the FPGA upgrade process during the issu runversion step, and will continue to upgrade other cable line cards in the system. These two processes execute at the same time, and one process can finish before the other.

The show upgrade fpd progress command can be used to check the status of the FPGA upgrade process.

ISSU Single-Step Upgrade Process

Single-step upgrade process is the ability of the ISSU feature to upgrade the entire CMTS system using the **issu changeversion** command. This process allows the corresponding networking device to inform the system that the networking device is performing a complete upgrade cycle automatically, and the state transitions to move to the next step automatically.

The ISSU upgrade process consists of three states:

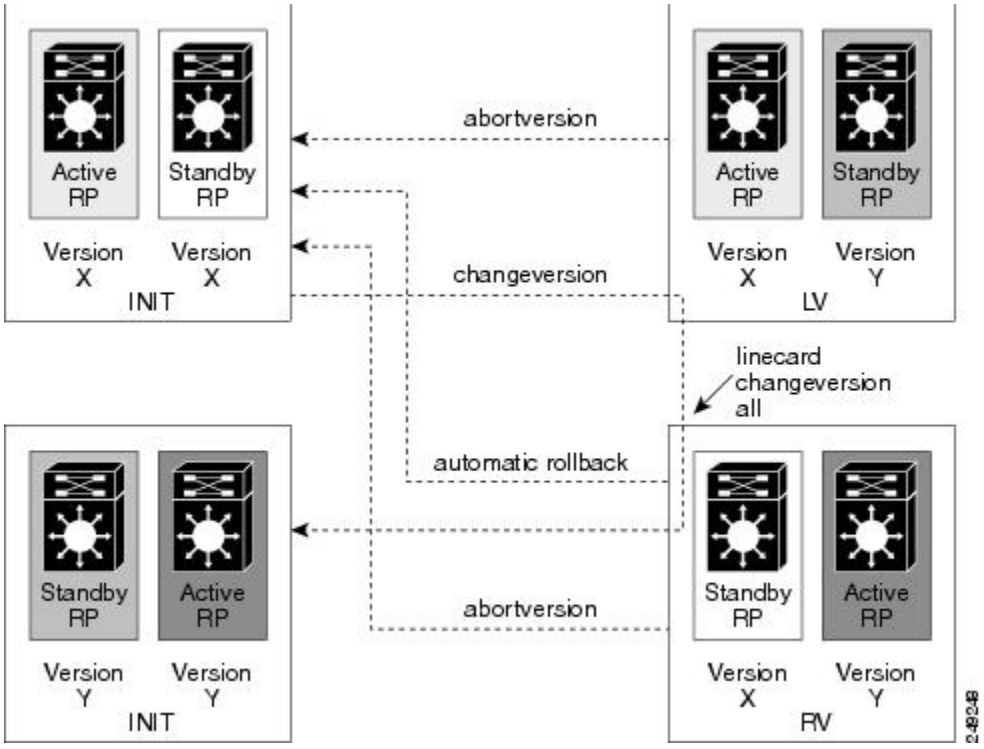
1. Initialization (INIT) state—It is the steady state before any software upgrade is committed.
2. Load version (LV) state—It is the state when the issu loadversion command is executed to start the ISSU process.
3. Run version (RV) state—It is the state when the issu runversion command is executed to force a switchover from the active Route Processor (RP) to the standby RP.

Each of these states is defined by a set of variables, that is, primary version (PV), secondary version (SV), current version (CV), and ISSU state (IS). The transition of all these states is accomplished using the **issu changeversion** command, which automatically performs these state transitions.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU can be performed using the single step upgrade process using the **issu changeversion** command.

Figure below provides a graphical overview of the single-step upgrade process.

Figure 13: Single-step Upgrade Process Summary View



The advantages of the Single-Step Upgrade process are:

- Reduces human interaction during the ISSU upgrade cycle.
- Avoids executing multiple commands to complete the ISSU cycle.

How to Perform the RP ISSU Process

Unlike SSO, which is a mode of operation for the device and a prerequisite for performing RP 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 RP ISSU Process

The following list provides basic restrictions for performing the RP 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.

Restrictions for Performing the RP ISSU Process on the Cisco uBR10012 Universal Broadband Router

- The RP ISSU process is supported beginning in Cisco IOS Release 12.2(33)SCB using the following Cisco IOS software images:
  - ubr10k2-k9p6u2-mz
  - ubr10k4-k9p6u2-mz
- The RP ISSU process is supported beginning in Cisco IOS Release 12.2(5th)SB using the following Cisco IOS software image:
  - ubr10k2-k9p6u2-mz
- If you are performing the RP and RLC ISSU process on the Cisco uBR10012 Universal Broadband Router, read first the How to Perform the Redundant LC ISSU Process, on page 31. This section describes which RP ISSU tasks are prerequisites for the RLC ISSU process.

Note The examples provided in the RP ISSU process sections of this document reflect certain Cisco 10000 Series Router software image names. Be aware when referring to these examples that you replace these sample image names with the appropriate supported image name for your platform.

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

Restrictions for Performing the RP-only ISSU Process on the Cisco uBR10012 Universal Broadband Router

Effective from Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU process is supported using the following Cisco IOS line card software images:

– ubr10kg4clc-lck8-mz

ISSU Multi-Step Upgrade Process

The ISSU multi-step upgrade process consists of the following tasks:

Note Starting Cisco IOS Release 12.2(33)SCD2 onwards, you can you can complete the RP upgrade using the ISSU Single-Step Upgrade Process, on page 28 and skip the tasks mentioned above.

Note Effective from Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process may be performed using the three steps of the ISSU Multi-Step Upgrade Process or the t_ISSU_Single-Step_Upgrade_Process_1150348.xml#task_1150348.

Loading Cisco IOS Software on the Standby RP

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

Before You Begin

- 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.
- Ensure that there is console access to both PREs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**issu loadversion***active-slot active-image**standby-slot standby-image* [**force** **Example:** `Router# issu loadversion a disk0:ubr10k2-k9p6u2-mz.new b stby-disk0:ubr10k2-k9p6u2-mz.new`	Starts the ISSU process. It may take several minutes after the **issu loadversion** command is entered for Cisco IOS software to load onto the standby RP and for the standby RP to transition to SSO mode.
Step 3	**show issu state** [**detail** **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process. At this point in the ISSU process, use this command to check that the standby RP is loaded and is in SSO mode. It may take several seconds after entering the **issu loadversion** command for Cisco IOS software to load onto the standby RP and the standby RP to transition to SSO mode. If you enter the **show issu state** command too soon, you may not see the information you need.

Switching to the Standby RP

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

Note Run the show redundancy states command to view the current redundancy status and make sure the system has reached SSO before executing the issu runversion command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**issu runversion active-slot-name [active-image-URL]** **Example:** `Router# issu runversion b stby-disk0:ubr10k2-k9p6u2-mz.new`	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image. The image URL is optional.

Stopping the RP 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 RP ISSU process and reverts to the original Cisco IOS software version if the next RP ISSU procedure is not performed prior to the rollback timer timeout. For example, the RP ISSU process would abort after the **issu acceptversion** command was entered only if the **issu runversion** command was not entered before rollback timeout.

Note Once you successfully stop the RP ISSU rollback timer using the **issu acceptversion** command, you can begin to execute the RLC ISSU process as applicable for redundant cable line cards on the Cisco uBR10012 Universal Broadband Router.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**issu acceptversion***active-slot-name* [*active-image-URL*] **Example:** `Router# issu acceptversion b disk0:ubr10k2-k9p6u2-mz.new`	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process. The image URL is optional.

Verifying the RP ISSU Software Installation

During the RP 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 theduring the ISSU process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show issu state** [**A** | **B** | **detail** **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process.
Step 3	**show redundancy**[**clients** | **config-sync** | **counters** | **force-rpr** | **history** | **idb-sync-history** | **interlink** | **linecard** | **platform** | **states** | **switchover**] **Example:** `Router# show redundancy`	Displays the current or historical status, mode, and related redundancy information about the device.

ISSU Single-Step Upgrade Process

You can upgrade the entire CMTS system by issuing the issu changeversion command. This command executes individual ISSU phases in the correct sequence automatically, and reduces the human effort involved in executing the other ISSU commands. The issu changeversion command upgrades the router processors first and then upgrades the line cards.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade may be deployed using the Single-Step Upgrade Process by issuing the **issu changeversion** command.

When the issu changeversion command is issued, it executes the functionality of the issu loadversion, issu runversion, issu acceptversion, issu linecard changeversion all and issu commitversion commands, without any user intervention required to navigate through each step of the single-step upgrade process.

The single-step upgrade process involves the following steps:

1. Run the issu changeversion command. This command invokes the issu loadversion command to reload the standby RP with the new Cisco IOS image.
2. The reload triggers the issu runversion command to switch over the RP from Active to Standby state to run the new Cisco IOS image.
3. After the two RPs reach the Stateful Switchover (SSO) mode, the single-step upgrade process resumes on the newly active RP with the new image to complete individual line card upgrades using the line card changeversion all command.
4. The single-step upgrade process on the active RP executes the issu commitversion command to complete the entire upgrade.

Note The issu changeversion command also upgrades the line card ISSU process. This command executes the linecard changeversion command before the issu commitverison command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu changeversion** *image to upgrade* **Example:** `Router# issu changeversion disk0:ubr10k4-k9p6u2-mz.122-33.SCC2`	Upgrades the CMTS system for a specific Cisco IOS image.

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.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process may be aborted by using the **issu abortversion** command.

Note Always abort the active RP in conjunction with the target Cisco IOS release.

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.

Beginning Cisco IOS Release 12.2(5th)SB, if the RP ISSU process is aborted on the Cisco uBR10012 universal broadband router using the **issu abortversion** command, or the RP is rolled back due to a switchover, the **issu linecard abortversion** command must also be executed. For more information, see the Manually Rolling Back a Software Upgrade Using RLC ISSU, on page 39.

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu abortversion** *slot image* **Example:** `Router# issu abortversion b disk0:ubr10k2-k9p6u2-mz.new`	Cancels the ISSU upgrade or downgrade process that is 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.

DETAILED STEPS

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

Displaying ISSU Compatibility Matrix Information

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

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu comp-matrix** {**negotiated** | **stored** **Example:** `Router# show issu comp-matrix`	Displays information regarding the ISSU compatibility matrix.

How to Perform the Redundant LC ISSU Process

Just as with RP ISSU, the RLC ISSU process is a series of steps performed while the router is in operation. The steps result in the implementation of a new or modified software image on a cable line card, and have minimal impact to traffic. The RLC ISSU process can be run automatically for certain cable line cards or globally for all cable line cards, or you can run the process manually for individual cable line cards.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the Redundant LC ISSU Process is optional while performing the RP-only ISSU Upgrade process. The Redundant LC ISSU Process need not be performed if the new image used for the upgrade is an RP-only ISSU Upgrade image.

Prerequisites for Performing the Redundant LC ISSU Process

- For the ISSU process to run on cable line cards, the cable line cards must be configured for N+1 redundancy.

For more information about configuring N+1 redundancy, refer to the "N+1 Redundancy for the Cisco Cable Modem Termination System" chapter of the Cisco CMTS Feature Guide at:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

Note For cable line cards that are not configured redundantly, you can manually load images using the **issu linecard reloadversion** command. However, this type of upgrade cannot be executed without affecting the network availability of the cable line card. For more information about how to do this, see the Reloading Non-Redundant Cable Line Cards, on page 40.

- Be sure that the following software image prerequisites are met:
  - The old and new versions of the RP and LC software images must be ISSU-capable and compatible. The LC software image is bundled with the RP image. For more information about software image compatibility for RLC ISSU, see the Compatibility Information for ISSU-uBR10K on the Cisco uBR10012 Universal Broadband Router, on page 19.
  - Both the original and target line card images need to be downloaded to disk or bootflash areas, but not necessarily on the same device. Because the image size is greater than 32MB, two images might not fit on a single flash device. You can put either image on disk0, disk1, or bootflash.
  - Verify that the system is configured to automatically boot the new image using the following global configuration command:

```
Router(config)# config-register 0x2
```

- Verify that the **boot system** global configuration command is configured for the path that specifies the location of the new target image, as shown in the following example:

```
Router(config)# boot system disk0:ubr10k2-k9p6u2-mz.new
```

- The following tasks must be run before the RLC ISSU process can begin:
  - Loading Cisco IOS Software on the Standby RP, on page 25 (required)
  - Switching to the Standby RP, on page 26 (required)
  - Stopping the RP ISSU Rollback Timer, on page 26 (required)
  - Verifying the RP ISSU Software Installation , on page 27 (required)

Once you verify that the active RP is in Run Version (RV state) after using the **issu acceptversion** command, you can begin the RLC ISSU process.

Restrictions for Performing the Redundant LC ISSU Process

The following list describes the restrictions for performing the RLC ISSU process:

- As with RP ISSU, it is recommended that upgrades be performed during a maintenance window.

- Any new features should not be enabled (if they require a change of configuration) during the RLC ISSU process.
- In a downgrade scenario, if any feature is not available in the downgrade revision of the line card software image, that feature should be disabled prior to initiating the RLC ISSU process.
- Do not run the **issu commitversion** command before performing the RLC ISSU process. The RLC ISSU process can not be executed if the RP is in the INIT state.
- N+1 fault protection is not disabled while the RLC ISSU process is in progress. However, the secondary (or protect) cable line card will not be available to provide redundancy services for a failing primary (or working) cable line card while the protect cable line card has become active for another working line card during the RLC ISSU process. Once the activated protect cable line card goes back to its standby state, it will again be available for redundant failover.

If a working line card fails during this period while the protect line card is unavailable, the working line card will reload with the software image that corresponds to the currently active RP. N+1 synchronization between the working and protect line cards is maintained.

- You cannot configure any line card redundancy commands or initiate any line card switchovers while an automatic or manual RLC ISSU process is in progress.
- The RLC ISSU process is not SSO capable. Therefore, the RLC ISSU process needs to be restarted on a newly active RP.
- Partial upgrades between RP and LC versions is not supported. Therefore, the RP and each LC should be upgraded to the same version. When you commit the new version using the **issu commitversion** command, both the RP and LC images are confirmed and enabled in the new standby RP card and protected cable line card.
- The RLC ISSU process does not support any configurable rollback timers. However, there are certain platform-dependent timeout values associated with the various stages of the RLC ISSU process within which the different stages are expected to complete. These timeout values apply to both the automated and manual execution of the RLC ISSU process. If a stage of the RLC ISSU process does not complete within the timeout period, an error results. An error message is produced and the RLC ISSU process is stopped.

The timeout values for the Cisco uBR10012 router are:

- ◦ Waiting for line cards to prepare for switchover—240 seconds. This timer begins when either **issu linecard prepareversion** or **issu linecard changeversion** commands are issued.
  - ◦ Switchover timer—240 seconds. This timer runs as part of the **issu linecard prepareversion** or **issu linecard changeversion** command to allow completion of the line card switchover.
  - ◦ **issu linecard loadversion** command—360 seconds. Time allowed for the Load Version stage to complete.
  - ◦ **issu linecard runversion** command—240 seconds. Time allowed for the Run Version stage to complete.
  - ◦ **issu linecard reloadversion** command—360 seconds. Time allowed for the Reload Version stage to complete.

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

- Use one of the following required methods to run the RLC ISSU process:
  - Running the RLC ISSU Process Automatically, on page 34 or
  - Running the RLC ISSU Process Manually, on page 35
- Verifying the RLC ISSU Software Installation, on page 37 (required)
- Forcing the RLC ISSU Process to Run , on page 39 (optional)
- Manually Rolling Back a Software Upgrade Using RLC ISSU, on page 39 (optional)
- Reloading Non-Redundant Cable Line Cards, on page 40 (optional)
- Finishing the ISSU Process to Enable the New Cisco IOS Software Version on the RP and Cable Line Cards, on page 41 (required)

Running the RLC ISSU Process Automatically

When you run the RLC ISSU process automatically using the **issu linecard changeversion** command, you can specify running the process for all redundant cable line cards, or for specified working cable line cards.

If you want to force the RLC ISSU process regardless of the image version status, or you want to ignore any potential service outage and error handling, use the **issu linecard changeversion forced** form of the command.

You can also use the **issu linecard changeversion** command to restart the RLC ISSU process if you previously used the **issu linecard process stop** command.

Note If you include any non-redundant cable line cards as part of the automatic RLC ISSU process, please run the **issu linecard reloadversion** command for the non-redundant line card. For more information, see the Reloading Non-Redundant Cable Line Cards, on page 40.

Once the automatic RLC ISSU process is complete, you need to verify the installation and commit the RP and LC images. The following sections describe these tasks:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard changeversion all** | *slot_1 /subslot_1*]. . .[*slot_n*/*subslot_n*]} [**forced** **Example:** `Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1`	Starts the ISSU process to run all stages automatically for the specified cable line cards. **Note** It is preferred to use the all *option.*

Stopping the Automatic RLC ISSU Process

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

You can stop the automatic RLC ISSU process if you want to interrupt the process from continuing for the next cable line card that is configured for RLC ISSU.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard process stop** **Example:** `Router# issu linecard process stop`	Stops the automatic RLC ISSU process from continuing for the next specified cable line card.

Running the RLC ISSU Process Manually

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

Once you accept the RLC ISSU process, you can begin the manual RLC ISSU process for another cable line card. If you have completed the RLC ISSU process, then you need to verify the installation and commit the RP and LC images. The following sections describe these tasks:

The following sections explain optional tasks that you can perform as part of the manual RLC ISSU process:

Manually Switching the Primary Working Cable Line Card to Standby

To begin the RLC ISSU process manually, use the **issu linecard prepareversion** command and specify the slot/subslot location of the primary working cable line card. When you enter this command, the redundant configuration and image version of the cable line card are checked. If the image version needs to be changed, then a switchover occurs placing the primary working cable line card in standby mode, and activating the protect cable line card.

If you want to force the switchover regardless of the image version status, or you want to ignore any potential service outage and error handling, use the **issu linecard prepareversion forced** form of the command.

You can also use the **issu linecard prepareversion** command to restart the RLC ISSU process if you previously used the **issu linecard process stop** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard prepareversion** *slot*/*subslot* [**forced** **Example:** `Router# issu linecard prepareversion 6/0`	Manually starts the ISSU process for the specified working cable line card. During this stage the working cable line card switches to standby, and the protect cable line card becomes active.

Manually Loading the New Image on the Primary Line Card in Standby

To load the new target line card image on the specified working cable line card that is currently in standby mode as part of the manual RLC ISSU process, use the **issu linecard loadversion** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard loadversion** *slot* / *subslot* **Example:** `Router# issu linecard loadversion 6/0`	Loads the new target line card image on the specified working cable line card.
Step 3	**show hccp brief** **Example:** `Router# show hccp brief`	Displays summary information about the N+1 line card redundancy configuration.

Manually Switching to the Standby Cable Line Card

To initiate an N+1 switchover to the current standby cable line card (the original working primary cable line card) as part of the manual RLC ISSU process, use the **issu linecard runversion** command. During this stage,

the primary working cable line card becomes active (with the new target image) for all of the interfaces on the secondary protect cable line card. A 3-second rollback timer for the primary working cable line card is started.

If you want to force the switchover regardless of any image version incompatibility, or you want to ignore any potential service outage and error handling, use the **issu linecard runversion forced** form of the command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard runversion** *slot* /*subslot* [**forced**] **Example:** `Router# issu linecard runversion 6/0`	Starts a switchover to the current standby cable line card.

Accepting the RLC ISSU Process

To mark completion of and accept the Prepare Version, Load Version, and Run Version stages of the RLC ISSU process, use the **issu linecard acceptversion** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard acceptversion** *slot* / *subslot* **Example:** `Router# issu linecard acceptversion 6/0`	Stops the RLC ISSU rollback timer.

Verifying the RLC ISSU Software Installation

During the RLC ISSU process, there are many different valid states. Use the show issu linecard state command display these line card states:

- PSLC READY state—Waiting for the protect (or secondary) line card to become ready for line card switchover.
- PREPAREVERSION state—Waiting for the line card switchover from working (primary) to protect (secondary) to complete.
- LOADVERSION state—Waiting for the original working/primary line card to finish loading the new image, and become standby-ready for the secondary line card.
- RUNVERSION state—Waiting for completion of the line card switchover to reactivate the original working/primary line card with the new image.
- ACCEPTVERSION state—Transient state for performing Accept Version stage of process.
- RELOAD state—Completed manual execution of the **issu linecard reloadversion** command.
- SINGLE OP PV DONE state—Completed manual execution of the **issu linecard prepareversion** command.
- SINGLE OP LV DONE state—Completed manual execution of the **issu linecard loadversion** command.
- SINGLE OP RV DONE state—Completed manual execution of the **issu linecard runversion** command.

You can also use some other **show** commands to display the status of the N+1 redundancy configuration and the status of the RP ISSU process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu state**[slot / port] [**detail**] **Example:** `Router# show issu state`	Displays the state of theduring the ISSU process.
Step 3	**show issu linecard state** | **history** **Example:** `Router# show issu state`	Displays the state of theduring the RLC ISSU process.
Step 4	**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.

	Command or Action	Purpose
Step 5	**show hccp brief** **Example:** `Router# show hccp brief`	Displays summary information about the N+1 line card redundancy configuration.

Forcing the RLC ISSU Process to Run

You can configure the automatic RLC ISSU process, or certain stages of the manual RLC ISSU process to continue processing regardless of any potential service outage and subsequent error handling, by using the **forced** keyword option on the corresponding commands.

For more information, see the following topics:

Manually Rolling Back a Software Upgrade Using RLC ISSU

If you determine that the system running the new software image does not function as expected, you can configure the RLC ISSU process to roll back all cable line cards or certain cable line cards to the previous version using the **issu linecard abortversion** command.

If you want to force the abort process and ignore any potential service outage and error handling, use the **issu linecard abortversion forced** form of the command.

Note If the RP ISSU process is aborted using the **issu abortversion** command, or the RP is rolled back due to a switchover, the **issu linecard abortversion** command must also be used.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard abortversion** {**all** | *slot*/*subslot*} [**forced**] **Example:** `Router# issu linecard abortversion 6/0`	Cancels the RLC ISSU operation and reloads the cable line card with the original version of the line card image prior to the RLC ISSU process.

Reloading Non-Redundant Cable Line Cards

To load a new target line card image on a cable line card that is not configured redundantly, use the **issu linecard reloadversion** command.

Caution While executing, the **issu linecard reloadversion** command will disrupt network services for the specified non-redundant cable line card.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**issu linecard reloadversion** {*original-image* | *target-image*} {**all** | *slot_1*[/*subslot_1*]. . .[*slot_n*[/*subslot_n*] **Example:** `Router# issu linecard reloadversion disk0:ubr10k2-k9p6u2-mz.new 6/0`	Loads the new target line card image on the specified working cable line card.

Stopping a Manual RLC ISSU Process

Note Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

To manually stop any RLC ISSU operation, use the **issu linecard process stop** command.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**issu linecard process stop** **Example:** `Router# issu linecard process stop`	Stops the current RLC ISSU operation.

Restarting a Stopped RLC ISSU Process

If you have previously stopped an RLC ISSU operation using the **issu linecard process stop** command, you can restart the process using either the **issu linecard changeversion** or **issu linecard prepareversion** commands.

The RLC ISSU process will restart at the next logical ISSU operation to be performed depending on the current state of the system.

For more information about how to use these commands, see the Running the RLC ISSU Process Automatically, on page 34 or the Manually Switching the Primary Working Cable Line Card to Standby, on page 35.

Finishing the ISSU Process to Enable the New Cisco IOS Software Version on the RP and Cable Line Cards

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.

Beginning in Cisco IOS Release 12.2(5th)SB on the Cisco uBR10012 Universal Broadband Router, the **issu commitversion** command is used to confirm both the new RP and new LC images that were upgraded using the RLC ISSU process.

Note The **issu commitversion** command can be executed only when all of the primary cable line cards are upgraded to the latest target image, either by **issu linecard changeversion** command, or **issu linecard reloadversion** command or by system reset.

Note Effective with Cisco IOS Release 12.2(33)SCH2, the **issu commitversion** command is must be used for completing the RP-only ISSU Upgrade process.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**issu commitversion standby-slot-name** [**standby-image-url**] **Example:** `Router# issu commitversion a stby-disk0:ubr10k2-k9p6u2-mz.new`	Allows the new Cisco IOS software image to be loaded into the standby RP.

Configuration Examples for Performing ISSU

This section contains the following configuration examples:

Note The examples provided in the RP ISSU process sections of this document reflect certain Cisco 10000 Series Router software image names. Be aware when referring to these examples that you must replace these sample image names with the appropriate supported image name for your platform.

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 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
Redundancy State              = SSO
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 45
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
Router# show redundancy
```

```
Redundant System Information :
------------------------------
       Available system uptime = 18 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 = 17 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower
NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                         BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                        BOOTLDR =
        Configuration register = 0x2

Peer Processor Information :
----------------------------
              Standby Location = slot B
        Current Software state = STANDBY HOT
       Uptime in current state = 16 minutes
                 Image Version = Cisco IOS Software, 10000 Software (UBR10K2-K9P6U2-M),
Version 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower
NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                         BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                        BOOTLDR =
        Configuration register = 0x2
```

Example: Verifying the ISSU State

The following example provides information about the ISSU state:

```
Router# show issu state detail

                         Slot = A
                    RP State = Active
                   ISSU State = Init
                  Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
                 Variable Store = PrstVbl
                         Slot = B
                    RP State = Standby
                   ISSU State = Init
                  Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                 Operating Mode = SSO
                Primary Version = N/A
              Secondary Version = N/A
                Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
Slot Red Role  Peer Act/Sby  Image Match RP LC ISSU State      ISSU Proc
---- --------- ---- -------- -------------- ------------------ ----------
5/0  Secondary -    standby  Yes            -                  -
6/0  Primary   5/0  active   Yes            -                  -
```

```
7/0  Primary   5/0  active   Yes            -                 -
8/0  Primary   5/0  active   Yes            -                 -
PRE is the new active: FALSE
Waiting for MDR:  FALSE
No Transitional Line Card State information registered.
No Peer Line Card State information registered.
Peer Line Card Action:
-------Card Type-------- -----Action------ --Slots---
24rfchannel-spa-1        NO ACTION         0x00000004
4jacket-1                NO ACTION         0x00000004
2cable-dtcc              NO ACTION         0x00000028
1gigethernet-hh-1        NO ACTION         0x00000200
```

The new version of the Cisco IOS software must be present on both of the RPs. The initial bootflash directory examples show the presence of the old image, and the disk0 directory information shows that the new version is present on both disks.

```
Directory of bootflash:/

    1  -rw-     2530312   Jan 1 2000 01:42:10 +00:00  c10k2-eboot-mz.122-16.BX
    2  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.old

Directory of stby-bootflash:/

    1  -rw-     2530312   Jan 1 2000 01:42:10 +00:00  c10k2-eboot-mz.122-16.BX
    2  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.old

Directory of disk0:/

    1  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.new

Directory of stby-disk0:/

    1  -rw-    35530056   May 9 2007 17:11:42 +00:00  ubr10k2-k9p6u2-mz.new
```

Examples for Performing the RP ISSU Process

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

Example: Initiating the RP ISSU Process

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

```
Router# issu loadversion a disk0:ubr10k2-k9p6u2-mz.new b stby-disk0:ubr10k2-k9p6u2-mz.new
```

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 = bootflash:ubr10k2-k9p6u2-mz.old,12;
                          Slot = B
                     RP State = Standby
                    ISSU State = Load Version
                 Boot Variable =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
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
```

Example: 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 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:ubr10k2-k9p6u2-mz.new
```

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 (UBR10K2-K9P6U2-M), Version
 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                         BOOT =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
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 (UBR10K2-K9P6U2-M), Version
 12.2(nightly.BEMR070507) NIGHTLY BUILD, synced to mayflower NIGHTLY_MAYFLOWER_041607_0143
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 08-May-07 01:23 by torowe
                         BOOT = bootflash:ubr10k2-k9p6u2-mz.old,12;
                    CONFIG_FILE =
                      BOOTLDR =
        Configuration register = 0x2
Router# show issu state
                           Slot = B
                       RP State = Active
                     ISSU State = Run Version
                  Boot Variable =
disk0:ubr10k2-k9p6u2-mz.new,12;bootflash:ubr10k2-k9p6u2-mz.old,12;
                           Slot = A
                       RP State = Standby
```

```
                  ISSU State = Run Version
                Boot Variable = bootflash:ubr10k2-k9p6u2-mz.old,12;
```

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.

Example: Stopping the RP 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 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:
ubr10k2-k9p6u2-mz.new
```

Example: Committing the New Software to the Standby RP

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:
ubr10k2-k9p6u2-mz.new
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 (UBR10K2-K9P6U2-M),
Version 12.2(nightly.CISCO070530) NIGHTLY BUILD, synced to V122_32_8_23_SBK
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 30-May-07 02:02 by torowe
                     BOOT = disk0:ubr10k2-k9p6u2-mz.new,12;
                   CONFIG_FILE =
                     BOOTLDR =
       Configuration register = 0x2
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 (UBR10K2-K9P6U2-M),
Version 12.2(nightly.CISCO070530) NIGHTLY BUILD, synced to V122_32_8_23_SBK
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 30-May-07 02:02 by torowe
                     BOOT = disk0:ubr10k2-k9p6u2-mz.new,12;
                   CONFIG_FILE =
                     BOOTLDR =
       Configuration register = 0x2
Router# show issu state
                         Slot = B
                   RP State = Active
                 ISSU State = Init
            Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

                         Slot = A
                   RP State = Standby
                 ISSU State = Init
            Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;
Router# show issu state detail
                         Slot = B
                   RP State = Active
                 ISSU State = Init
            Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

             Operating Mode = SSO
            Primary Version = N/A
          Secondary Version = N/A
            Current Version = disk0:ubr10k2-k9p6u2-mz.new
                         Slot = A
                   RP State = Standby
                 ISSU State = Init
            Boot Variable = disk0:ubr10k2-k9p6u2-mz.new,12;disk0:ubr10k2-k9p6u2-mz.new,1;

             Operating Mode = SSO
            Primary Version = N/A
          Secondary Version = N/A
            Current Version = disk0:ubr10k2-k9p6u2-mz.new
```

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.

Example: Aborting the RP ISSU Process

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

```
Router# issu abortversion b disk0:ubr10k2-k9p6u2-mz.new
```

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.

Example: Verifying RP Rollback Timer Information

To display rollback timer information for the RP ISSU process, 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
```

Example: Verifying the ISSU Single Step Upgrade

The following example provides information about the state and current version of the RPs including the Single Step Upgrade process.

```
Router# show issu state detail

                         Slot = A
                    RP State = Active
                   ISSU State = Init
                 Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                Operating Mode = SSO
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
                Variable Store = PrstVbl
                         Slot = B
                    RP State = Standby
                   ISSU State = Init
                 Boot Variable = disk0:ubr10k4-k9p6u2-mz.122SC_20100329,12;
                Operating Mode = SSO
               Primary Version = N/A
             Secondary Version = N/A
               Current Version = disk0:ubr10k4-k9p6u2-mz.122SC_20100329
Slot Red Role  Peer Act/Sby  Image Match RP LC ISSU State      ISSU Proc
---- --------- ---- -------- -------------- ------------------ ---------
5/0  Secondary -    standby  Yes            -                  -
6/0  Primary   5/0  active   Yes            -                  -
7/0  Primary   5/0  active   Yes            -                  -
8/0  Primary   5/0  active   Yes            -                  -
PRE is the new active: FALSE
Waiting for MDR:  FALSE
No Transitional Line Card State information registered.
No Peer Line Card State information registered.
Peer Line Card Action:
-------Card Type-------- -----Action------ --Slots---
24rfchannel-spa-1        NO ACTION         0x00000004
4jacket-1                NO ACTION         0x00000004
2cable-dtcc              NO ACTION         0x00000028
1gigethernet-hh-1        NO ACTION         0x00000200
```

Configuration Examples for Performing RLC ISSU

This section provides configuration examples for the RLC ISSU process. It includes the following sections:

Configuration Examples for the Automatic RLC ISSU Process

This section provides the following configuration examples:

Example: Initiating the RLC ISSU Process for all Cable Line Cards

The following example shows how to initiate the RLC ISSU process automatically for all cable line cards in a redundant configuration:

```
Router> enable
Router# issu linecard changeversion all
```

Example: Initiating the RLC ISSU Process for Specific Cable Line Cards

The following example shows how to initiate the RLC ISSU process automatically for certain working cable line cards in a redundant configuration:

```
Router> enable
Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1
```

Example: Stopping the Automatic RLC ISSU Process

The following example shows how to stop the automatic RLC ISSU process in between the ISSU process for each configured cable line card:

```
Router# issu linecard changeversion stop
```

Example: Forcing an Automatic RLC ISSU Process

The following example shows how to force the automatic RLC ISSU process and ignore any error processing:

```
Router> enable
Router# issu linecard changeversion 6/0 6/1 7/1 8/0 8/1 forced
```

or, alternatively:

```
Router> enable
Router# issu linecard changeversion all forced
```

Configuration Examples for the Manual RLC Process

Example: Performing the RLC ISSU Process Manually

The following example shows how to run the complete RLC ISSU process manually for a specified working cable line card installed in slot 6 and subslot 0 of the Cisco uBR10012 router:

```
Router> enable
Router# issu linecard prepareversion 6/0
Router# issu linecard loadversion 6/0
Router# issu linecard runversion 6/0
Router# issu linecard acceptversion 6/0
Router# issu commitversion a disk0:ubr10k2-k9p6u2-mz.new
```

Example: Manually Rolling Back a Software Upgrade Using RLC ISSU

The following example shows how to manually roll back the line card software image to the original version:

```
Router# issu linecard abortversion 6/0
```

Example: Reloading Non-Redundant Cable Line Cards

The following example shows how to load a software image for a specific cable line card that is not configured redundantly:

```
Router# issu linecard reloadversion disk0:ubr10k2-k9p6u2-mz.new 6/0
```

Example: Stopping a Manual RLC ISSU Process

The following example shows how to stop any manual RLC ISSU operation:

```
Router# issu linecard process stop
```

Additional References

The following sections provide references related to performing ISSU.

Related Documents

Related Topic	Document Title
Performing ISSU	*Cisco IOS Software: Guide to Performing In-Service Software Upgrades*
Information about Cisco Nonstop Forwarding	*Cisco Nonstop Forwarding* http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnsf20s.html
Information about stateful switchover	*Stateful Switchover* http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html
ISSU and MPLS clients	ISSU MPLS Clients
Information about N+1 line card redundancy	"N+1 Redundancy for the Cisco Cable Modem Termination System" chapter of the Cisco CMTS Feature Guide http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

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/cisco/web/support/index.html

Feature Information for ISSU

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

Note The below 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.

Table 2: Feature Information for ISSU

Feature Name	Releases	Feature Information
	12.2(5th)SB	Support for the ISSU-uBR10K feature was introduced on the Cisco uBR10012 Universal Broadband Router with the Performance Routing Engine 2.
	12.2(31)SB2	Support for the following new features were added to the 12.2(31)SB2 release: • ISSU - Dynamic Host Configuration Protocol (DHCP) on-demand address pool (ODAP) client/server • ISSU - DHCP proxy client • ISSU - DHCP relay on unnumbered interface • ISSU - DHCP server • ISSU - First Hop Routing Protocol (FHRP) - Gateway Load Balancing Protocol (GLBP) • ISSU - Intermediate System-to-Intermediate System (IS-IS) • ISSU - Quality of Service (QoS)

Feature Name	Releases	Feature Information
	12.2(31)SGA	Support for ISSU was introduced on the Cisco Catalyst 4500 series platform. Support for the following new features was added on the Cisco Catalyst 4500 series platform: • Dynamic Host Configuration Protocol (DHCP) snooping • EtherChannel - Port Aggregation Protocol (PagP) and Link Aggregate Control Protocol (LACP) • IEEE 802.1x protocol • IEEE 802.3 • Internet Group Management Protocol (IGMP) snooping • IP Host • Port security • Spanning-Tree Protocol (STP) The following commands were introduced or modified: **configure issu set rollback timer**, **issu abortversion**, **issu acceptversion**, **issu commitversion**, **issu load version**, **issu runversion**, **show issu comp-matrix**, **show issu state**.
	12.2(28)SB	This feature was introduced.

Feature Name	Releases	Feature Information
ISSU	12.2(33)SCB	Support for the following new features were added to this release. • ISSU Compatibility Matrix • Minimal Disruptive Restart (MDR) and the Cisco Wideband SPA • Cable ISSU Clients • Support for Performance Routing Engine 4 • Support for 10000-SIP-600 (4-bay Cisco 10000 SPA jacket card) • Support for Wideband SPA • ISSU Time Enhancement The following commands were introduced or modified: **issu linecard abortversion**, **issu linecard acceptversion**, **issu linecard changeversion**, **issu linecard loadversion**, **issu linecard prepareversion**, **issu linecard reloadversion**, **issu linecard runversion**.
ISSU	12.2(33)SCB3	A general prerequisite for Cisco uBR10012 router was added. The following commands were introduced or modified: **show processes cpu**, **show controllers cable [proc-cpu]**.
Single Step Upgrade Process	12.2(33)SCD2	This feature was introduced on the Cisco CMTS routers to perform a single-step complete ISSU upgrade process cycle using the new issu changeversion command.
ISSU	12.2(33)SCG	Starting Cisco IOS Release 12.2(33)SCG, the **issu linecard process stop** command is *not* supported on the Cisco CMTS router.

Feature Name	Releases	Feature Information
RP-only ISSU Upgrade	12.2(33)SCH2	Effective with Cisco IOS Release 12.2(33)SCH2, the RP-only ISSU Upgrade process supports the upgrade of only the RP images without upgrading the line card images.