Cisco CMTS High Availability Features Configuration Guide

First Published: December 17, 2008

Last Modified: February 14, 2014

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

Text Part Number: OL-27607-03

CONTENTS

CHAPTER 1

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	Cisco IOS Release 12.2(33)SCA and later
	- PRE2	- Cisco uBR10-MC5X20S/U/H
	Cisco IOS Release 12.2(33)SCB and later	Cisco IOS Release 12.2(33)SCC and later
	- PRE4	- Cisco UBR-MC20X20V
	Cisco IOS Release 12.2(33)SCH and later	Cisco IOS Release 12.2(33)SCE and later
	- PRE5	- 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:

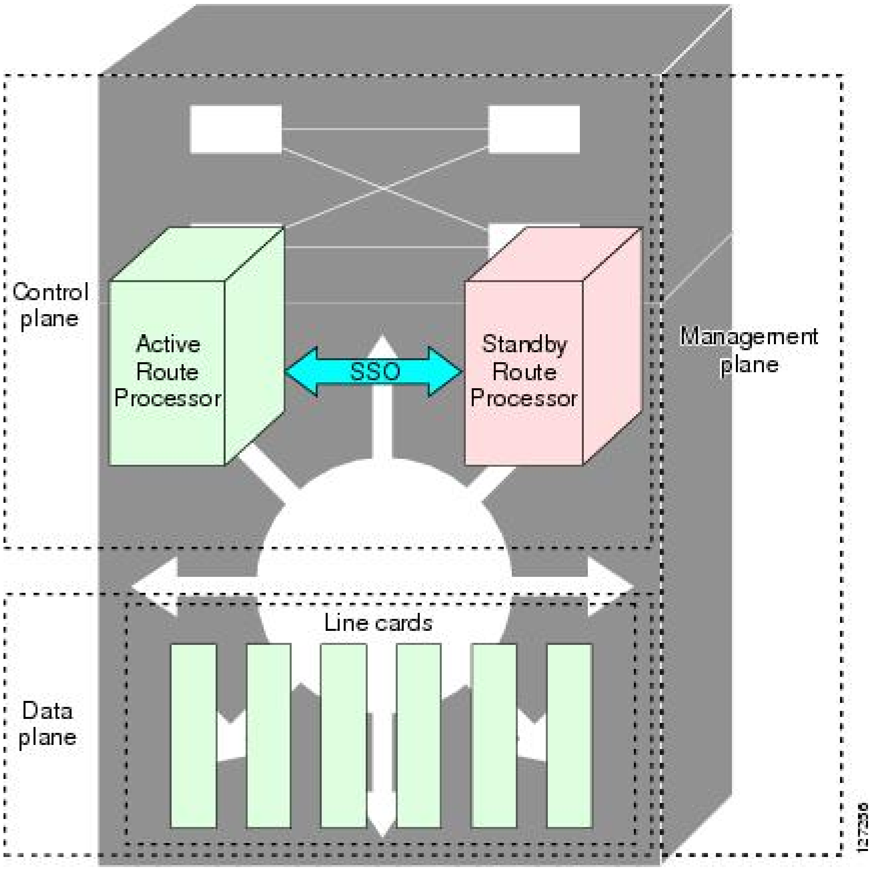
1. The RP-only ISSU Upgrade may be done using the ISSU Multi-Step Upgrade Process, page 24 or the ISSU Single-Step Upgrade Process, page 29.
2. 2.If the Multi-Step Upgrade process is used, the Redudndant LC ISSU process may be performed using the Running the RLC ISSU Process Automatically, page 36. The 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.

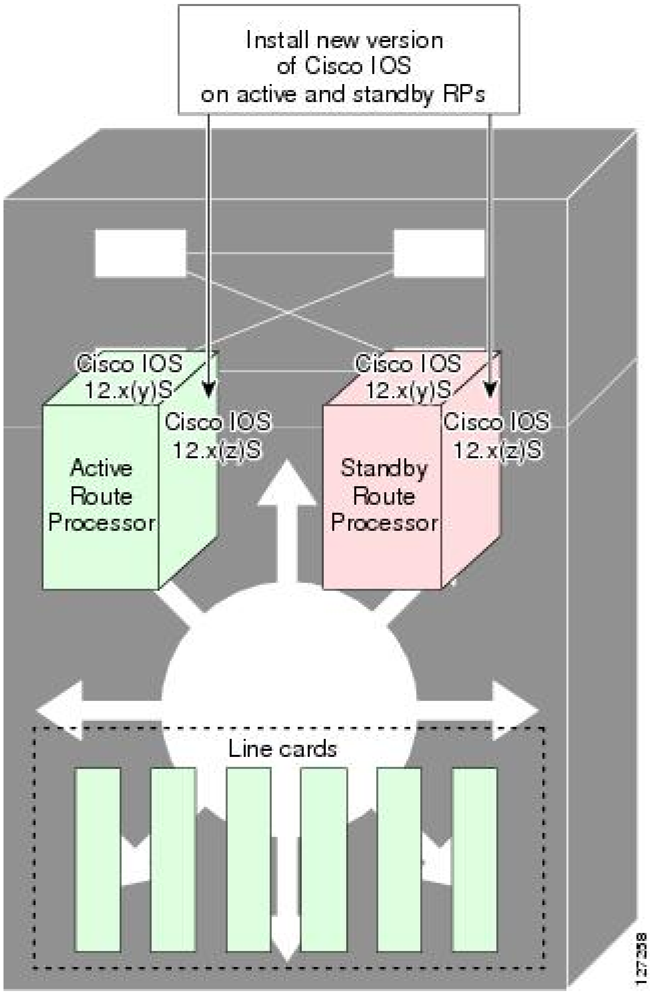
SSO mode supports configuration synchronization. When images on the active and standby RPs are different, this feature allows the two RPs to be kept in synchronization although they may support different sets of commands.

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



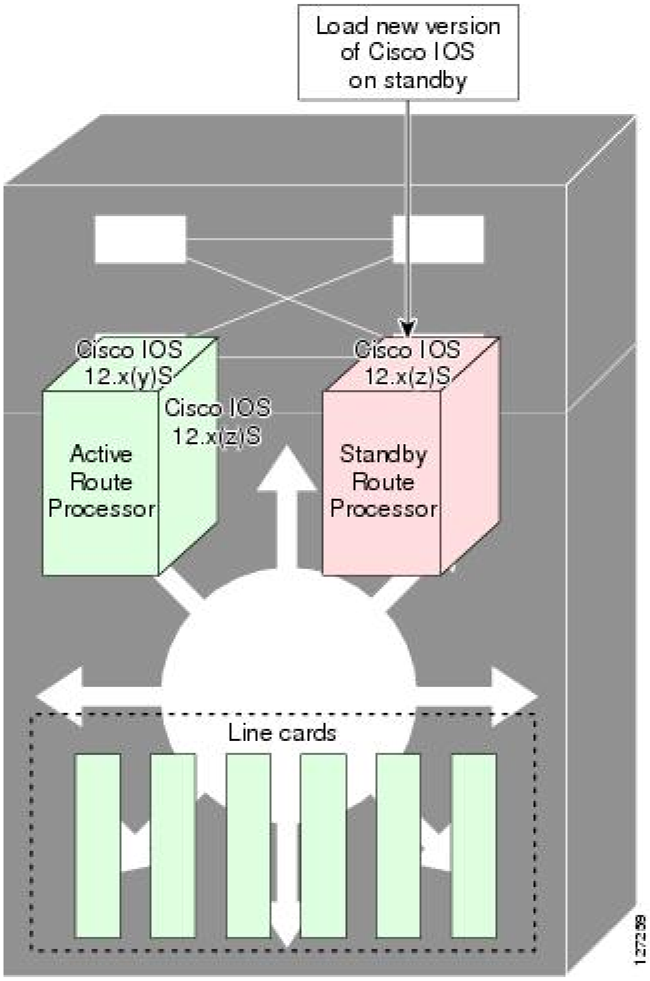
An ISSU-capable router consists of two RPs (active and standby) and one or more line cards. Before initiating the ISSU process, copy the Cisco IOS software into the file systems of both RPs (see Figure below).

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



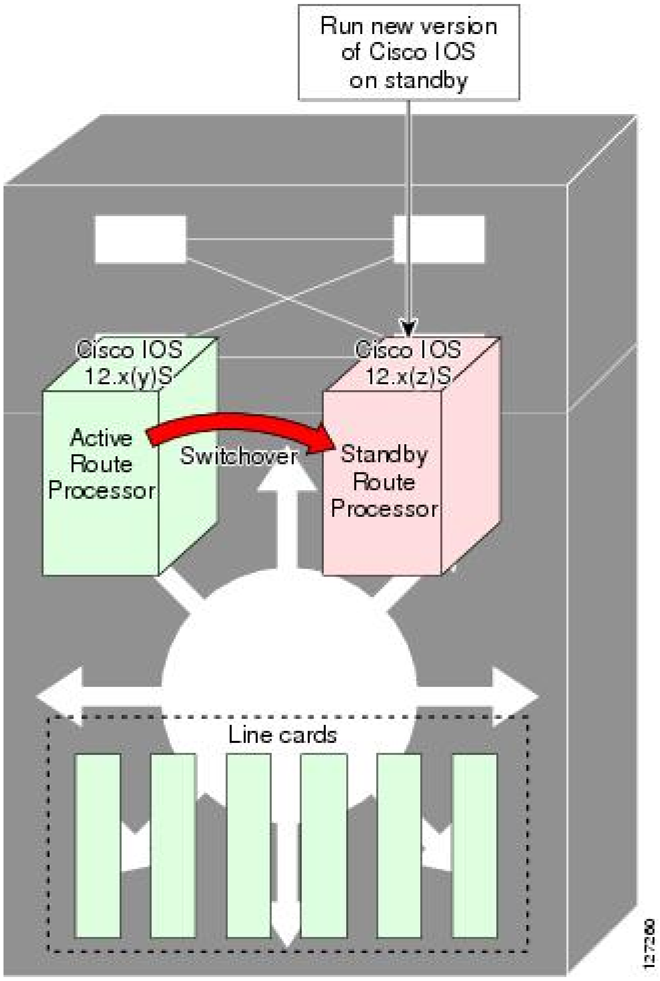
After you have copied the Cisco IOS software to both file systems, load the new version of Cisco IOS software onto the standby RP (see Figure below).

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



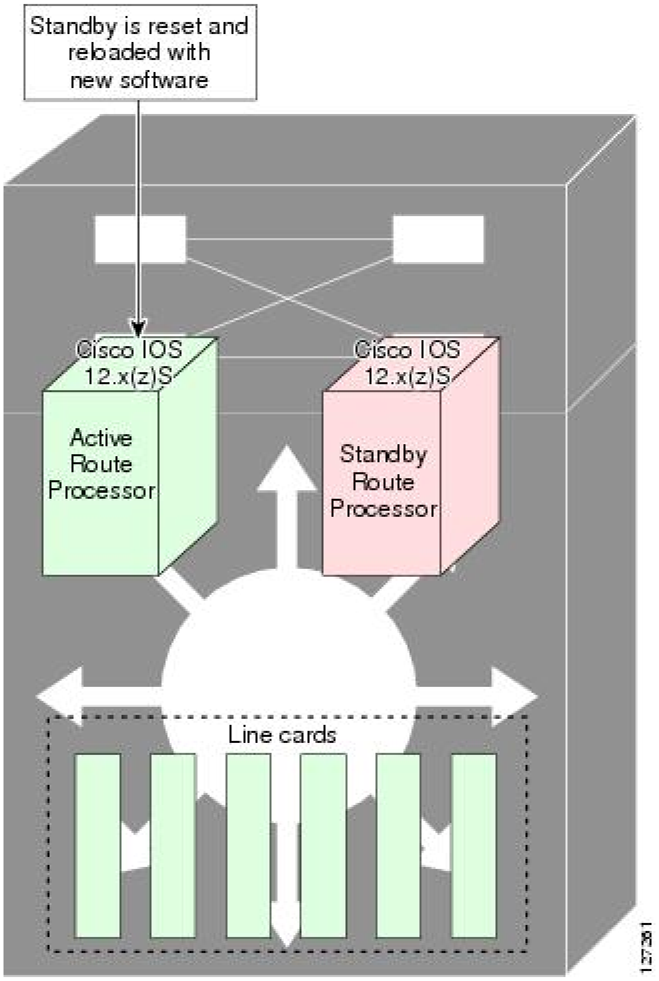
After switchover, the standby RP takes over as the new active RP (see Figure below).

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

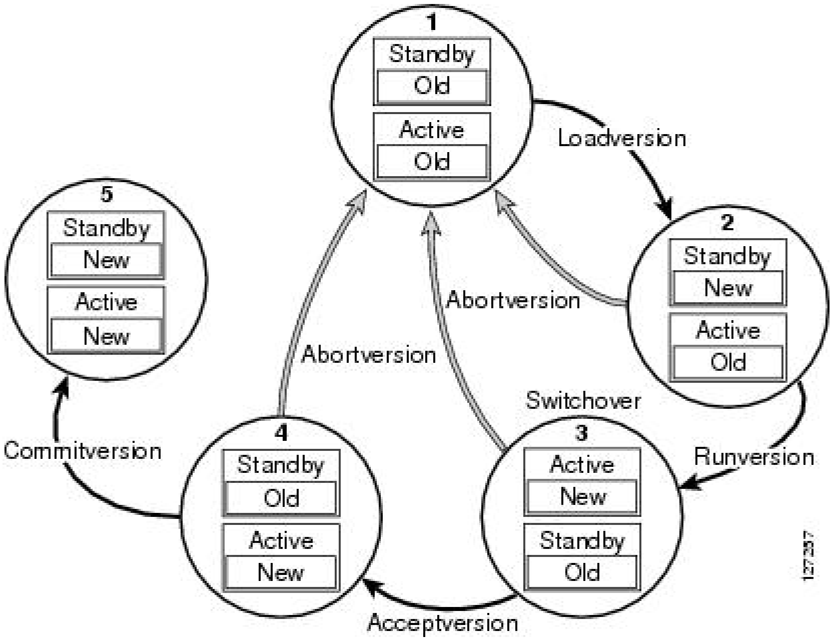


The two RPs in a system can be in one of three different states during ISSU:

- 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.

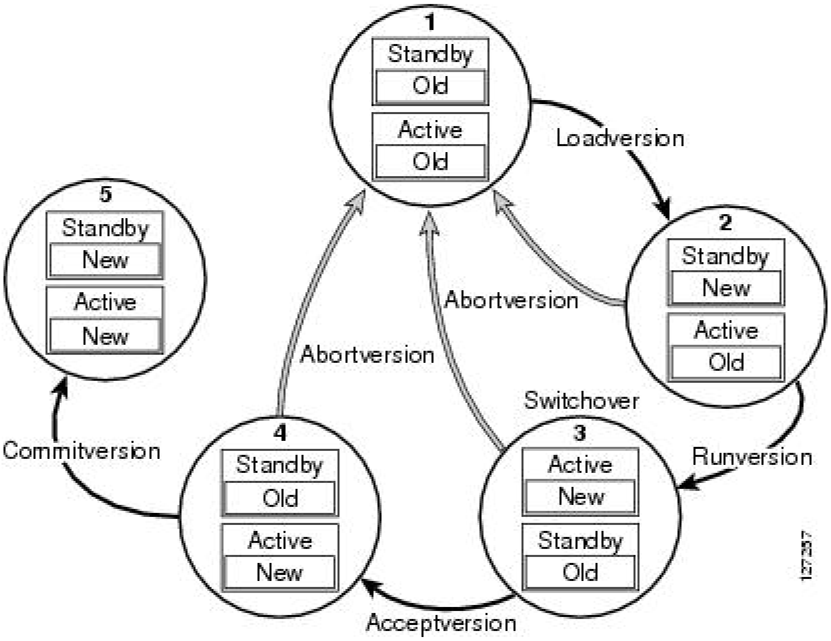
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

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.

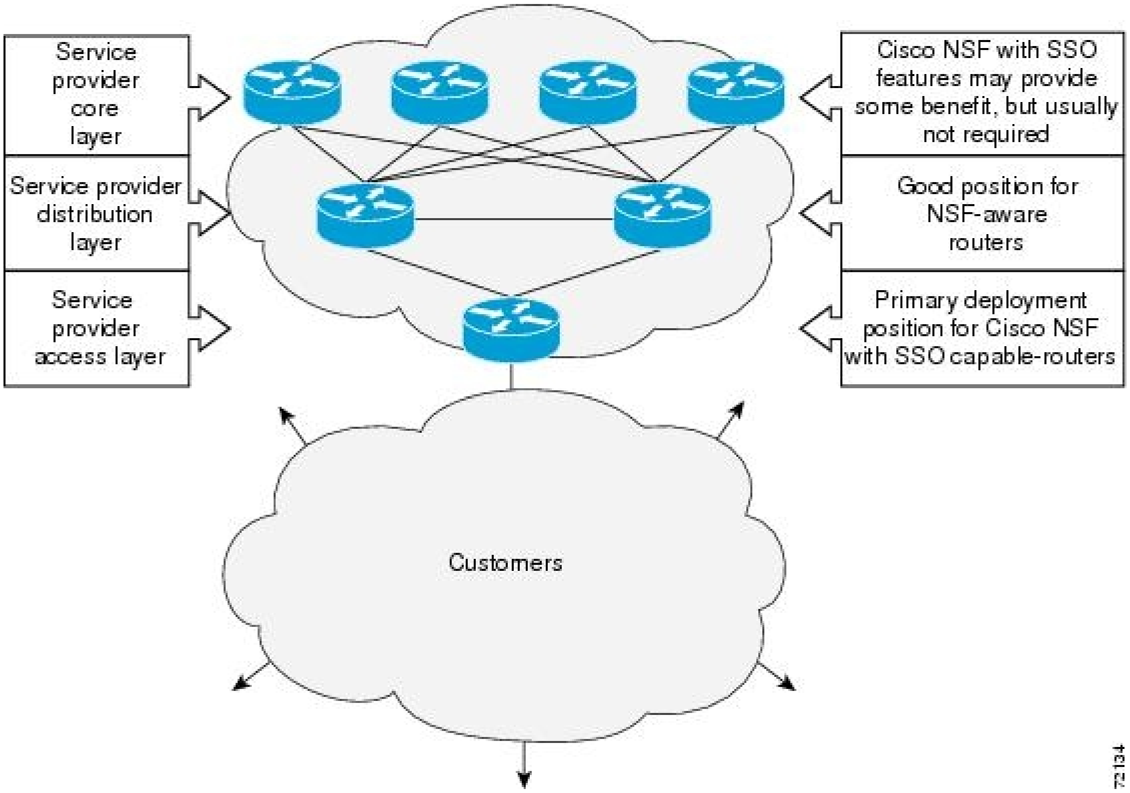
For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco NSF-aware software images must be installed on those neighboring distribution layer devices. Depending on your objectives, you may decide to deploy Cisco NSF and SSO features at the core layer of your network. 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


Service provider core layer
Service provider distribution layer
Service provider access layer
Cisco NSF with SSO features may provide some benefit, but usually not required
Good position for NSF-aware routers
Primary deployment position for Cisco NSF with SSO capable-routers
Customers
72134

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.

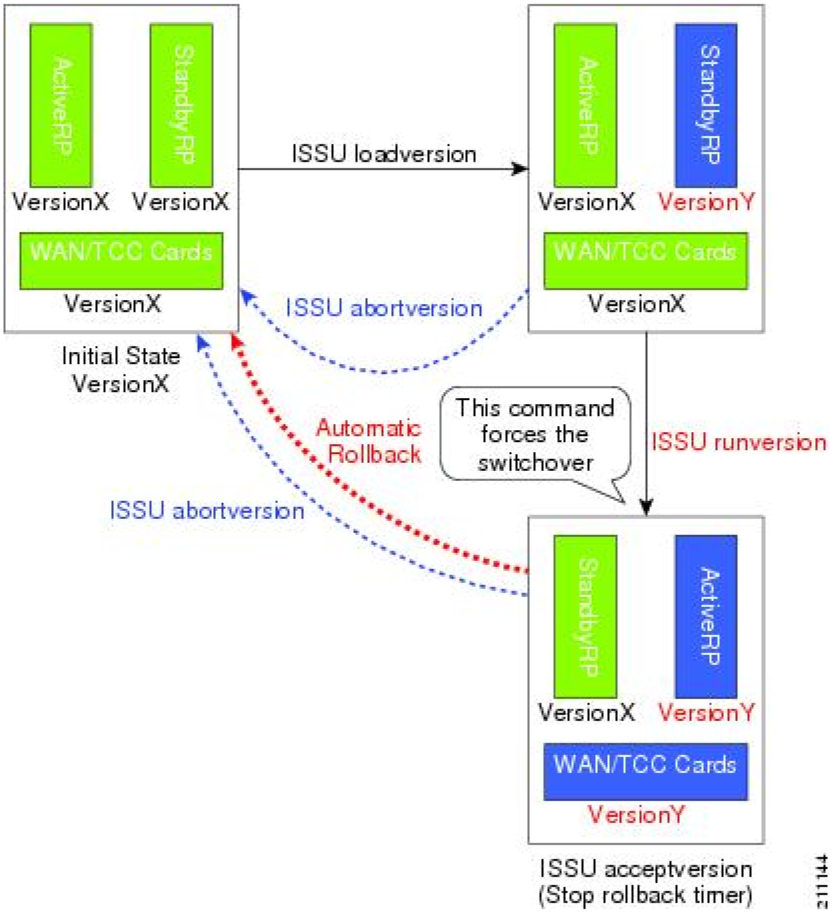
Redundant LC ISSU Process Overview

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.

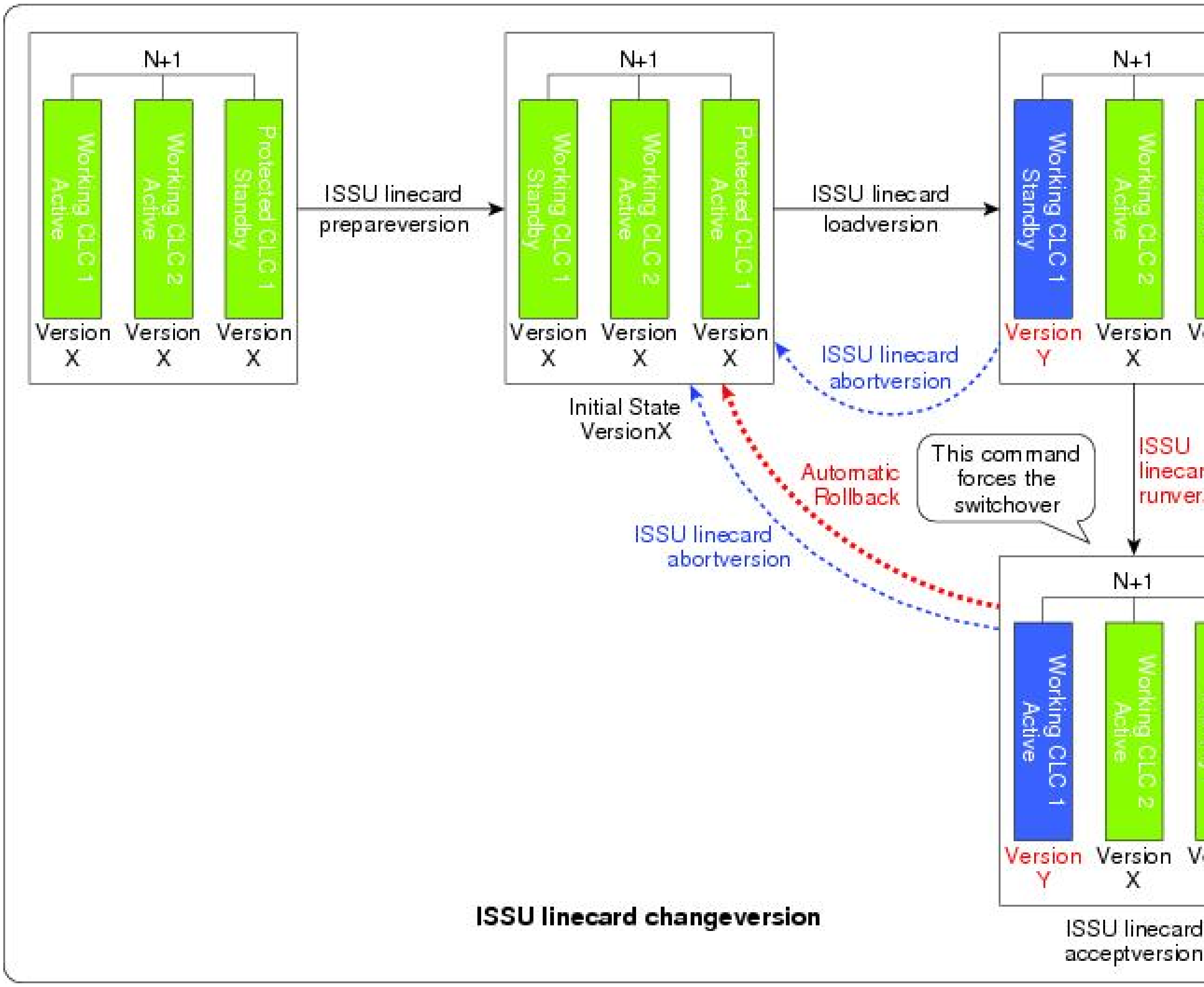
The RLC ISSU process has some dependencies with the RP ISSU process. First, the RLC ISSU process can be started only when the RP ISSU process reaches the Run Version (RV) state. In the RV state, the RP rollback timer is stopped (via the **issu acceptversion** command) and the active RP is running the 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

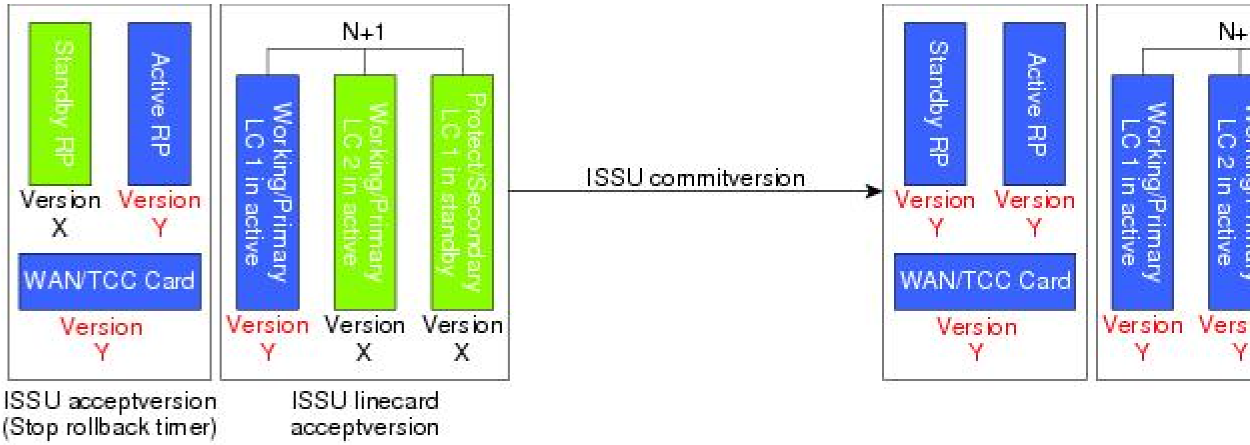


The RLC ISSU process runs serially for each targeted cable line card. A subsequent cable line card may start the process when the previous cable line card's RLC ISSU process is complete. This process is different from the ISSU process for other line cards supporting MDR, which reloads simultaneously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

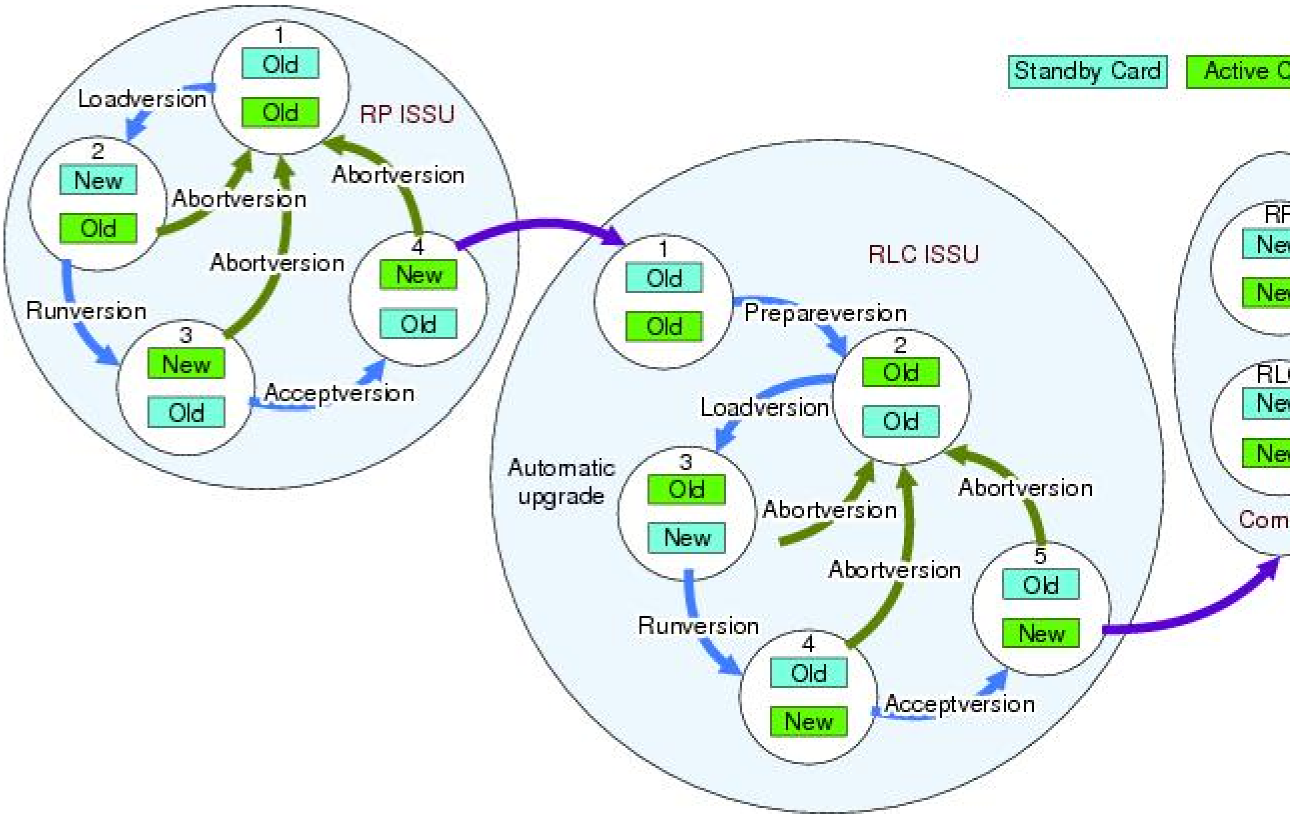
Figure 11: Combined RP and RLC ISSU Commit Version Stage



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:

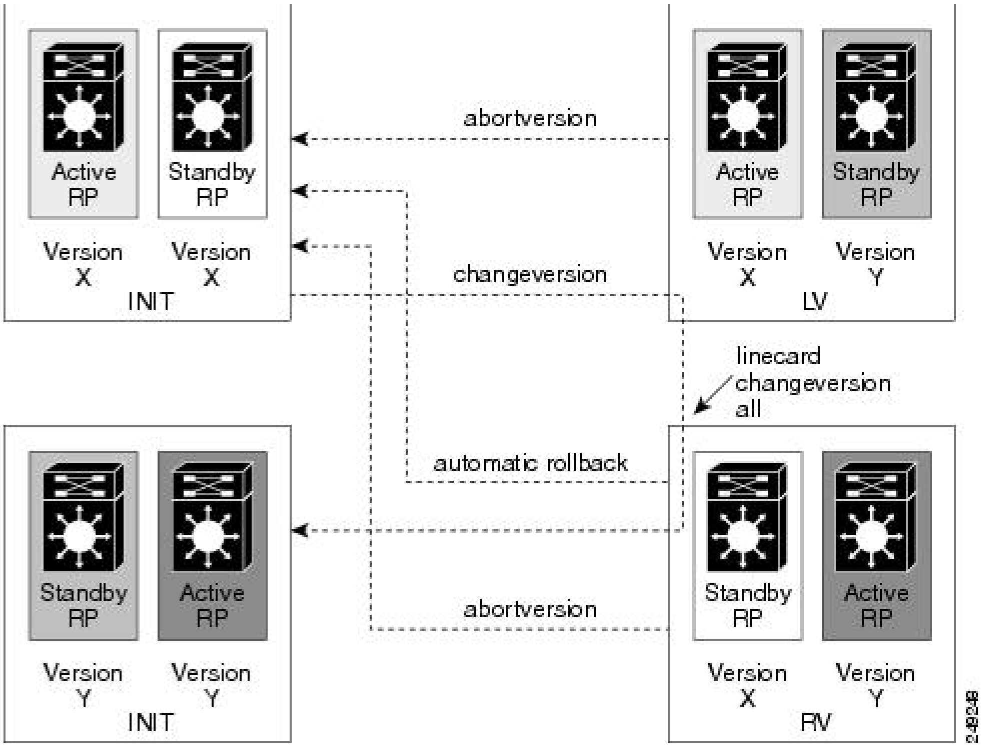
1. Initialization (INIT) state—It is the steady state before any software upgrade is committed.
2. Load version (LV) state—It is the state when the issu loadversion command is executed to start the ISSU process.
3. Run version (RV) state—It is the state when the issu runversion command is executed to 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-imagestandby-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.

CHAPTER 2

N+1 Redundancy for the Cisco Cable Modem Termination System

First Published: February 14, 2008

Last Updated: October 01, 2012

Note Cisco IOS Release 12.2(33)SCA and later releases integrate support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The N+1 Redundancy feature provides high availability on CMTS and telecommunications networks that use broadband media. N+1 redundancy can help limit customer premises equipment (CPE) downtime by enabling robust automatic switchover and recovery in the event that there is a localized system failure. The N+1 redundancy protection scheme you select for your system depends on your CMTS platform and upon the number of cable interface line cards or broadband processing engines (BPEs) that you have installed in the Cisco CMTS router.

Note This document describes the N+1 redundancy configuration and support with the Cisco uBR 3x10 RF Switch in detail. Starting with Cisco IOS Release 12.2(33)SCG, support for the Cisco uBR Advanced RF Switch has been added. For the N+1 redundancy configuration and support information with the Cisco uBR Advanced RF Switch, see the Cisco uBR Advanced RF Switch Software Configuration Guide .

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

To use N+1 redundancy, ensure the following conditions are met:

- To implement N+1 redundancy, you must use an image from a supported Cisco IOS software release. Refer to the release notes for your platform on Cisco.com to verify the availability of the N+1 Redundancy feature.
- Your downstream plant must meet Data-over-Cable Service Interface Specifications (DOCSIS 1.0 or later) requirements.
- Customer cable modems must meet requirements for your network and server offerings. All third-party cable modems must comply with DOCSIS 1.0 or later versions.

Table below shows the hardware compatibility prerequisites for the N+1 Redundancy feature.

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

Table 3: N+1 Redundancy 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)SCB and later • Cisco uBR10-MC5X20U/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 [2]

[2] The Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Note Cisco uBR7200 series routers do not support N+1 redundancy.

Restrictions and Limitations

The following sections describe restrictions and guidelines for configuring N+1 line card redundancy.

Note It is important to be aware that in Cisco IOS software releases earlier to Cisco IOS Release 12.2(33)SCC, line card redundancy is configured in two ways: N+1 HCCP Redundancy and Global N+1 Line Card Redundancy. The N+1 HCCP Redundancy configuration is not supported beginning with Cisco IOS Release 12.2(33)SCC. As you consider the restrictions and configuration information in this chapter, keep the distinction between the legacy HCCP configuration and the global configuration in mind.

General N+1 Redundancy Restrictions

The following are the general restrictions applicable to the N+1 Redundancy feature. These restrictions apply to both N+1 HCCP Redundancy and Global N+1 Line Card Redundancy configurations.

- A DOCSIS Timing, Communication and Control (DTCC) card or a TCC+ card must be installed in your Cisco uBR10012 router in order to employ the Cisco RF Switch in your cable headend system. For more detailed information on the DTCC and TCC+ cards, see the following documents:
  - Cisco uBR10012 Universal Broadband Router DTCC Card
  - Cisco uBR10012 Universal Broadband Router TCC+ Card

- Using slot 5/1 as the protect interface is easiest for physical wiring to the Cisco RF Switch when used with the Cisco uBR10012 router.
- The Cisco uBR10012 SNMP community string and N+1 Cisco RF Switch community string must be different. If the same community string is used, the Cisco uBR10012 router cannot be reached through SNMP until the community string is adjusted.
- The HCCP Switchover Enhancements feature has the following restrictions:
    - The feature is supported on the Cisco uBR10012 router only.
    - The line card switchover performance improvements are valid for networks scaling to less than 5000 cable modems per line card, and less than 1000 voice calls per line card.
    - The working and protect line cards must have the same channel width.
    - Upconverter failure detection is not included as part of the line card switchover performance improvements.
    - Virtual interface bundling is required. If you are upgrading from an earlier Cisco IOS software release and virtual bundling is not configured upon startup, the Cisco IOS software will automatically generate a virtual bundling configuration. Therefore, beginning in Cisco IOS Release 12.3(21)BC, Layer 3 information cannot be configured directly at the cable interface. The maximum number of virtual bundle interfaces supported is 40, and bundle numbers can be between 1–255.
    - In Cisco IOS Release 12.2(33)SCA and later, keepalive failure detection is enabled only for upstreams that have 15 or greater modems online. However, a switchover due to keepalive failure will trigger only if there is not any traffic on all of the upstreams associated with a cable interface that is enabled for keepalive.

For example, on a cable line card interface enabled for keepalive (this is the default) you have the following US status: US0 (200 CMs online), US1 (10 CMs online), US2 (16 CMs online), US3 (shutdown). US0 and US2 are enabled for keepalive detection because they each have more than 15 modems online.

If US0 has a keepalive failure due to a cable cut, but US2 is still passing traffic, then no keepalive switchover is triggered on that domain or interface. The calculation looks at all relevant US ports in a MAC domain and if those relevant ports have no traffic, then keepalive detection will begin. In this example, only two ports were relevant and both of those ports did not lose traffic, so keepalive still did not activate the failover.

If US0 had a cable cut while US2 also had no traffic, then a keepalive switchover would be triggered.

Note Beginning with Cisco IOS Release 12.2(33)SCE and later, the High Availability keepalive failure detection feature is disabled on Cisco UBR-MC20X20V and Cisco uBR-MC3GX60V line cards to prevent false alarms. The downstream connectivity loss can be detected by DEPI control session on the Cisco uBR-MC3GX60V line card whereas downstream PHY is able to detect the fatal error on the Cisco UBR-MC20X20V line card.

Information About N+1 Redundancy

This section describes the concepts that relate to N+1 redundancy: N+1 redundancy refers to (N) cable interface line cards, called “working” line cards being protected by one additional line card (+1), called the “protect” line card.

The two types of Cisco N+1 configuration are as follows:

- 7+1—Refers to an eight-card redundancy scheme in which seven working cable interface line cards are protected by one additional protect line card. This is the default N+1 configuration for the Cisco uBR10012 router, and requires two Cisco uBR 3x10 RF Switches or one Cisco uBR Advanced RF Switch.

Note The term "7+1 Redundancy" is also referred to as "8+1 Redundancy" in the field—physically, eight line cards in "8+1" mode are configured as seven working line cards with one protect line card. Therefore, "7+1 Redundancy" is the more physically accurate term.

- 4+1—Refers to a four-card redundancy scheme in which four working cable interface line cards are protected by one additional protect line card. This requires only one Cisco RF Switch.

Upconverters may reside between the Cisco uBR 3x10 RF Switch and the downstream (DS) interface on the Cisco CMTS. Cisco IOS supports both SNMP and non-SNMP-capable upconverters. No upconverters are required with the Cisco uBR Advanced RF Switch.

Note Globally configured N+1 line card redundancy and the legacy form of HCCP line card redundancy configurations are mutually exclusive in Cisco IOS Release 12.2(33)SCB and earlier.

You can configure N+1 redundancy in the following two ways:

N+1 HCCP Redundancy

Configured using HCCP commands at the interface level.

N+1 redundancy adds synchronization between Hot-Standby Connection-to-Connection Protocol (HCCP) working interface configurations and those inherited upon switchover to HCCP protect interfaces. This makes the configuration of both easier and switchover times faster.

Note N+1 HCCP Redundancy configuration is supported only in Cisco IOS Release 12.2(33)SCB and earlier.

Restrictions for N+1 HCCP Redundancy

Use the IP address from the local loopback interface (required in SCA and SCB only) as the working interface IP address when configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router. We recommend that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface IP address to the HCCP protect configuration.

Restrictions with the Cisco UBR10-MC 5X20 Cable Interface Line Card

- MAC domains and corresponding DS interface pairs switch over together— Each ASIC processor on the Cisco UBR10-MC 5X20 line card supports two MAC domains. MAC domains that share a common ASIC processor (JIB) must be configured so that they share the same state, Active or Standby. As a result, each interface in the pair switches over with the other.

Downstream MAC domain pairings would be downstream (DS) ports 0 and 1, ports 2 and 3, and a solitary port 4, which has its own JIB. For example, these interface pairings share the same JIB and switch over together as follows:

- ◦ Cable interface 5/0/0 and 5/0/1

  ◦ Cable interface 5/0/2 and 5/0/3

  ◦ Cable interface 5/0/4 is on the third ASIC processor, which is not shared with another interface.

- If Cisco uBR10-MC5X20 line card is used as working line card and Cisco uBR-MC20X20V line card used as protect line card, the HCCP feature is not supported when the working line card is replaced (using Online Insertion and Removal (OIR)) with a Cisco uBR-MC20X20V line card.

Note If HCCP is not configured on an interface that shares a MAC processor with another configured interface, it does not switch over and could cause issues. The same holds true if an ASIC companion is "locked out" during a failover.

Prerequisites for N+1 HCCP Redundancy

Before a switchover can occur, the HCCP protect interface automatically loads multiple configurations from the HCCP working interface. All configurations are loaded to protect automatically except DS modulation, DS interleave depth, and the DOCSIS Annex mode. If protect interface configuration occurs at the time of switchover, the PHY parameters are reset and cable modems go offline. To prevent this scenario, the protect interface is synchronized with the latest 'sync' status received from any working interface. Therefore, it is required that all HCCP working interfaces within an HCCP group have identical configurations for the command-line interfaces described in this section. Any one of these working interfaces provides the configuration of HCCP protect interfaces.

Preconfiguring HCCP Protect Interfaces

The following three specific HCCP functions are synchronized between working and protect interfaces:

- downstream modulation—the modulation scheme used for downstream traffic to the subscriber’s cable modem.
- downstream interleave depth—the interleaving amount of downstream symbols for impulse noise issues
- the DOCSIS Annex mode—the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card:

  ◦ Annex A (Europe)

  ◦ Annex B (North America)

Each of these three preconfigurations should be the same for all members of the HCCP groups; otherwise the cable modem may go offline during switchover and the switchover performance may be impacted due to the delay in applying the new change in the downstream PHY chip.

Global N+1 Line Card Redundancy

Global N+1 Line Card Redundancy feature simplifies the configuration of working and protect interfaces by eliminating the need to configure the more complex **hccp** interface configuration commands. Global N+1 Line Card Redundancy is supported on the Cisco uBR10012 router only.

The following set of simpler CLIs are used to configure global N+1 line card redundancy:

- **redundancy** command in global configuration mode
- **linecard-group cable** command in redundancy configuration mode. This command auto-enables line card redundancy configuration mode.
- **member subslot** command in line card redundancy configuration mode

Note The **member subslot** commands implement HCCP on each cable interface for the line card subslot position.

This feature allows plug-and-play operation of the Cisco RF switch in 7+1 HCCP Redundancy configuration with the Cisco uBR10012 universal broadband router because the Cisco RF switch is shipped with certain default settings to allow a quick bringup of a 7+1 redundant configuration with the router. However, some configuration of the router is required.

Global 4+1 Redundancy on the Cisco uBR10012 Router

This configuration entails one Cisco RF Switch and the router. In this configuration, four working interfaces are supported with one protect interface, but at a line card level. When one interface on a line card switches over, this triggers switchover for the entire line card.

Global 7+1 Redundancy on the Cisco uBR10012 Router

This configuration entails two Cisco uBR 3x10 RF Switches or one Cisco uBR Advanced RF Switch and the router. In this configuration, seven working interfaces are supported with one protect interface, but at a line card level. When one interface on a line card switches over, this triggers switchover for the entire line card.

Cisco IOS and Cisco RF Switch Firmware for N+1 Redundancy

Two operating systems govern the configuration and operation of N+1 redundancy on the Cisco CMTS:

- Cisco Internetwork Operating System (IOS)—Governs the configuration and operation of Cisco universal broadband routers, and works closely with Cisco RF Switch when configured in N+1 redundancy.

Note The Cisco IOS CLI synchronizes configurations between HCCP working and protect interfaces. Preconfiguration of the protect interfaces is no longer required in most circumstances.

- Cisco uBR 3x10 RF Switch Firmware—Governs the configuration and operation of the Cisco RF Switch, including the IP address on the RF Switch.

Refer to the Cisco RF Switch Firmware Command Reference Guide on Cisco.com for complete feature descriptions and command histories for the Firmware Versions listed above.

Note With the Cisco uBR 3x10 RF Switch, both command-line interfaces are required for configuration and testing of N+1 redundancy.

- Cisco uBR Advanced RF Switch—The Cisco uBR10012 router controls the configuration and operation of the Cisco uBR Advanced RF Switch.

Refer to the Cisco uBR Advanced RF Switch Software Configuration Guide and Cisco IOS CMTS Cable Command Reference for complete feature descriptions and command usage.

N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router

The 7+1 redundancy scheme for the Cisco uBR10012 router supports redundancy for the cable interface line cards installed in a fully populated Cisco uBR10012 chassis. Other redundancy schemes are designed to support partial cable interface line card populations in a Cisco uBR10012 chassis.

A single Cisco uBR10012 CMTS can support up to eight Cisco cable interface line cards.

A single Cisco RF Switch can then be connected to this Cisco uBR10012 router, allowing you to deploy an N+1 redundancy scheme where one protecting cable interface line card supports from one to seven working cable interface line cards in the same chassis.

N+1 Redundancy and the Cisco RF Switches

The Cisco RF Switch can be operated in two separate modes, either in 7+1 configuration, or in 4+1 configuration.

Note The default N+1 redundancy mode for the Cisco RF Switch is 7+1. This does not require change when configuring N+1 redundancy on the Cisco uBR10012 router.

Note The show configuration command and other Cisco RF Switch commands contain the Card Protect Mode field. When this field displays 7+1, this indicates that the Cisco RF Switch is configured for N+1 redundancy, where eight or less working line cards are possible.

In both of the Cisco RF Switches, the slot number is the chassis slot in which an Ethernet controller or an upstream or downstream card is installed, and the logical interface number is the physical location of the interface port on an Ethernet controller.

The Cisco RF switch module is a switching matrix that allows flexibility in the routing of RF signals between "N" working RF cable interface line cards and one protect RF cable interface line card.

IF Muting on the Cisco CMTS for non-SNMP-Capable Upconverters

IF muting with both SNMP and non-SNMP-capable upconverters is supported in N+1 redundancy. IF muting offers the following benefits:

- IF muting for either type of upconverter significantly increases the N+1 protection schemes that are available for Cisco CMTS routers.
- IF Muting offers the additional benefit of being faster than RF Muting.
- IF Muting is enabled by default.

IF Muting functions in the following manner:

- IF output from the working cable interface line card is enabled.
- IF output from the protect cable interface line card is disabled.
- When a switchover occurs from working to protect, the IF output of the working card is disabled and that of the protect is enabled. If an interface is in Active mode, RF output is enabled.
- When the cable interface line card first comes up after a system failure, IF output is muted until the Cisco CMTS determines if each interface is in active or standby mode (in either working or protect state). When an interface is active (working or protect), IF output is enabled. When an interface is in standby mode, IF output is muted.

The relevance and support for IF Muting is dependent on the type of Cisco CMTS being used. This is a summary of IF Muting in relation to three sample scenarios:

- Case1—External upconverters are not controlled nor controllable. In this type of scenario, the external upconverter either cannot be controlled remotely or the Cisco CMTS is not configured to control the external upconverter.
- Case 2—The Cisco CMTS is configured to control an external upconverter. Cisco continues to support N+1 redundancy in this scenario (in which IF Muting is not required). The Cisco CMTS uses RF Muting of the upconverter in this scenario—automatically enabled when an HCCP upconverter statement is configured.
- Case 3—The Cisco CMTS uses internal upconverter(s). Cisco continues to support N+1 redundancy in this scenario (in which IF muting is not required). The Cisco CMTS uses RF muting in this scenario (automatically enabled) because the upconverter is configured by the CMTS to do RF Muting.

IF Muting and HCCP Configuration

HCCP interface configuration typically entails three tasks:

- Working or protect mode
- Upconverter statement
- RF switch statement

When you configure HCCP on an interface, but you do not specify an upconverter statement, this dictates whether IF Muting is active. With no upconverter statement in the interface configuration, IF Muting becomes active by default.

Restrictions for IF Muting

Shared Downstream Frequency

All the interfaces in the same HCCP group must use the same downstream frequency. To define the downstream center frequency for the cable interface line card, use the cable downstream frequency command in cable interface configuration mode. On cable interfaces with an integrated upconverter, use the no form of this command to remove the downstream frequency and to disable the RF output.

The usable center frequency range depends on whether the downstream is configured for DOCSIS or EuroDOCSIS operations:

-
    - DOCSIS — 91 to 857 MHz
    - EuroDOCSIS — 112 to 858 MHz

The Cisco IOS supports a superset of these standards, and setting a center frequency to a value outside these limits violates the DOCSIS or EuroDOCSIS standards. Cisco does not guarantee the conformance of the downstream and upconverter outputs when using frequencies outside the DOCSIS or EuroDOCSIS standards.

Requirements for IF Muting

For non-SNMP-capable upconverters to be used with IF Muting, RF output must be less than -3 dBmV when:

- IF input is absent.
- The switchover time from working to protect is less than one second. That is, when IF is applied to the upconverter, the RF output must be present within one second.

If either of these requirements is not met, the integrity of the N+1 switchover operations could be compromised.

Default Line Card and Bitmap Settings on the Cisco uBR 3x10 RF Switch for Global N+1 Line Card Redundancy

The Cisco uBR 3x10 RF Switch is pre-configured with certain settings to allow plug-and-play with the Cisco uBR10012 universal broadband router for a global 7+1 line card redundancy configuration.

The default bitmap on the Cisco uBR 3x10 RF Switch is 0xFFFFFFFF. This value assumes rfsw-2 on the top half of the Cisco UBR10-MC5X20 BPE, and rfsw-1 on the lower half.

For the protect interface, global configuration uses the IP address of an internal FastEthernet interface.

In 7+1 Redundancy mode, the default header settings are as follows:

- interface 8/0 in header 1
- interface 8/1 in header 2
- interface 7/0 in header 3
- interface 7/1 in header 4

This default setting is based on the line card slot/subslot being configured. The following table lists the mapping of line card interfaces to RF Switch slots (rfsw-slots):

Line Card Slot	5/0	5/1	6/0	6/1	7/0	7/1	8/0	8/1
RFSw-Slot 7+1 mode	7	0	5	6	3	4	1	2

Note Value 0 signifies by default the protect slot. RFSw-Slot header and RF Switch slot # refer to the same thing.

Default Line Card and Bitmap Settings on the Cisco uBR Advanced RF Switch for Global N+1 Line Card Redundancy

Table below shows the default mapping between the slot ID of the Cisco uBR Advanced RF Switch and the line card on the Cisco uBR10012 router.

Table 4: Default Mapping between the Cisco uBR Advanced RF Switch with the Line Card on the Cisco uBR10012 Router

Slot ID on the Cisco uBR Advanced RF Switch	Line Card on the Cisco uBR10012 Router
1	8/0
2	8/1
3	7/0
4	7/1
5	6/0
6	6/1
7	5/0
0	5/1

High Availability Support for Encrypted IP Multicast

The Cisco CMTS router supports IP Multicast streams during switchover events in a High Availability environment. This feature is supported for Route Processor Redundancy Plus (RPR+), N+1 redundancy, and encrypted BPI+ streams.

For additional information about IP Multicast and High Availability, refer to these documents on Cisco.com:

- Dynamic Shared Secret for the Cisco CMTS
- IP Multicast in Cable Networks , White Paper

How to Configure N+1 Redundancy

You must configure and activate both the Cisco RF Switch and the Cisco CMTS to ensure that N+1 redundancy operates correctly.

Note The below configurations are for the Cisco uBR 3x10 RF Switch. For instructions on how to configure the Cisco uBR Advanced RF Switch, see the Cisco uBR Advanced RF Switch Software Configuration Guide .

Common Tasks for Configuring N+1 HCCP Redundancy and Global N+1 Line Card Redundancy

Configuring the Cisco RF Switch for N+1 Redundancy

DETAILED STEPS

	Command or Action	Purpose
Step 1	**set mac address** *mac-address* **Example:** `rfswitch> set mac address 0000.8c01.1111`	(Optional) To specify the MAC address of the Ethernet port on the Cisco RF Switch (used to connect to the LAN), use the set mac address command at the Cisco RF Switch command line interface. The MAC address must be specified using a trio of hexadecimal values. For example, set mac address hex.hex.hex. To negate the existing MAC address assignment and specify a new one, use the no form of this command. If no MAC address is specified, the Cisco RF Switch assumes the default OUI MAC address value.
Step 2	**set ip address** *ip-address* **netmask** [*dhcp*] **Example:** `rfswitch> set ip address 172.16.10.3 255.255.255.0`	(Optional) To specify a static IP address and relative netmask of the Ethernet interface on the Cisco RF Switch, use the set ip address command in User mode. To restore the default setting, user the no form of this command. Default setting differs according to your Firmware Version: • The default IP configuration for Version 3.30 and 3.50 is DHCP enabled. • The dhcp keyword enables the specified IP address as the address for DHCP services on the network. This keyword also produces the same result as the no form of this command for Version 3.30 and 3.50—it enables DHCP. • The default IP configuration for Version 2.50 is the static IP address of 10.0.0.1 255.255.255.0.

	Command or Action	Purpose

Step 3	**set slot config** {*upstreamslots* | *downstreamslots*}
	Example:
	`Cisco 3x10 RF Switch (default)`
	`rfswitch>` **`set slot config 0x03ff 0x1c00`**
		(Optional) Sets the chassis slot-to-line card configuration. The command no set slot config restores the default, which is a 3x10 configuration.
		Setting a bit position tells the Cisco RF Switch to expect that type of card installed in the slot. A zero in both parameters indicates that the slot should be empty. Both *upstreamslots* and *downstreamslots* are 16-bit hex integer bit-masks that represent whether the slot is enabled/configured for that type of card. The right-most bit represents slot 1.
		For additional bitmap conversion information, refer to the *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* (Microsoft Excel format)
		http://www.cisco.com/warp/public/109/BitMap.xls
		As there are only 14 slots in the Cisco RF Switch chassis, the upper two Most Significant Bits (MSBs) of the 16-bit integer are ignored.
		Note Changes made to the slot configuration on the Cisco RF Switch do not take effect until the system is rebooted (reload command), or an event occurs which causes the enumeration of the chassis line cards to reset.

Step 4	**set snmp community read-write private** **Example:** `rfswitch>` **`set snmp community read-write private`**	(Optional) To specify the Simple Network Management Protocol (SNMP) community string on the Cisco RF Switch, use the set snmp community command at the Cisco RF Switch command line interface. This command enables you to gain read and write access to the Cisco RF Switch. The community string must be entered as a string of text. To negate the existing community string and make way for a new one, use the no form of this command. If no SNMP string is entered, the SNMP string assumes the default value private. **Note** Currently, the private keyword is the only SNMP community string supported on communication between the Cisco RF Switch and the Cisco uBR10012 router. The default value of private is the proper setting under normal circumstances.
Step 5	**set snmp host** *ip-address* **Example:** `rfswitch>` **`set snmp host 172.16.10.3`**	(Optional) To specify the IP address that receives SNMP notification messages, use the set snmp host command at the Cisco RF Switch command line interface. You can specify more than one SNMP IP address simply by entering this command once for each IP address you want to specify. To negate an existing SNMP IP address assignment, use the no form of this command. If no SNMP IP address is specified, the Cisco RF Switch does not transmit any SNMP notification messages.
Step 6	**set snmp traps** • **Example:** `rfswitch>` **`set snmp traps`**	(Optional) To enable SNMP reporting for all modules on the Cisco RF Switch, use the set snmp traps command in the Cisco RF Switch User mode. To deactivate SNMP reporting, use the no form of this command. SNMP reporting is enabled by default on the Cisco RF Switch.

Step 7	**set protection {4|8}**
	Example:
	`rfswitch>` **`set protection 8`**
		To set the line card protection scheme, specifying the N+1 protection scheme under which the Cisco RF Switch operates, use the set protection command in Cisco RF Switch User mode.
		• **set protection4—**Specifies that the Cisco RF Switch operate using a 4+1 protection scheme.

	Command or Action	Purpose
		• **set protection8—**Specifies that the Cisco RF Switch operate using a 7+1 protection scheme. To negate the existing protection scheme specification, use the no form of this command. The default protection scheme for the Cisco RF Switch is 7+1.
Step 8	**set password** *text* **Example:** `rfswitch>` **`set password cisco`**	(Optional) To specify an access password for the Cisco RF Switch command line interface, use the set password command at the Cisco RF Switch command line interface. To negate the existing access password, use the no form of this command.
Step 9	**set tftp-host** *ip-address* **Example:** `rfswitch>` **`set tftp host 172.16.10.17`**	(Optional) To specify the host IP address of the TFTP server through which the Cisco RF Switch enables file transfer, use the set tftp-host command at the Cisco RF Switch command line interface. To negate an existing host IP address specification for the remote TFTP server, use the no form of this command. (No default TFTP server IP address is supported on the Cisco RF Switch.)
Step 10	**set switchover-group** *group-name module-bitmap* |**all** **Example:** `rfswitch>` **`set switchover-group a12345 0xAA200000`**	To specify a new or existing switchover group name (to which a Cisco RF Switch module is assigned), use the set switchover group command at the Cisco RF Switch command line interface. A switchover group is a collection of Cisco RF Switch interfaces that are all configured to switch over at the same time. • *group-name* — Can be an alpha-numeric string beginning with a non-numeric character. • *module-bitmap* le-bitmap — Defines a Cisco RF Switch module, and must be specified as an eight-character hexadecimal identifier or assigned the all keyword. **Note** Refer to the Creating Cisco RF Switch Module Bitmaps, on page 71 for instructions on creating an appropriate hexadecimal module bitmap. • **all** — Keyword instructs the Cisco RF Switch to automatically switch over all upstream and downstream interfaces connected to the switch module in question. **Note** When setting bit maps on the RF Switch, type 0x in front of the bitmap identifier so that the RF Switch recognizes hexadecimal code. Otherwise, the RF Switch assumes the bitmap is in decimal code. To negate an existing switchover group, use the no set switchover-group command at the Cisco RF Switch command line interface. **Note** You do not need to specify module-bitmap when negating an existing switchover group. For example, the command no set switchover-group a12345 will eliminate the switchover group named “a12345.” Once a switchover group containing one or more Cisco RF Switch modules has been defined, you can use the switch command to enable N+1 redundancy behavior on the Cisco RF Switch, as described in the section Switchover Testing Tasks for N+1 Redundancy, on page 90

	Command or Action	Purpose
Step 11	**save config** **Example:** `rfswitch> save config`	This command saves the latest configuration or image upgrade changes in both Flash and Bootflash, and synchronizes Backup and working copies in each.

Step 12	Choose one of the following:**reboot**
	• **reboot**
	• **reload**
	Example:
	`rfswitch>reboot`
	`or`
	`rfswitch> reload`
		This command restarts the Cisco RF Switch so that all changes above take effect.

Operating DHCP with the Cisco RF Switch

DHCP operation is enabled by default, unless the user has set a static IP address using the **set ip address** command in User mode.

When the RF Switch boots, it checks to see if DHCP has been enabled. This is done via the RF Switch commands in a variety of ways. You can use any of the following commands in User mode to enable DHCP:

- **set ip address dhcp**
- **set ip address** *ip-address subnet-mask*
- **no set ip address** (to set the default DHCP operation)

Note The RF Switch Firmware no longer assumes a static IP address of 10.0.0.1 as in versions prior to 3.00. For details on DHCP configuration, see the Cisco RF Switch Firmware Configuration Guide .

Creating Cisco RF Switch Module Bitmaps

Perform the following steps to produce a hexadecimal-format module bitmap that you can then assign to working or protect Cisco RF Switch modules. Module bitmaps for the Cisco RF Switch are comprised of 32-bit map assignments that you translate to an eight-character hexadecimal module bitmap identifier.

Note The Cisco RF Switch ships with some additional pre-configured defaults to ease initial bringup of the switch. For more information on these default settings, see the Default Line Card and Bitmap Settings on the Cisco uBR 3x10 RF Switch for Global N+1 Line Card Redundancy, on page 66.

This procedure cites an example of a typical working cable interface module map with 7+1 redundancy configuration. This scenario connects cable interfaces to the Cisco RF Switch following the example described in the " Cabling " chapter of the Cisco RF Switch Hardware Installation and Configuration Guide :

- Interfaces A, B, C, D, and F comprise the four upstream and one downstream connections to the first MAC domain of a UBR10-LCP2-MC28C cable interface line card installed in a Cisco uBR10012 Series chassis.
- Interfaces H, I, J, K, and M comprise the four upstream and one downstream connections to the second MAC domain on the same cable interface line card.

Note Also refer to the *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* in Microsoft Excel format—available for download and use from Cisco.com.

Step 1 Logically break the two MAC domains up into separate groups and deal with them on their own.
Begin by determining the 32 binary values for the first MAC domain that will eventually define the eight decimal characters leading to the eight hexadecimal characters comprising your module bitmap by laying out the individual bits as follows.

Note In order to optimize N+1 redundancy behavior among the switch modules in the Cisco RF Switch, the internal mapping of the switch circuitry calls for the interfaces to be addressed as they are displayed in the example, below—A H B I C J D K L F M G N.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Step 2 Convert the eight resulting binary quartets into decimal values as follows:
Interim step.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	1 0				1 0				2				0				0				0				0				0			

Step 3 Convert the eight resulting decimal values into hexadecimal values as follows.
The eight resulting hexadecimal characters (in sequence) comprise the eight-character hexadecimal module bitmap for the first MAC domain featuring cable connections to interfaces A, B, C, D, and F on the Cisco RF Switch. Therefore, the resulting module bitmap is AA200000.

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	10				10				2				0				0				0				0				0			
Hexadecimal	A				A				2				0				0				0				0				0			

Step 4 Repeat the steps above for the second MAC domain.
Your resulting hexadecimal values should be as follows:

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	5				5				1				0				0				0				0				0			
Hexadecimal	5				5				1				0				0				0				0				0			

Therefore, the resulting module bitmap is 55100000.

Note It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure. In such an instance, the combined layout of the two groups exemplified above would be as follows:

Interface	A	H	B	I	C	J	D	K	E	L	F	M	G	N	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Binary	1	1	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Decimal	15				15				5				0				0				0				0				0			
Hexadecimal	F				F				5				0				0				0				0				0			

After this combination, the resulting module bitmap is FF500000.

Tip Cisco has provided for switchover of an entire cable interface line card by implementing a default module bitmap (referred to by the keyword all) that features an actual hexadecimal module bitmap value of FFFFFFFF.

It is also permissible (and in some cases, recommended) to map the entire collection of cables from a cable interface line card into a single bitmap so that the entire cable interface line card switches over in the event of a local or remote failure.

In such an instance, the combined layout of the two groups illustrated above would be as follows:

- If you have a fault on one MAC domain, the other MAC domains will not switch over gracefully merely by toggling the Cisco RF Switch relays. If you have keepalive configured on the other MAC domains, they will eventually switch over, but not efficiently.

- Another method is to have each interface track the other. Therefore, if one interface from a UBR10-LCP2-MC28C cable interface line card goes down, the other interfaces will follow if they have the tracking statement. With this approach, the interface cable 5/0/0 would show the following configuration, for example:

Note Tracking is not needed when using global N+1 configuration. Beginning in Cisco IOS Release 12.3(21)BC, tracking of HCCP interfaces is removed. The **hccp track** command is obsolete.

```
hccp 1 track c5/0/1
```

Interface 5/0/1 would show the following configuration:

```
hccp 2 track c5/0/0
```

Tip We recommend that you disable automatic HCCP revertive functions on both protect downstream channels of a JIB that use keepalive or tracking. Refer to the Disabling HCCP Revertive on Protect Cable Interfaces, on page 88.

Enabling the HCCP Switchover Enhancements Feature

The HCCP Switchover Enhancements feature implements performance improvements for traffic recovery during line card switchover under certain scalability limits.

Within the required network scalability limits, the HCCP Switchover Enhancements feature provides the following switchover benefits:

- Less than 1-second voice call recovery.
- Less than 20-second data recovery.

Prerequisites for the HCCP Switchover Enhancements Feature

- Each line card must support less than 5000 cable modems.
- Each line card must support less than 1000 voice calls.
- The working and protect line cards must have the same channel width.
- The cable line cards must use virtual interface bundling.
- No Layer 3 configuration is supported on the cable interface
- Virtual interface bundling configuration is required to enable the HCCP Switchover Enhancements feature.

Note When you upgrade to Cisco IOS Release 12.2(33)SCA and later, all preexisting cable bundles are automatically converted to virtual bundles, and standalone cable interfaces must be manually configured to be in a virtual bundle. For configuration examples, see Example: Virtual Interface Bundling, on page 131.

Tasks for Configuring Global N+1 Line Card Redundancy

Configuring Global N+1 Line Card Redundancy

Starting with Cisco IOS Release 12.2(33)SCF, you can configure a card with a lower license as the protect card for a working card with a higher license. This protect card remains in a nonfunctional mode (not in standby mode) and does not become active until it is upgraded and reloaded with a higher license, when a switchover occurs.

Before You Begin

- This High Availability configuration describes one or two Cisco RF Switches in the scheme.
- DHCP must be accounted for prior to or during this procedure. An external DHCP server must be installed and operational on the network, or an internal DHCP server must be operational within the Cisco router. The DHCP server configuration, of either type, must have the following DHCP and DNS entries. Two Cisco RF Switches are illustrated for example:
- Be sure to configure the RF switch name using the **rf-switch name** line card redundancy configuration command, and the RF switch IP addresses prior to configuring line card redundancy.

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# config terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**ip host rf-sw1***ip_addr* **Example:** `Router(config)# ip host rf-sw1 10.4.4.1`	Assigns the Domain Name System (DNS) entry to the first or only Cisco RF switch in the redundancy scheme.
Step 4	**ip host rf-sw2***ip_addr* **Example:** `Router(config)# ip host rf-sw2 10.4.4.2`	(Required when using two Cisco RF Switches) Assigns the DNS entry to the second Cisco RF switch in the redundancy scheme.

	Command or Action	Purpose

Step 5	**redundancy**
	Example:
	`Router(config)# redundancy`
	`Router(config-red)#`
		Enables global N+1 redundancy for cases in which factory-configured N+1 redundancy has been disabled, and enters redundancy configuration mode.
		This command is supported in Cisco IOS Release 12.3(13a)BC and later releases.

Step 6	**linecard-group 1 cable** **Example:** `Router(config-red)# linecard-group 1 cable`	This command assigns the HCCP group to all interfaces on the cable interface line card, or Cisco Broadband Processing Engine.
Step 7	**member subslot** *slot/card* **working** **Example:** `Router(config-red)# member subslot 8/0 working`	This command configures all interfaces on the specified line card to function as HCCP working interfaces in the redundancy scheme. Repeat this step for each working line card in the Cisco router.

Step 8	Do one of the following:
	• **member subslot** *slot /card* **protect**
	• **member subslot** *slot /card* **protectconfig***slot /card*
	Example:
	`Router(config-red)#  member subslot 8/1 protect`
	`or`
	`Router(config-red)# member subslot 8/1 protect config 8/0`
		Configures all interfaces on the specified line card to function as HCCP protect interfaces in the redundancy scheme.
		For faster switchover results, configures the protect interface for the most appropriate working interface configuration.

Step 9	**end**
	Example:
	`Router(config-red)# end`
	`Router#`
		Exits global and redundancy configuration modes and returns to Privileged EXEC mode.

Step 10	**write memory** **Example:** `Router# write memory`	After configuring all domains, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Configuring DHCP to Assign IP Addresses on the Cisco RF Switch

To support global N+1 line card redundancy, you must configure either your external DHCP server, or the internal DHCP server on the Cisco uBR10012 universal broadband router to provide the appropriate IP addressing for the Cisco RF switch.

The DHCP server configuration requires the following forms of DHCP and DNS settings:

```
ip dhcp pool rfswitch-pool
      network ...
   !
   ip dhcp pool rfsw-1  [ DHCP MAC->IP mapping for RF-switch # 1 ]
     host a.b.c.d <mask>
     client-id 01aa.bbcc.ddee.ff
   !
   ip dhcp pool rfsw-2  [ DHCP MAC->IP mapping for RF-switch # 2 ]
     host b.c.d.f <mask>
     client-id 01aa.bbcc.ddee.ff
```

You also need to configure DNS entry for each RF-switch, as follows:

```
   ip host rfsw-1 a.b.c.d  [ DNS mapping IP to RF-switch name for rfsw 1 and 2 ]
   ip host rfsw-2 b.c.d.f
```

The following example shows a sample DNS and DHCP configuration on the Cisco uBR10012 universal broadband router for the Cisco RF switch:

```
   ip host rfsw-1 10.10.107.202
   ip host rfsw-2 10.10.107.203
   ip dhcp pool rfsw-1
      host 10.10.107.202 255.255.255.254
      client-identifier 0003.8f00.0019
   !
   ip dhcp pool rfswitch-pool
      network 10.10.107.200 255.255.255.252
      next-server 10.10.107.101
      default-router 10.10.107.101
      option 7 ip 10.10.107.101
      option 2 hex ffff.8f80
      option 4 ip 10.10.107.101
      lease infinite
   !
   ip dhcp pool rfsw-2
      host 10.10.107.203 255.255.255.254
      client-identifier 0003.8f00.0020
   !
```

The sample configuration above provides a mechanism to make sure that rfsw-1 only gets IP address 10.10.107.202, and rfsw-1 only gets DHCP IP address 10.10.107.203.

Note The DNS entries for the Cisco RF Switch should be configured before any line card redundancy configuration is attempted.

Enabling Line Card Switchover in Redundancy Mode

The Cisco CMTS router enables switchover on an entire line card at one time, instead of one interface at a time. To switch over a cable interface line card in redundancy mode, use the following command in privileged EXEC mode:

```
Router# redundancy linecard-group switchover from
```

```
working-slot
/
working-subslot
```

Note

This command switches over a working slot only when active, but not when in protect mode. Also, this command does not switch over the locked interfaces.

To revert to original working and protect status, use the following command in privileged EXEC mode:

```
Router# redundancy linecard-group revertback
working-slot
/
working-subslot
```

This command reverts interfaces from the protect subslot to specified working subslot. If the protect subslot is not active, or is active for some other working subslot, then this command aborts and displays a system error message.

Locking a Switchover for all Interfaces

To lock or unlock a switchover for all interfaces on a given subslot, use the redundancy linecard-group command in privileged EXEC mode:

This command creates a wrapper that locks and unlocks switchover events on all interfaces for the given subslot (for example, interface 5/0). This command only locks or unlocks HCCP interfaces when in working slots.

Note

To remove an HCCP configuration from a working or protect interface, use the member subslot command in line card redundancy configuration mode after locking the interface using the redundancy linecard-group command.

For example, to lock the cable line card switchover (set the lockout flag to TRUE), use the following command:

Router# **redundancy linecard-group lockout 5/0**

To force switchover on a locked interface, use the cable power command in privileged EXEC mode.

Enabling Service Internal on HCCP Protect and Standby Working Interfaces

In Cisco IOS Release 12.3(33)SCC and later, to modify the configuration on an HCCP protect and standby working cable interfaces, use the **service internal** command in global configuration mode.

Note

When **service internal** command is disabled, you can only change the configuration of an active working interface. The protect line card does not become active directly when it starts up due to hardware reset, or power off/on or other reasons. It will always go to standby state after startup. We recommend that you do not enable **service internal** on the standby working controller, wideband and intergrated cable interfaces of a line card.

Changing Default RF Switch Subslots for Global N+1 Line Card Redundancy

The **member subslot** command enables you to configure a non-default 7+1 wiring other than factory settings. This command supports the option to cable any line card to any RF Switch slot. For example, interface 7/0 might need to be wired to RF Switch slot 7 (instead of the default 3).

To change the factory configuration of subslot mapping to a custom (non-default) mapping, do the following:

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# config terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.
Step 4	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. • *1*—Line card group number. • **cable**—Specifies the redundancy type.
Step 5	**member subslot***slot* / *subslot* **working rfsw-slot** [*slot-number*] **Example:** `Router(config-red-lc)# member subslot 7/0 working rfsw-slot 7`	Changes the factory configuration of subslot mapping to a custom (non-default) mapping. • *slot* —Chassis slot number of the cable interface line card. The valid range is from 5 to 8. • *subslot* —(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1. • **working**—Specifies the working slot in the line card group. • **rfsw-slot** [*slot-number*]—(Optional) Specifies the RF switch slot for the working line card.

Step 6	**end**
	Example:
	`Router(config-red-lc)# end`
		Returns to privileged EXEC mode.

Changing the Default RF Switch Name and SNMP Community String

The default RF Switch names (rfsw-1 for switch 1 and rfsw-2 for switch 2) are used to perform a DNS lookup for the RF-Switch IP address.

If on an external DHCP server, the RF-Switch DNS names are to be different from the default names, then you need to enter the new RF Switch name as part of line card redundancy configuration.

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# config terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.
Step 4	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. • *1*—Line card group number. • **cable—**Specifies the redundancy type.
Step 5	**rf-switch name {1|2}** *name* **Example:** `Router(config-red-lc)# rf-switch name {1|2} switch5`	Changes the default RF switch name. • *name* —Alphanumeric name to replace the default name of the Cisco RF Switch.
Step 6	**rf-switch snmp-community community-name** **Example:** `Router(config-red-lc)# rf-switch snmp-community RFswitchstring`	Changes the default SNMP community string. This command updates the Cisco uBR10012 SNMP software only and does not update the new snmp RW community string into the RF Switch. So the user must get into the RF Switch via telnet and set the new snmp RW community string in there. • *community-name* —SNMP community string name.

	Command or Action	Purpose

Step 7	end
	Example:
	`Router(config-red-lc)# end`
		Returns to privileged EXEC mode.

Removing Global N+1 Redundancy Configuration

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**redundancy linecard-group lockout** *slot* /*subslot* **Example:** `Router# redundancy linecard-group lockout 6/1`	Locks a line card switchover from the specified working slot and subslot. - *slot*—Chassis slot number of the cable interface line card. The valid range is from 5 to 8. - *subslot*—(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1.
Step 3	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 4	**redundancy** **Example:** `Router# redundancy`	Enters redundancy configuration mode.
Step 5	**linecard-group1cable** **Example:** `Router(config-red)# linecard-group 1 cable`	Enters line card redundancy configuration mode. - *1*—Line card group number. - **cable**—Specifies the redundancy type.

	Command or Action	Purpose
Step 6	**no member subslot***slot* /*subslot* **working** **Example:** `Router(config-red-lc)# `**`no member subslot 6/1 working`**	Removes the specified line card from the global redundancy configuration. • *slot*—Chassis slot number of the cable interface line card. The valid range is from 5 to 8. • *subslot*—(Cisco uBR10012 router only) Secondary slot number of the cable interface line card. Valid subslots are 0 and 1.

Step 7	end
	Example:
	`Router(config-red-lc)# `**`end`**
		Returns to privileged EXEC mode.

Tasks for Configuring N+1 HCCP Redundancy

Note Global configuration procedures render interface-level configuration of **hccp** commands obsolete. Legacy HCCP configuration and the newer global N+1 redundancy configuration are mutually exclusive.

Configuring HCCP Groups

This procedure defines HCCP working and protect interfaces for N+1 HCCP Redundancy.

Note When the Cisco CMTS CLI descriptions include the term channel switch, this term refers to the Cisco RF Switch. When configuring HCCP on the Cisco uBR10012 router, use the IP address from the local loopback interface as the working interface IP address. We recommend that you create a loopback interface on the Cisco uBR10012 router, and then assign the loopback interface's IP address to the HCCP protect configuration.

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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**hccp** *group* **working** *member-id* **Example:** `Router(config-if)# hccp 1 working 1`	Designates a cable interface on a CMTS in the specified HCCP group to be a working CMTS. The hccp working command is to be used for working line card interfaces only. • *group* —The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	**hccp** *group* **protect***member-idip-address* **Example:** `Router(config-if)# hccp 1 protect 2 10.10.10.1`	Assigns the HCCP group number, defines the corresponding HCCP member, and defines the working IP address of the interface used for HCCP communication. The hccp protect command is to be used for protect line card interfaces only. **Note** Working and protect line cards are located on the same Cisco uBR10012 router chassis. In the latter case, we recommend that you use the Loopback IP address in this configuration.
Step 6	**hccp** *group* **channel-switch** *member-id upconverter name* **wavecom-xx** *protect-upconverter-ip-address module working-ip-address its-module* **Example:** `Router(config-if)# hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14`	Configures the upconverter (UPx) topology so that the Vecima upconverter becomes part of the specified HCCP member in a particular HCCP group. **Note** This procedure is not required when configuring N+1 redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20 BPE. **Note** Steps 6 and 7 of this procedure are required for both the working and the protect interfaces.
Step 7	**hccp group channel-switch member-id rf-switch-name rfswitch-group** *ip address* **module-bitmap position** **Example:** `Router(config-if)#`	Configures the Cisco CMTS so that the specified Cisco RF Switch becomes part of the specified HCCP member in a particular HCCP group. • *ip address* — The IP address of the Cisco RF Switch. • — Specifies the name of the Cisco RF Switch, and must also include the hexadecimal module-bitmap argument. See the Creating Cisco RF

	Command or Action	Purpose
	`hccp 1 channel-switch 2 rfswitch-name rfswitch-group 10.97.1.20 AA200000 2`	Switch Module Bitmaps, on page 71 for instructions on creating an appropriate hexadecimal module bitmap. - **position** — This value specifies the slot/header of the Cisco RF Switch—there are eight on the Cisco uBR10012. **Note** Steps 6 and 7 of this procedure are required for both the working and the protect interfaces.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns to global configuration mode.
Step 9	**write memory** **Example:** `Router# write memory`	After configuring all domains, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Enabling HCCP Protect Interfaces for N+1 Switchover

To enable HCCP protect interfaces, making them available for N+1 switchover should the HCCP working interfaces fail, use the no shutdown command in interface configuration mode on each HCCP protect interface.

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# config terminal`	Enters global configuration mode.

Step 3	**interface cable** *slot/subslot/port*
	Example:
	`Router# interface cable 8/1/0`
	`Router(config-if)#`
		Ensure that you specify the variables for an HCCP protect interface to enter the interface configuration mode of that protect interface. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference.
		- *slot*—Slot where the cable interface line card resides.

	Command or Action	Purpose
		• *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the HCCP protect interface.
Step 5	Repeat	Repeat steps 3-4 for every HCCP protect interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns you to global configuration mode.
Step 7	**write memory** **Example:** `Router#  write memory`	After enabling all HCCP protect interfaces, save your settings to the nonvolatile random access memory (NVRAM) to ensure that the system retains the settings after a power cycle.

Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces

- Before removing HCCP configuration from an active working interface, either shut down the protect or lockout switchover functions using the hccp lock command in interface configuration mode. Otherwise the protect interface will declare the working interface to have failed and will attempt to switch over.
- Do not remove HCCP configuration from an active protect interface. The active member should be restored to its corresponding working interface before removing HCCP configuration from the protect interface.

Note This restriction does not apply when removing HCCP configuration from a protect interface while it is in standby mode and N+1 redundancy is in normal working mode.

To prevent cable modems from going offline during removal of HCCP configuration (on working interfaces), we recommend using one of the following three procedures as a best practice:

Shutting Down HCCP Protect Interfaces

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# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/subslot/port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the specified interface. This does not remove interface configuration—merely disables it.
Step 5	Repeat.	Repeat the above steps 3 and 4 as required to shut down all Protect HCCP interfaces.

Locking out HCCP Interface Switchover

Use the hccp lockout command to prevent a working HCCP interface from automatically switching to a protect interface in the same group. This command locks out the HCCP interface. To remove the lockout, use the hccp unlockout command in privileged EXEC mode (re-enabling N+1 redundancy on the working interface).

Note The **hccp lockout** command is not supported starting with Cisco IOS Release 12.2(33)SCE.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hccp** *group* **lockout** *member-id* **Example:** `Router# hccp 1 lockout 1`	To prevent a working HCCP interface from automatically switching to a Protect interface in the same group, use the hccp lockout command in privileged EXEC mode. This command disables HCCP for the specified member of the specified group. • *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. • *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive. **Note** Even if an HCCP member is locked out, it switches over in circumstances in which it is tracking another HCCP interface. This condition applies when HCCP interfaces are configured manually to track each other, or when HCCP interfaces share the same JIB, such as with the Cisco UBR10-MC 5X20.
Step 3	Repeat.	Repeat the above steps as required to prevent a working interface from switching over. This manual override can be removed when desired, and retains HCCP configuration on the interface.
Step 4	**hccp** *group* **unlockout** *member* **Example:** `Router# hccp 1 unlockout 1`	Disables the HCCP lockout feature when desired

Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces

Before You Begin

Restriction Starting with Cisco IOS Release 12.2(33)SCC and later, interface level HCCP configuration is not supported. The below configuration step is supported on Cisco IOS Release 12.2(33)SCB and earlier.

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	- Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot/subslot/port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. - *slot*—Slot where the cable interface line card resides. - *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. - *port*—Downstream port number.
Step 4	**no hccp** *group* {**working** | **protect**} *member-id* **Example:** `Router(config-if)# no hccp 1 protect 1`	Turns off HCCP, and removes the specified HCCP configuration from the specified interface. - *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive. - *member-id* — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.
Step 5	Repeat.	Repeat the above steps as required to remove HCCP configuration from all desired HCCP protect interfaces.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Disabling HCCP Revertive on Protect Cable Interfaces

The cable interface line cards pair up interfaces that share the same JIB (ASIC processor). As a result, when HCCP keepalive is enabled on paired DS channels, both DS channels in the pair switch over together if either DS channel has a keepalive failure. For example, if HCCP is configured on DS channels 0 and 1, and DS channel 0 has a keepalive failure, then DS channel 1 also fails because it shares the same JIB with DS channel 0.

When HCCP revertive is enabled on both downstream channels in the pair, the interface that experiences the keepalive failure does not revert automatically to active state. This is desirable behavior because it prevents reverting to active state prematurely—before the cause of an external failure is confirmed and remedied.

The default HCCP revertive time for HCCP interfaces is 30 minutes.

However, the JIB companion interface may act upon the default revertive time of 30 minutes. The companion interface attempts to revert to active state after 30 minutes (when HCCP revertive is enabled). This creates conflict with the failed companion interface on the same JIB.

Note Therefore, we recommend that you disable automatic HCCP revertive functions on both protect downstream channels of a JIB that use keepalive or tracking. If you have keepalive and tracking enabled, or you are using the UBR10-MC 5X20 in N+1 configuration, disable the revertive function on both protect interfaces.

To disable the HCCP revertive function on protect interfaces, do the following:

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# config terminal`	Enters global configuration mode.
Step 3	**interface cable** *slot*/*subslot*/*port* **Example:** `Router# interface cable 8/1/0`	Enters interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference. • *slot*—Slot where the cable interface line card resides. • *subslot*—(Cisco uBR10012 only) Secondary slot number of the cable interface line card. • *port*—Downstream port number.
Step 4	**nohccp** *group* **revertive** **Example:** `Router(config-if)# no hccp 2 revertive`	Disables the automatic HCCP revertive function on the protect interface. • *group* — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

What to Do Next

After configuring the redundancy scheme, you can refer to these additional sections:

Switchover Testing Tasks for N+1 Redundancy

Each of these switchover test methods below provides an opportunity to test N+1 redundancy on your Cisco uBR10012 router. Each test method results in the cable modems dropping connectivity temporarily, but staying online, with switchover to protect line cards and interfaces.

Electromagnetic relays can develop a magnetic charge over time that could interfere with normal operations. Therefore, Cisco Systems recommends periodic testing using these procedures to ensure smooth operation. The tests in this section help to improve overall system availability.

These switchover testing tasks apply to switchover from HCCP working interfaces to HCCP protect interfaces, or vice versa, when configured in N+1 redundancy.

Pre-testing System Check Procedures

As a best practice, we strongly recommend analyzing the CMTS headend status prior to switchover testing.

Caution Switchover testing with latent configuration or status problems can create disruptions in subscriber service.

Use these pre-test system checks prior to manual switchover testing:

Displaying HCCP Working and HCCP Protect Interface Status

To display a brief summary of the HCCP groups, configuration types, member numbers, and status for cable interfaces, use the **show hccp brief** command at the Cisco uBR 3x10 RF Switch prompt. rfswitch> **show hccp brief**

```
Interface Config    Grp Mbr Status
Ca5/0/0   Protect   1   3   standby
Ca7/0/0   Working   1   3   active
```

Displaying HCCP Group Status on the Cisco CMTS

As a best practice, we recommend that you perform this test prior to performing any manual switchovers. This status check verifies stable redundancy operations. Should this procedure reveal any problems with online states, resolve these problems prior to performing a manual switchover. Otherwise, manual switchover for testing purposes might create additional problems.

To display HCCP group status on the Cisco CMTS, including Cisco RF Switch information relevant to N+1 redundancy behavior, use the show hccp channel-switch command in privileged EXEC mode. This command displays status for all channel switches belonging to the specified HCCP group and HCCP member. For details on the sample output the show hccp channel-switch command, see the Example: Channel Switch Information from the Cisco uBR10012 Router, on page 101.

Displaying Cisco RF Switch Module Status on the Cisco uBR 3x10 RF Switch

As a best practice, we recommend that you perform this pretest status check prior to performing any manual switchovers. This status check confirms the online and administrative states for all modules on the Cisco uBR 3x10 RF Switch itself.

To display current module status for one or more modules on the Cisco uBR 3x10 RF Switch, use the show module all command at Cisco uBR 3x10 RF Switch prompt. For details on the show module all command sample output, see Example: Cisco 3x10 RF Switch Modules in 7+1 Mode, on page 97.

Switchover Testing Procedures

The first two procedure below describe how to test the performance of N+1 redundancy on your Cisco CMTS headend. The final procedure describes how to analyze Cisco CMTS headend status after switchover.

Testing Cisco RF Switch Relays with Manual Switchover

We recommend testing the switch relays once a week (optimal) and at least once a month (minimal). Perform these steps to test the working RF Switch relays with switchover to protect.

Tip You can toggle the relays on the switch without affecting the upconverter or any of the modems. This is important if testing the relays without actually switching any of the line cards or the corresponding upconverters. If a relay is enabled on the switch and a fail-over occurs, it will go to the proper state and not just toggle from one state to another.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**telnet ip-address /noecho** **Example:** `Router# telnet 172.16.10.3 /noecho`	Initiate configuration by connecting to the Cisco RF Switch using the console or by using a Telnet session. Either provides CLI access for initiating a switchover. If a Telnet password is set on the Cisco RF Switch, type password string, where string is the previously-defined password set on the RF Switch. The Telnet password is set using the separate set password string command in Cisco RF Switch User mode. **Note** To prevent multiple users from changing the Firmware configuration at any one time, only a single Telnet client connection can be opened at a time, regardless of whether this connection is password-protected. Telnet access to the RF Switch from the router console makes double entries when typing. One workaround is to disable local echo. For example, from the Cisco uBR10012 router CLI, use the /noecho option (as shown at left). Common Telnet disconnect methods are as follows: • Press Ctrl+Break. • Press Ctrl+].

	Command or Action	Purpose
		• Type quit or send break. Another Telnet disconnect method is as follows: • Press Ctrl+Shift 6 6 x. • Type disc 1 from the router CLI. For additional Telnet break sequences, refer to the document Standard Break Key Sequence Combinations During Password Recovery on Cisco.com.
Step 2	Do one of the following: • **test module** • **switch group-name** *x* **Example:** `rfswitch>` **`test module`** `or` `rfswitch>` **`switch 13 1`**	The test module command tests all the relays at once, and then returns to the normal working mode. **Caution** Do not use the test module command while in the protect mode. Alternately, you can test an entire bitmap with switch group-name x, where x is the RF Switch header number. For example, the switch 13 1 tests port G on slot 1 of the Cisco RF Switch.
Step 3	switch group-name 0 **Example:** `rfswitch> switch 13 0`	Use the command switch group name 0 (or idle) to disable the relays, and to return to normal working mode.

Testing HCCP Groups with Manual Switchover

Cisco Systems recommends that you perform a periodic CLI switchover test of an HCCP group from the CMTS to test the protect card and path. However, this type of switchover may take 4-6 seconds and could cause a small percentage of modems to go offline. Therefore, this test should be performed less often than previous tests, and only during off-peak hours.

SUMMARY STEPS

1. **enable**
2. **hccp** *group* **switch** *member*

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**hccp** *group* **switch** *member* **Example:** `Router# hccp 1 switch 1`	Manually switches a working CMTS with its protect CMTS peer (or vice versa).

Using the show cable modem Command After a Manual Switchover

If you are using HCCP 1+1 or N+1 redundancy, the new primary processor after a switchover automatically creates a new database of the online cable modems. Use the following procedure to force IP traffic and to display cable modem status and information.

DETAILED STEPS

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

Step 2	**show cable modem** *ip-address*
	Example:
	`Router# show cable modem 172.16.10.3`
	`MAC Address IP Address I/F MAC Prim RxPwr Timing Num BPI`
	`State Sid (db) Offset CPE Enb`
	`0000.3948.ba56 8.60.0.8 C6/0/0/U0 online 1 0.50 2138 0 N`
		Identifies the IP address of a specific cable modem to be displayed. You can also specify the IP address for a CPE device behind a cable modem, and information for that cable modem is displayed.

Step 3	**ping ip-address** **Example:** `Router# ping 172.16.10.3`	Forces IP traffic by sending an ICMP ECHO packet.

Verifying N+1 Redundancy Configuration

The following example of the show running configuration command illustrates the N+1 redundancy scheme configured on the Cisco uBR10012 router with two Cisco uBR 3x10 RF Switches:

```
Router# show running config
...
redundancy
 linecard-group 1 cable
  rf-switch name 1 rfsw1
  rf-switch name 2 rfsw2
  rf-switch protection-mode [4+1/7+1]
  rf-switch snmp-community private123
  revertive <1-35791>
  member subslot 5/0 working
  member subslot 5/1 protect
  member subslot 8/1 working
  member subslot 5/1 protect config 8/1
  mode sso
...
```

The following is a sample output of the show redundancy linecard all command in privileged EXEC mode for Global N+1 Line Card Redundancy. This redundancy configuration supports two Cisco uBR 3x10 RF Switches on the Cisco CMTS router.

```
Router# show redundancy linecard all
 hccp config sync list:
 end
 Don't generate default PHY config configuration: FALSE
 User defined PHY config configuration: FALSE
 Redundancy Mode: 7 + 1
 Linecard Redundancy Detail
 ---------------------------
Card      Config   Mbr RfSw-Name       RfSw-IP-Addr    RfSw-Slot Bitmap
card 8/0  Working  80  rfsw-2          5.37.0.20       8         0xFFFFFFFF
card 8/0  Working  80  rfsw-1          5.37.0.19       8         0xFFFFFFFF
card 7/0  Working  70  rfsw-2          5.37.0.20       7         0xFFFFFFFF
card 7/0  Working  70  rfsw-1          5.37.0.19       7         0xFFFFFFFF
 Subslot Summary
--------------------
                               RF Switch Slot*
   Subslot        Status      Current         Default
 ---------------------------------------------------------
    5/0           Unknown       -                7
    5/1           Unknown       -                P
    6/0           Unknown       -                5
    6/1           Unknown       -                6
    7/0           Working       7                3
    7/1           Unknown       -                4
    8/0           Working       8                1
    8/1           Unknown       -                2
 --------------------------------------------------------------
 NOTE:
 Legend: - = Unused; P= Protect
```

The following is a sample output of the show redundancy linecard all command in privileged EXEC mode for N+1 HCCP Redundancy. This redundancy configuration supports two Cisco uBR 3x10 RF Switches on the Cisco router.

```
Router# show redundancy linecard all
Interface Config   Grp Mbr RfSw-Name       RfSw-IP-Addr    RfSw-Slot Bitmap
Ca6/1/0   Working  1   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/1   Working  2   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/2   Working  3   61  rfsw-1          10.4.4.1        6         0xFFFFFFFF
Ca6/1/2   Working  3   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca6/1/3   Working  4   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
Ca6/1/4   Working  5   61  rfsw-2          10.4.4.2        6         0xFFFFFFFF
```

```
Ca7/0/0   Protect  1   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca7/0/0   Protect  1   61  rfsw-1          10.4.4.1        6          0xFFFFFFFF
Ca7/0/1   Protect  2   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca7/0/1   Protect  2   61  rfsw-1          10.4.4.1        6          0xFFFFFFFF
Ca7/0/2   Protect  3   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca7/0/2   Protect  3   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
Ca7/0/2   Protect  3   61  rfsw-1          10.4.4.1        6          0xFFFFFFFF
Ca7/0/2   Protect  3   61  rfsw-2          10.4.4.2        6          0xFFFFFFFF
Ca7/0/3   Protect  4   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
Ca7/0/3   Protect  4   61  rfsw-2          10.4.4.2        6          0xFFFFFFFF
Ca7/0/4   Protect  5   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
Ca7/0/4   Protect  5   61  rfsw-2          10.4.4.2        6          0xFFFFFFFF
Ca8/0/0   Working  1   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca8/0/1   Working  2   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca8/0/2   Working  3   80  rfsw-1          10.4.4.1        1          0xFFFFFFFF
Ca8/0/2   Working  3   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
Ca8/0/3   Working  4   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
Ca8/0/4   Working  5   80  rfsw-2          10.4.4.2        1          0xFFFFFFFF
```

In addition to the show redundancy linecard all command illustrated above, you can use the following command to display additional redundancy information for a specified slot:

- **show redundancy linecard all | incCa8/0/1**

The following table summarizes HCCP group and member information that is assigned to HCCP configuration on the Cisco CMTS. These factory-configured settings configure the Cable slot/subslot interfaces on the router, and supporting slot configuration on the Cisco uBR 3x10 RF Switches in either 4+1 or 7+1 redundancy.

Table 5: HCCP Member Numbers for Cisco uBR10012 Slots/ Subslots in Global N+1 Redundancy

Downstream Number	Group Number	8/0	8/1	7/0	7/1	6/0	6/1	5/0	5/1
DS 0	1	80	81	70	71	60	61	50	P1
DS 1	2	80	81	70	71	60	61	50	P1
DS 2	3	80	81	70	71	60	61	50	P1
DS 3	4	80	81	70	71	60	61	50	P1
DS 4	5	80	81	70	71	60	61	50	P1
Default RF Switch Slot (7+1 Mode)	1	2	3	4	5	6	7	P1	
Default RF Switch Slots (4+1 Mode)	5, 1	6, 2	7, 3	8, 4	-	-	-	P1, P2	

Configuration Examples for Cisco N+1 Redundancy

This section provides the following configuration examples of N+1 redundancy. Each chassis-level example below illustrates a distinct implementation of N+1 redundancy on the Cisco CMTS.

Note For configuration examples for the Cisco uBR Advanced RF Switch, see Cisco uBR Advanced RF Switch Software Configuration Guide .

Table 6: Summary Table of N+1 Configuration Examples—Cisco IOS 12.2(15)BC2a, Firmware 3.50

Example	Cisco RF Switch[3]	N+1 Mode	Cisco Router Chassis[4]	Cisco Cable Interface Line Cards
Cisco RF Switch Module Examples				
Example: Cisco 3x10 RF Switch Modules in 7+1 Mode, on page 97	3x10 RF	7+1[5]	uBR10012	Not described
Cisco uBR10012 Chassis Configuration Examples				
Examples: N+1 HCCP Redundancy in 4+1 Mode, on page 98	3x10 RF	4+1	uBR10012	UBR10-MC 5X20 (five)
Example: Channel Switch Information from the Cisco uBR10012 Router, on page 101	3x10 RF	7+13	uBR10012	Not described
Example: Global N+1 Redundancy Using the Cisco uBR-MC3GX60V Line Card , on page 113	3x10 RF (two)	7+13	uBR10012	uBR-MC3GX60V
Example: Global N+1 Redundancy Using the Cisco UBR10-MC5X20 Line Card , on page 120	3x10 RF (two)	7+13	uBR10012	UBR10-MC 5X20

Example	Cisco RF Switch[3]	N+1 Mode	Cisco Router Chassis[4]	Cisco Cable Interface Line Cards
Example: Global N+1 Redundancy Using the Cisco UBR10-LCP2-MC28C Line Card, on page 126	3x10 RF	7+13	uBR10012	UBR10-LCP2-MC28C (eight)

[3] Assume one Cisco RF Switch per example unless more are cited.

[4] Assume one Cisco router chassis per example unless more are cited.

[5] The term "7+1 Redundancy" is also referred to as "8+1 Redundancy" in the field—physically, eight line cards in "8+1" mode are configured as seven working line cards with one protect line card. Therefore, "7+1 Redundancy" is the more physically accurate term. By contrast, "4+1 Redundancy" (predictably) refers to four working line cards with one additional protect line card.

Example: Cisco 3x10 RF Switch Modules in 7+1 Mode

The following is sample output for the **show module all** command from a Cisco RF Switch that has been configured for 7+1 Redundancy:

```
rfswitch> show module all
SNMP Cache: enabled
Module   Presence  Admin   Cache   Fault
     1     online      0       0      ok
     2     online      0       0      ok
     3     online      0       0      ok
     4     online      0       0      ok
     5     online      0       0      ok
     6     online      0       0      ok
     7     online      0       0      ok
     8     online      0       0      ok
     9     online      0       0      ok
    10     online      0       0      ok
    11     online      0       0      ok
    12     online      0       0      ok
    13     online      0       0      ok
    14    offline      0       0      ok
```

The Administrative State field (Admin) indicates the following potential states:

- 0 — Indicates normal working state.
- 1-8 — Indicates that there has been a switchover and the corresponding module is in protect mode, and the header is being protected. For example, an Admin state of 8 for Module 1 would indicate a switchover for port A (Module 1) on header 8 on the Cisco RF Switch. After a switchover, verify that this Admin state corresponds with the actual wiring on the Cisco RF Switch.
- 9—Indicates fault for the specified module.

The following is sample output of the **show config** command from a Cisco 3x10 RF Switch configured in 7+1 Redundancy mode:

```
rfswitch> show config
IP addr: 10.74.59.242
Subnet mask: 255.255.255.192
MAC addr: 00-03-8F-01-13-BB
Gateway IP: 10.74.59.193
```

```
TFTP host IP: 20.4.0.2
ARP timeout: 14400 secs
DHCP lease time: infinite
TELNET inactivity timeout: 600 secs
TELNET echo mode: on
Password: (none)

SNMP Community: private
SNMP Cache: enabled
SNMP Traps: enabled
SNMP Trap Interval: 300 sec(s)
SNMP Trap Hosts: none
Card Protect Mode: 8+1
Protect Mode Reset: disabled
Slot Config: 0x03ff 0x1c00 (13 cards)
Watchdog Timeout: 20 sec(s)
Group definitions: 1
  ALL        0xffffffff
```

Note The show config command for the Cisco RF Switch contains the Card Protect Mode field. When this field displays 8+1 , this indicates that the Cisco RF Switch is configured for N+1 redundancy, where eight or less working line cards are possible. This field may also display 4+1 , where four or less working line cards are possible.

Examples: N+1 HCCP Redundancy in 4+1 Mode

The following output from the Cisco IOS show running configuration command illustrates the configuration of N+1 redundancy using the following CMTS:

- One Cisco 3x10 RF Switch configured as two working RF Switches in 4+1 mode
- One Cisco uBR10012 router
- Five Cisco UBR10-MC 5X20 broadband processing engines

The Protection mode affects the bitmaps of the Cisco RF Switch and CMTS configuration.

Note If you add one additional Cisco UBR10-MC 5X20 BPE, the entire CMTS configuration below must be changed. Refer to the cabling in the following document for additional information:

- Cabling the Cisco UBR10-MC 5X20 Cable Interface Line Card

http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/quick/start/MC52_cbl.html

Example: HCCP Working 1

The following configuration example illustrates HCCP working member 1 for five HCCP groups:

```
interface c8/0/0
hccp 1 working 1
hccp 1 channel-switch 1 rfswa rfswitch-group 10.10.10.10 44440400 1
interface c8/0/1
hccp 2 working 1
hccp 2 channel-switch 1 rfswa rfswitch-group 10.10.10.10 11110100 1
```

```
interface c8/0/2
hccp 3 working 1
hccp 3 channel-switch 1 rfswa rfswitch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfswb rfswitch-group 10.10.10.10 0000a080 1
interface c8/0/3
hccp 4 working 1
hccp 4 channel-switch 1 rfswb rfswitch-group 10.10.10.10 88880800 1
interface c8/0/4
hccp 5 working 1
hccp 5 channel-switch 1 rfswb rfswitch-group 10.10.10.10 22220200 1
```

Example: HCCP Working 2

The following configuration example illustrates HCCP working member 2 for five HCCP groups:

```
interface c8/1/0
hccp 1 working 2
hccp 1 channel-switch 2 rfswa rfswitch-group 10.10.10.10 44440400 2
interface c8/1/1
hccp 2 working 2
hccp 2 channel-switch 2 rfswa rfswitch-group 10.10.10.10 11110100 2
interface c8/1/2
hccp 3 working 2
hccp 3 channel-switch 2 rfswa rfswitch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfswb rfswitch-group 10.10.10.10 0000a080 2
interface c8/1/3
hccp 4 working 2
hccp 4 channel-switch 2 rfswb rfswitch-group 10.10.10.10 88880800 2
interface c8/1/4
hccp 5 working 2
hccp 5 channel-switch 2 rfswb rfswitch-group 10.10.10.10 22220200 2
```

Example: HCCP Working 3

The following configuration example illustrates HCCP working member 3 for five HCCP groups:

```
interface c7/0/0
hccp 1 working 3
hccp 1 channel-switch 3 rfswa rfswitch-group 10.10.10.10 44440400 3
interface c7/0/1
hccp 2 working 3
hccp 2 channel-switch 3 rfswa rfswitch-group 10.10.10.10 11110100 3
interface c7/0/2
hccp 3 working 3
hccp 3 channel-switch 3 rfswa rfswitch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfswb rfswitch-group 10.10.10.10 0000a080 3
interface c7/0/3
hccp 4 working 3
hccp 4 channel-switch 3 rfswb rfswitch-group 10.10.10.10 88880800 3
interface c7/0/4
hccp 5 working 3
hccp 5 channel-switch 3 rfswb rfswitch-group 10.10.10.10 22220200 3
```

Example: HCCP Working 4

The following configuration example illustrates HCCP working member 4 for five HCCP groups:

```
interface c7/1/0
hccp 1 working 4
hccp 1 channel-switch 4 rfswa rfswitch-group 10.10.10.10 44440400 4
interface c7/1/1
hccp 2 working 4
hccp 2 channel-switch 4 rfswa rfswitch-group 10.10.10.10 11110100 4
interface c7/1/2
```

```
hccp 3 working 4
hccp 3 channel-switch 4 rfswa rfswitch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfswb rfswitch-group 10.10.10.10 0000a080 4
interface c7/1/3
hccp 4 working 4
hccp 4 channel-switch 4 rfswb rfswitch-group 10.10.10.10 88880800 4
interface c7/1/4
hccp 5 working 4
```

HCCP Protect Interface Configuration Examples

The following examples illustrate the four HCCP protect members for five HCCP groups:

```
interface c5/1/0
hccp 1 protect 1 10.10.10.1
hccp 1 channel-switch 1 rfswa rfswitch-group 10.10.10.10 44440400 1
hccp 1 protect 2 10.10.10.1
hccp 1 channel-switch 2 rfswa rfswitch-group 10.10.10.10 44440400 2
hccp 1 protect 3 10.10.10.1
hccp 1 channel-switch 3 rfswa rfswitch-group 10.10.10.10 44440400 3
hccp 1 protect 4 10.10.10.1
hccp 1 channel-switch 4 rfswa rfswitch-group 10.10.10.10 44440400 4
interface c5/1/1
hccp 2 protect 1 10.10.10.1
hccp 2 channel-switch 1 rfswa rfswitch-group 10.10.10.10 11110100 1
hccp 2 protect 2 10.10.10.1
hccp 2 channel-switch 2 rfswa rfswitch-group 10.10.10.10 11110100 2
hccp 2 protect 3 10.10.10.1
hccp 2 channel-switch 3 rfswa rfswitch-group 10.10.10.10 11110100 3
hccp 2 protect 4 10.10.10.1
hccp 2 channel-switch 4 rfswa rfswitch-group 10.10.10.10 11110100 4
interface c5/1/2
hccp 3 protect 1 10.10.10.1
hccp 3 channel-switch 1 rfswa rfswitch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfswb rfswitch-group 10.10.10.10 0000a080 1
hccp 3 protect 2 10.10.10.1
hccp 3 channel-switch 2 rfswa rfswitch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfswb rfswitch-group 10.10.10.10 0000a080 2
hccp 3 protect 3 10.10.10.1
hccp 3 channel-switch 3 rfswa rfswitch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfswb rfswitch-group 10.10.10.10 0000a080 3
hccp 3 protect 4 10.10.10.1
hccp 3 channel-switch 4 rfswa rfswitch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfswb rfswitch-group 10.10.10.10 0000a080 4
interface c5/1/3
hccp 4 protect 1 10.10.10.1
hccp 4 channel-switch 1 rfswb rfswitch-group 10.10.10.10 88880800 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfswb rfswitch-group 10.10.10.10 88880800 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfswb rfswitch-group 10.10.10.10 88880800 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfswb rfswitch-group 10.10.10.10 88880800 4
interface c5/1/4
hccp 5 protect 1 10.10.10.1
hccp 5 channel-switch 1 rfswb rfswitch-group 10.10.10.10 22220200 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfswb rfswitch-group 10.10.10.10 22220200 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfswb rfswitch-group 10.10.10.10 22220200 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfswb rfswitch-group 10.10.10.10 22220200 4
```

Example: Channel Switch Information from the Cisco uBR10012 Router

The following is a sample output of the show hccp channel-switch command that provides information about the channel switch activity with Global N+1 Line Card Redundancy:

```
Router# show hccp channel-switch
Grp 1 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 2 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 3 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 4 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 5 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 6 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 7 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 8 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 9 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 10 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 11 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 12 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 13 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 14 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 15 Mbr 70 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 1 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 2 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
  "rfsw-1" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
    module 7  (Upstream)    normal
    module 8  (Upstream)    normal
    module 9  (Upstream)    normal
    module 10 (Upstream)    normal
    module 11 (Downstream)  normal
    module 12 (Downstream)  normal
    module 13 (Downstream)  normal
Grp 3 Mbr 80 Working channel-switch:
  "rfsw-2" - Configured 10/3, Detected 10/3
    module 1  (Upstream)    normal
    module 2  (Upstream)    normal
    module 3  (Upstream)    normal
    module 4  (Upstream)    normal
    module 5  (Upstream)    normal
    module 6  (Upstream)    normal
```

```
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 4 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 5 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 6 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 7 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 8 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 9 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 10 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 11 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 12 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
    "rfsw-1" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
      module 9  (Upstream)    normal
      module 10 (Upstream)    normal
      module 11 (Downstream)  normal
      module 12 (Downstream)  normal
      module 13 (Downstream)  normal
  Grp 13 Mbr 80 Working channel-switch:
    "rfsw-2" - Configured 10/3, Detected 10/3
      module 1  (Upstream)    normal
      module 2  (Upstream)    normal
      module 3  (Upstream)    normal
      module 4  (Upstream)    normal
      module 5  (Upstream)    normal
      module 6  (Upstream)    normal
      module 7  (Upstream)    normal
      module 8  (Upstream)    normal
```

```
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
      "rfsw-1" - Configured 10/3, Detected 10/3
        module 1  (Upstream)    normal
        module 2  (Upstream)    normal
        module 3  (Upstream)    normal
        module 4  (Upstream)    normal
        module 5  (Upstream)    normal
        module 6  (Upstream)    normal
        module 7  (Upstream)    normal
        module 8  (Upstream)    normal
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
    Grp 14 Mbr 80 Working channel-switch:
      "rfsw-2" - Configured 10/3, Detected 10/3
        module 1  (Upstream)    normal
        module 2  (Upstream)    normal
        module 3  (Upstream)    normal
        module 4  (Upstream)    normal
        module 5  (Upstream)    normal
        module 6  (Upstream)    normal
        module 7  (Upstream)    normal
        module 8  (Upstream)    normal
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
      "rfsw-1" - Configured 10/3, Detected 10/3
        module 1  (Upstream)    normal
        module 2  (Upstream)    normal
        module 3  (Upstream)    normal
        module 4  (Upstream)    normal
        module 5  (Upstream)    normal
        module 6  (Upstream)    normal
        module 7  (Upstream)    normal
        module 8  (Upstream)    normal
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
    Grp 15 Mbr 80 Working channel-switch:
      "rfsw-2" - Configured 10/3, Detected 10/3
        module 1  (Upstream)    normal
        module 2  (Upstream)    normal
        module 3  (Upstream)    normal
        module 4  (Upstream)    normal
        module 5  (Upstream)    normal
        module 6  (Upstream)    normal
        module 7  (Upstream)    normal
        module 8  (Upstream)    normal
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
      "rfsw-1" - Configured 10/3, Detected 10/3
        module 1  (Upstream)    normal
        module 2  (Upstream)    normal
        module 3  (Upstream)    normal
        module 4  (Upstream)    normal
        module 5  (Upstream)    normal
        module 6  (Upstream)    normal
        module 7  (Upstream)    normal
        module 8  (Upstream)    normal
        module 9  (Upstream)    normal
        module 10 (Upstream)    normal
        module 11 (Downstream)  normal
        module 12 (Downstream)  normal
        module 13 (Downstream)  normal
    RFswitch relay test in 2w5d
    RFswitch polling count = 2585/0
```

The following is a sample output of the show hccp channel-switch command that provides information about the channel switch activity with N+1 HCCP Redundancy:

```
Router# show hccp channel-switch
Grp 1 Mbr 1 Working channel-switch:
 "uc" - enabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
Grp 2 Mbr 1 Working channel-switch:
  "uc" - enabled, frequency 555000000 Hz
  "rfswitch" - module 2, normal
  module 4, normal
  module 6, normal
  module 9, normal
  module 13, normal
Grp 1 Mbr 7 Protect channel-switch:
 "uc" - disabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
Grp 1 Mbr 5 Protect channel-switch:
 "uc" - disabled, frequency 555000000 Hz
 "rfswitch" - module 1, normal
 module 3, normal
 module 5, normal
 module 7, normal
 module 11, normal
```

Example: Global N+1 Redundancy Using the Cisco uBR-MC3GX60V Line Card

The following output from the show run command illustrates the configuration of N+1 redundancy in remote learn DEPI mode on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco uBR-MC3GX60V line cards:

Router# show run

```
!
On the Cisco CMTS router
!
card 5/1 ubr10k-clc-3g60 license 72X60
card 7/1 ubr10k-clc-3g60 license 72X60
card 8/1 ubr10k-clc-3g60 license 72X60
l2tp-class l2tp_class_gi7_1
!
l2tp-class l2tp_class_gi8_1
depi-class depi_class_gi7_1
 mode mpt
!
depi-class depi_class_gi8_1
 mode mpt
!
depi-tunnel gi7_1
 dest-ip 60.3.2.9
 l2tp-class l2tp_class_gi7_1
 depi-class depi_class_gi7_1
 protect-tunnel qam5_pt
```

```
!
depi-tunnel gi8_1
 dest-ip 60.3.2.13
 l2tp-class l2tp_class_gi8_1
 depi-class depi_class_gi8_1
 protect-tunnel qam5_pt
!
depi-tunnel qam5_pt
 dest-ip 60.6.2.13

redundancy
 linecard-group 1 cable
  rf-switch protection-mode 4+1
  rf-switch name 1 rfsw1
  member subslot 5/1 protect
  member subslot 7/1 working rfsw-slot 2
  member subslot 8/1 working rfsw-slot 3
  member subslot 5/1 protect config 7/1
  mode sso
!
controller Modular-Cable 7/1/0
 rf-channel 0 cable downstream channel-id 9
 rf-channel 0 frequency 303000000 annex B modulation 256qam interleave 32
 rf-channel 0 depi-tunnel gi7_1 tsid 38009
 rf-channel 0 rf-power 52.0
 no rf-channel 0 rf-shutdown
 rf-channel 1 cable downstream channel-id 10
 rf-channel 1 frequency 309000000 annex B modulation 256qam interleave 32
 rf-channel 1 depi-tunnel gi7_1 tsid 38010
 rf-channel 1 rf-power 52.0
 no rf-channel 1 rf-shutdown
 rf-channel 2 cable downstream channel-id 11
 rf-channel 2 frequency 315000000 annex B modulation 256qam interleave 32
 rf-channel 2 depi-tunnel gi7_1 tsid 38011
 rf-channel 2 rf-power 52.0
 no rf-channel 2 rf-shutdown
 rf-channel 3 cable downstream channel-id 12
 rf-channel 3 frequency 321000000 annex B modulation 256qam interleave 32
 rf-channel 3 depi-tunnel gi7_1 tsid 38012
 rf-channel 3 rf-power 52.0
 no rf-channel 3 rf-shutdown
 rf-channel 4 cable downstream channel-id 13
 rf-channel 4 frequency 327000000 annex B modulation 256qam interleave 32
 rf-channel 4 depi-tunnel gi7_1 tsid 38013
 rf-channel 4 rf-power 52.0
 no rf-channel 4 rf-shutdown
 rf-channel 5 cable downstream channel-id 14
 rf-channel 5 frequency 333000000 annex B modulation 256qam interleave 32
 rf-channel 5 depi-tunnel gi7_1 tsid 38014
 rf-channel 5 rf-power 52.0
 no rf-channel 5 rf-shutdown
 rf-channel 6 cable downstream channel-id 15
 rf-channel 6 frequency 339000000 annex B modulation 256qam interleave 32
 rf-channel 6 depi-tunnel gi7_1 tsid 38015
 rf-channel 6 rf-power 52.0
 no rf-channel 6 rf-shutdown
 rf-channel 7 cable downstream channel-id 16
 rf-channel 7 frequency 345000000 annex B modulation 256qam interleave 32
 rf-channel 7 depi-tunnel gi7_1 tsid 38016
 rf-channel 7 rf-power 52.0
 no rf-channel 7 rf-shutdown
 rf-channel 8 cable downstream channel-id 81
 rf-channel 9 cable downstream channel-id 82
 rf-channel 10 cable downstream channel-id 83
 rf-channel 11 cable downstream channel-id 84
 rf-channel 12 cable downstream channel-id 85
 rf-channel 13 cable downstream channel-id 86
 rf-channel 14 cable downstream channel-id 87
 rf-channel 15 cable downstream channel-id 88
 rf-channel 16 cable downstream channel-id 89
 rf-channel 17 cable downstream channel-id 90
 rf-channel 18 cable downstream channel-id 91
 rf-channel 19 cable downstream channel-id 92
 rf-channel 20 cable downstream channel-id 93
 rf-channel 21 cable downstream channel-id 94
 rf-channel 22 cable downstream channel-id 95
 rf-channel 23 cable downstream channel-id 96
!
controller Modular-Cable 8/1/0
 rf-channel 0 cable downstream channel-id 17
 rf-channel 0 frequency 351000000 annex B modulation 256qam interleave 32
 rf-channel 0 depi-tunnel gi8_1 tsid 38017
 no rf-channel 0 rf-shutdown
 rf-channel 1 cable downstream channel-id 18
 rf-channel 1 frequency 357000000 annex B modulation 256qam interleave 32
 rf-channel 1 depi-tunnel gi8_1 tsid 38018
 no rf-channel 1 rf-shutdown
 rf-channel 2 cable downstream channel-id 19
 rf-channel 2 frequency 363000000 annex B modulation 256qam interleave 32
 rf-channel 2 depi-tunnel gi8_1 tsid 38019
 no rf-channel 2 rf-shutdown
 rf-channel 3 cable downstream channel-id 20
 rf-channel 3 frequency 369000000 annex B modulation 256qam interleave 32
 rf-channel 3 depi-tunnel gi8_1 tsid 38020
 no rf-channel 3 rf-shutdown
 rf-channel 4 cable downstream channel-id 21
 rf-channel 4 frequency 375000000 annex B modulation 256qam interleave 32
 rf-channel 4 depi-tunnel gi8_1 tsid 38021
 no rf-channel 4 rf-shutdown
 rf-channel 5 cable downstream channel-id 22
 rf-channel 5 frequency 381000000 annex B modulation 256qam interleave 32
 rf-channel 5 depi-tunnel gi8_1 tsid 38022
 no rf-channel 5 rf-shutdown
 rf-channel 6 cable downstream channel-id 23
 rf-channel 6 frequency 387000000 annex B modulation 256qam interleave 32
 rf-channel 6 depi-tunnel gi8_1 tsid 38023
 no rf-channel 6 rf-shutdown
 rf-channel 7 cable downstream channel-id 24
 rf-channel 7 frequency 393000000 annex B modulation 256qam interleave 32
 rf-channel 7 depi-tunnel gi8_1 tsid 38024
 no rf-channel 7 rf-shutdown
 rf-channel 8 cable downstream channel-id 81
 rf-channel 9 cable downstream channel-id 82
 rf-channel 10 cable downstream channel-id 83
 rf-channel 11 cable downstream channel-id 84
 rf-channel 12 cable downstream channel-id 85
 rf-channel 13 cable downstream channel-id 86
 rf-channel 14 cable downstream channel-id 87
 rf-channel 15 cable downstream channel-id 88
 rf-channel 16 cable downstream channel-id 89
 rf-channel 17 cable downstream channel-id 90
 rf-channel 18 cable downstream channel-id 91
 rf-channel 19 cable downstream channel-id 92
 rf-channel 20 cable downstream channel-id 93
 rf-channel 21 cable downstream channel-id 94
 rf-channel 22 cable downstream channel-id 95
 rf-channel 23 cable downstream channel-id 96
!
interface Cable7/1/0
 downstream Modular-Cable 1/0/0 rf-channel 0 upstream 0-3
 downstream Modular-Cable 7/1/0 rf-channel 0 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 1
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 cable upstream 0 attribute-mask 20000000
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 16400000
 cable upstream 1 channel-width 6400000 6400000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 1
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 cable upstream 1 attribute-mask 20000000
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 23800000
 cable upstream 2 channel-width 6400000 6400000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 1
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 30200000
 cable upstream 3 channel-width 6400000 6400000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 1
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
!
interface GigabitEthernet7/1/0
 ip address 60.3.2.10 255.255.255.252
 negotiation auto
!
interface Modular-Cable7/1/0:0
 cable bundle 1
 cable rf-bandwidth-percent 36
!
interface Wideband-Cable7/1/0:3
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
!
interface Wideband-Cable7/1/0:4
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
!
interface Wideband-Cable7/1/0:8
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
 cable rf-channel 4 bandwidth-percent 20
 cable rf-channel 5 bandwidth-percent 20
 cable rf-channel 6 bandwidth-percent 20
 cable rf-channel 7 bandwidth-percent 20
!
interface Cable8/1/0
 downstream Modular-Cable 1/0/0 rf-channel 1 upstream 0-3
 downstream Modular-Cable 8/1/0 rf-channel 0 upstream 0-3
 cable mtc-mode
 no cable packet-cache
 cable bundle 1
 cable upstream max-ports 4
 cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes A0000000
 cable upstream 0 connector 0
 cable upstream 0 frequency 10000000
 cable upstream 0 channel-width 6400000 6400000
 cable upstream 0 docsis-mode atdma
 cable upstream 0 minislot-size 1
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 221
 cable upstream 0 attribute-mask 20000000
 no cable upstream 0 shutdown
 cable upstream 1 connector 0
 cable upstream 1 frequency 16400000
 cable upstream 1 channel-width 6400000 6400000
 cable upstream 1 docsis-mode atdma
 cable upstream 1 minislot-size 1
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 221
 cable upstream 1 attribute-mask 20000000
 no cable upstream 1 shutdown
 cable upstream 2 connector 0
 cable upstream 2 frequency 23800000
 cable upstream 2 channel-width 6400000 6400000
 cable upstream 2 docsis-mode atdma
 cable upstream 2 minislot-size 1
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 221
 cable upstream 2 attribute-mask 20000000
 no cable upstream 2 shutdown
 cable upstream 3 connector 0
 cable upstream 3 frequency 30200000
 cable upstream 3 channel-width 6400000 6400000
 cable upstream 3 docsis-mode atdma
 cable upstream 3 minislot-size 1
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 221
 cable upstream 3 attribute-mask 20000000
 no cable upstream 3 shutdown
interface GigabitEthernet8/1/0
 ip address 60.3.2.14 255.255.255.252
 negotiation auto
!
interface Modular-Cable8/1/0:0
 cable bundle 1
 cable rf-bandwidth-percent 36
!
interface Wideband-Cable8/1/0:3
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
!
interface Wideband-Cable8/1/0:4
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
!
interface Wideband-Cable8/1/0:8
 cable multicast-qos group 22
 cable multicast-qos group 21
 cable bundle 1
 cable rf-channel 0 bandwidth-percent 20
 cable rf-channel 1 bandwidth-percent 20
 cable rf-channel 2 bandwidth-percent 20
 cable rf-channel 3 bandwidth-percent 20
 cable rf-channel 4 bandwidth-percent 20
 cable rf-channel 5 bandwidth-percent 20
 cable rf-channel 6 bandwidth-percent 20
 cable rf-channel 7 bandwidth-percent 20
!
interface Bundle1
 ip address 30.0.42.1 255.255.255.0 secondary
 ip address 30.0.43.254 255.255.255.0 secondary
 ip address 30.0.44.254 255.255.255.0 secondary
 ip address 30.0.41.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 cable dhcp-giaddr policy
 cable helper-address 20.1.0.9
!
On the Cisco RF Switch
!
l2tp-class l2tp_class_gi7_1
l2tp-class l2tp_class_gi8_1
depi-class depi_class_gi7_1
 mode mpt
depi-class depi_class_gi8_1
 mode mpt
depi-tunnel gi8_1
 dest-ip 60.3.2.14
 l2tp-class l2tp_class_gi8_1
 depi-class depi_class_gi8_1
 protect-tunnel qam5_pt
!
depi-tunnel gi7_1
 dest-ip 60.3.2.10
 l2tp-class l2tp_class_gi7_1
 depi-class depi_class_gi7_1
 protect-tunnel qam5_pt
!
depi-tunnel qam5_pt
 dest-ip 60.6.2.14
interface GigabitEthernet5/14
 no switchport
 ip address 60.3.2.9 255.255.255.252 secondary
 ip address 60.3.2.13 255.255.255.252
 no ip redirects
!
interface Qam5/3.1
 cable mode depi remote learn
 cable downstream tsid 38009
 depi depi-tunnel gi7_1
!
interface Qam5/3.2
 cable mode depi remote learn
 cable downstream tsid 38010
 depi depi-tunnel gi7_1
!
interface Qam5/3.3
 cable mode depi remote learn
 cable downstream tsid 38011
 depi depi-tunnel gi7_1
!
interface Qam5/3.4
 cable mode depi remote learn
 cable downstream tsid 38012
 depi depi-tunnel gi7_1
!
interface Qam3/5.1
 cable mode depi remote learn
 cable downstream tsid 38013
 depi depi-tunnel gi7_1
!
interface Qam3/5.2
 cable mode depi remote learn
 cable downstream tsid 38014
 depi depi-tunnel gi7_1
!
interface Qam3/5.3
 cable mode depi remote learn
 cable downstream tsid 38015
 depi depi-tunnel gi7_1
!
interface Qam3/5.4
 cable mode depi remote learn
 cable downstream tsid 38016
 depi depi-tunnel gi7_1
!
interface Qam5/1
 no ip address
!
interface Qam5/1.1
 cable mode depi remote learn
 cable downstream tsid 38017
 depi depi-tunnel gi8_1
!
interface Qam5/1.2
 cable mode depi remote learn
 cable downstream tsid 38018
 depi depi-tunnel gi8_1
!
interface Qam5/1.3
 cable mode depi remote learn
 cable downstream tsid 38019
 depi depi-tunnel gi8_1
!
interface Qam5/1.4
 cable mode depi remote learn
 cable downstream tsid 38020
 depi depi-tunnel gi8_1
!
interface Qam5/2
 no ip address
!
interface Qam5/2.1
 cable mode depi remote learn
 cable downstream tsid 38021
 depi depi-tunnel gi8_1
!
interface Qam5/2.2
 cable mode depi remote learn
 cable downstream tsid 38022
 depi depi-tunnel gi8_1
!
interface Qam5/2.3
 cable mode depi remote learn
 cable downstream tsid 38023
 depi depi-tunnel gi8_1
!
interface Qam5/2.4
 cable mode depi remote learn
 cable downstream tsid 38024
 depi depi-tunnel gi8_1
!
```

Example: Global N+1 Redundancy Using the Cisco UBR10-MC5X20 Line Card

The following output from the show run command illustrates configuration of N+1 redundancy on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco UBR10-MC 5X20 line cards:

```
Router# show run
Current configuration : 8567 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-15.BC1
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
!
!  Use this modulation profile if using current released BC3 IOS and 16-QAM is required.
!  A-TDMA IOS has different modulation profiles and requirements.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
 frequency 453000000
 service-class 1 max-upstream 10000
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1522
!
redundancy
  main-cpu
    auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigethernet-1
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 5/0 5cable-mc520s-d
card 5/1 5cable-mc520s-d
card 6/0 5cable-mc520s-d
card 6/1 5cable-mc520s-d
card 7/0 5cable-mc520s-d
card 7/1 5cable-mc520s-d
card 8/0 5cable-mc520s-d
card 8/1 5cable-mc520s-d
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
!  This is set for console access from the 10012 router to the Switch.
!  The IP address is for Loopback0.
!
ip dhcp pool MODEMS1
   network 172.25.1.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.1.1
   default-router 172.25.1.1
   option 7 ip 172.25.1.1
   option 4 ip 172.25.1.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp pool MODEMS2
   network 172.25.2.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.2.1
   default-router 172.25.2.1
   option 7 ip 172.25.2.1
   option 4 ip 172.25.2.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
!  An internal DHCP server is used in this example instead of external servers
!  (cable helper, TOD, TFTP, etc.).  External servers are recommended in a genuine
!  production network.
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
 ip address 10.97.1.8 255.255.255.0
 ip rip receive version 2
 no ip split-horizon
 no keepalive
!
interface GigabitEthernet1/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet2/0/0
 no ip address
 negotiation auto
!
!  Sample Interface Config for N+1: (This assumes rfsw2 is on the top as shown in
!  the RF Switch Cabling document).  Other interfaces will be the same except a
!  different member number for each HCCP group.
!
interface Cable5/1/0
!
!  This is the Protect interface for the first HCCP group.  It may be best to configure
!  the Protect interface(s) last; after the Working interfaces are configured,
!  or to keep the interface "shut" (disabled) until all configurations are completed.
!
 no ip address
!
!  There is no need to set the IP address because it comes from the Working card via SNMP.
!
 no keepalive
!
!  This is defaulted to 10 seconds with the N+1 IOS code, but should be disabled on
!  the Protect interface or set relatively high.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
!
!  The DS modulation and Interleave must be the same on the Protect and Working interfaces
 !  of the same HCCP group. The Protect interface itself must be "no shut" (enabled)
!  for HCCP to activate
!
 cable downstream rf-shutdown
 cable upstream 0 shutdown
!
!  These interfaces automatically become "no shut" (enabled) when a switchover occurs.
!
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 hccp 1 protect 1 10.10.10.1
!
!  This is the first HCCP group and it is protecting member 1 with member 1's
!  FE IP address.  If it is intra-chassis, you can use the Loopback0 IP address.
!
 hccp 1 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of the RF Switch and it is protecting member 1, which
!  has a bitmap of AA200000 in Switch slot 1.
!
 hccp 1 protect 2 10.10.10.1
!
!  This is the first HCCP group and it is protecting member 2 with the loopback
!  IP address.
!
 hccp 1 channel-switch 2 rfsw2 rfswitch-group 10.97.1.20 AA200000 2
!
!  This is the IP address of the RF Switch and it is protecting member 2, with a
!  bitmap of AA200000 in Switch slot 2.
!
 hccp 1 protect 3 10.10.10.1
 hccp 1 channel-switch 3 rfsw2 rfswitch-group 10.97.1.20 AA200000 3
 hccp 1 protect 4 10.10.10.1
 hccp 1 channel-switch 4 rfsw2 rfswitch-group 10.97.1.20 AA200000 4
 hccp 1 protect 5 10.10.10.1
 hccp 1 channel-switch 5 rfsw2 rfswitch-group 10.97.1.20 AA200000 5
 hccp 1 protect 6 10.10.10.1
 hccp 1 channel-switch 6 rfsw2 rfswitch-group 10.97.1.20 AA200000 6
 hccp 1 protect 7 10.10.10.1
 hccp 1 channel-switch 7 rfsw2 rfswitch-group 10.97.1.20 AA200000 7
!
!  These channel-switch configurations can be copied and pasted into their respective
!  Working interfaces.
!
 hccp 1 timers 5000 15000
!
!  Cisco IOS command = hccp 1 timers <hellotime> <holdtime>
!  This is mostly for inter-chassis communication, so set it high for the uBR10012
!  as this can create extra CPU load.
!
 no hccp 1 revertive
!
interface Cable5/1/1
!
!  This is the Protect interface for the second group.
!
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 !
 hccp 2 protect 1 10.10.10.1
 hccp 2 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 55100000 1
!
!  Because this MAC domain is on right side of header, the bitmap in
!  hexadecimal code is 55100000.
!
 hccp 2 protect 2 10.10.10.1
 hccp 2 channel-switch 2 rfsw2 rfswitch-group 10.97.1.20 55100000 2
 hccp 2 protect 3 10.10.10.1
 hccp 2 channel-switch 3 rfsw2 rfswitch-group 10.97.1.20 55100000 3
 hccp 2 protect 4 10.10.10.1
 hccp 2 channel-switch 4 rfsw2 rfswitch-group 10.97.1.20 55100000 4
 hccp 2 protect 5 10.10.10.1
 hccp 2 channel-switch 5 rfsw2 rfswitch-group 10.97.1.20 55100000 5
 hccp 2 protect 6 10.10.10.1
 hccp 2 channel-switch 6 rfsw2 rfswitch-group 10.97.1.20 55100000 6
 hccp 2 protect 7 10.10.10.1
 hccp 2 channel-switch 7 rfsw2 rfswitch-group 10.97.1.20 55100000 7
 hccp 2 timers 5000 15000
 no hccp 2 revertive
interface Cable5/1/2
!
!  This is the Protect interface for the third group.
!
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 hccp 3 protect 1 10.10.10.1
 hccp 3 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 00C80000 1
 hccp 3 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 00C00000 1
!
!  Because the third MAC domain will traverse both Switches, two statements are needed.
!  The "00" in front of the bitmaps are dropped when viewing the running configuration.
!
 no hccp 3 revertive
interface Cable5/1/3
!
!  This is the Protect interface for the fourth group.
!
 hccp 4 protect 1 10.10.10.1
 hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
 hccp 4 protect 2 10.10.10.1
 hccp 4 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 AA200000 2
 hccp 4 protect 3 10.10.10.1
 hccp 4 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 AA200000 3
 hccp 4 protect 4 10.10.10.1
 hccp 4 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 AA200000 4
 hccp 4 protect 5 10.10.10.1
 hccp 4 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 AA200000 5
 hccp 4 protect 6 10.10.10.1
 hccp 4 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 AA200000 6
 hccp 4 protect 7 10.10.10.1
 hccp 4 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 AA200000 7
 no hccp 4 revertive
.
interface Cable5/1/4
!
!  This is the Protect interface for the fifth group.
!
 hccp 5 protect 1 10.10.10.1
 hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
 hccp 5 protect 2 10.10.10.1
 hccp 5 channel-switch 2 rfsw1 rfswitch-group 10.97.1. 19 55100000 2
 hccp 5 protect 3 10.10.10.1
 hccp 5 channel-switch 3 rfsw1 rfswitch-group 10.97.1. 19 55100000 3
 hccp 5 protect 4 10.10.10.1
 hccp 5 channel-switch 4 rfsw1 rfswitch-group 10.97.1. 19 55100000 4
 hccp 5 protect 5 10.10.10.1
 hccp 5 channel-switch 5 rfsw1 rfswitch-group 10.97.1. 19 55100000 5
 hccp 5 protect 6 10.10.10.1
 hccp 5 channel-switch 6 rfsw1 rfswitch-group 10.97.1. 19 55100000 6
 hccp 5 protect 7 10.10.10.1
 hccp 5 channel-switch 7 rfsw1 rfswitch-group 10.97.1. 19 55100000 7
.
.
```

```
.
!  Interface configurations continue as such for the remaining Protect interfaces.
!
interface Cable8/1/0
!
!  This is the Working interface for the first group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.1.1 255.255.255.0
!
!  Interface bundling is supported as are subinterfaces.
!
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
!
!  The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!  Only set this value after modems have stabilized.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
!
!  This is the DS frequency, which must be set for the internal upconverter to operate.
!
 cable downstream channel-id 0
 no cable downstream rf-shutdown
!
!  This is needed to turn on the DS RF output.
!
 cable upstream 0 frequency 24000000
!
!  If doing dense mode combining, the upstream frequencies will need to be different.
!  If no two US ports are shared, the same frequency can be used.
!
 cable upstream 0 power-level 0
 cable upstream 0 connector 0
!
cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 22
 no cable upstream 0 shutdown
.
.
.
 cable dhcp-giaddr policy
!
!  This tells cable modems to get an IP address from the primary scope and CPEs to use
!  the secondary scope.
!
 hccp 1 working 1
!
!  This is Working member 1 of HCCP Group 1.
!
hccp 1 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of Switch & member 1, which has a bitmap of
!  AA200000 in Switch slot 1.
!
 hccp 1 reverttime 120
!
!  This is the time in minutes (+ 2 minute suspend) for the card to switch back to
!  normal mode if the fault has cleared.  If a fault was initiated by a keepalive
!  and you had a fault on the Protect card, it would revert back after the suspend
!  time and not wait the full revert time.
!
interface Cable8/1/1
!
!  This is the Working interface for the second HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.2.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 1
 no cable downstream rf-shutdown
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 cable upstream 0 connector 4
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 22
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
.
.
.
 cable dhcp-giaddr policy
 hccp 2 working 1
!
!  This is Working member 1 of HCCP Group 2.
!
 hccp 2 channel-switch 1 rfsw2 rfswitch-group 10.97.1.20 55100000 1
!
!  This is the IP address of Switch & Member 1 of Group 2, which has a bitmap of
!  55100000 in Switch slot 1.
!
 hccp 2 reverttime 120
!
interface Cable8/1/2
!
!  This is the Working interface for the third HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.3.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 2
 no cable downstream rf-shutdown
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 cable upstream 0 connector 8
 cable upstream 0 channel-width 3200000
 cable upstream 0 minislot-size 2
 cable upstream 0 modulation-profile 22
 no cable upstream 0 shutdown
 cable dhcp-giaddr policy
.
.
.
 hccp 3 working 1
!
!  This is the Working member 1 of HCCP Group 3.
!
 hccp 3 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 00c80000 1
 hccp 3 channel-switch 1 rfsw2 rfswitch-group 10. 97.1.20 00c00000 1
 hccp 3 reverttime 120
interface Cable8/1/3
!
!  This is the Working interface for the fourth HCCP group.
!
 hccp 4 working 1
 hccp 4 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 AA200000 1
 hccp 4 reverttime 120
interface Cable8/1/4
!
```

```
!  This is the Working interface for the fifth HCCP group.
!
 hccp 5 working 1
 hccp 5 channel-switch 1 rfsw1 rfswitch-group 10.97.1.19 55100000 1
 hccp 5 reverttime 120
!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
!  This does not affect the HCCP communications between the Switch and uBR10012.
!
snmp-server enable traps cable
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
alias exec t configure terminal
alias exec scm show cable modem
alias exec scr sh cab mode remote
alias exec shb sh hccp br
alias exec shd sh hccp detail
alias exec shc sh hccp chan
!
line con 0
 logging synchronous
line aux 0
 no exec
 transport input all
!
!  The three lines above were used to console from the Auxiliary port of the uBR10012
!  to the Switch.
!
line vty 0 4
 session-timeout 400
 password xx
 login
endBuilding configuration...
```

Example: Global N+1 Redundancy Using the Cisco UBR10-LCP2-MC28C Line Card

The following output from the show run command illustrates configuration of N+1 redundancy on the Cisco CMTS router with two Cisco RF Switches, each in 7+1 mode, and Cisco UBR10-LCP2-MC28C line cards:

```
Router# show run
Current configuration : 8567 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR10k
!
boot system flash slot0: ubr10k-k8p6-mz.122-4.BC1b
logging rate-limit console all 10 except critical
enable secret 5 $1$.Dvy$fcPOhshUNjyfePH73FHRG.
!
no cable qos permission create
no cable qos permission update
```

```
cable qos permission modems
cable time-server
!
cable config-file docsis.cm
 frequency 453000000
 service-class 1 max-upstream 10000
 service-class 1 max-downstream 10000
 service-class 1 max-burst 1522
!
redundancy
  main-cpu
    auto-sync standard
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
card 1/0 1gigethernet-1
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 5/0 2cable-mc28c
card 5/1 2cable-mc28c
card 6/0 2cable-mc28c
card 6/1 2cable-mc28c
card 7/0 2cable-mc28c
card 7/1 2cable-mc28c
card 8/0 2cable-mc28c
card 8/1 2cable-mc28c
ip subnet-zero
ip host rfswitch 2001 10.10.10.1
!
!  This is set for console access from the uBR10012 router to the RF Switch.
!  The IP address is for Loopback0.
!
ip dhcp pool MODEMS1
   network 172.25.1.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.1.1
   default-router 172.25.1.1
   option 7 ip 172.25.1.1
   option 4 ip 172.25.1.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp pool MODEMS2
   network 172.25.2.0 255.255.255.0
   bootfile docsis.cm
   next-server 172.25.2.1
   default-router 172.25.2.1
   option 7 ip 172.25.2.1
   option 4 ip 172.25.2.1
   option 2 hex 0000.0000
   lease 2 3 4
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
!
!  An internal DHCP server was used for testing in this example instead of external
!  servers (cable helper, TOD, TFTP, etc.).  External servers are recommended in a
!  genuine production network.
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0/0
 ip address 10.97.1.8 255.255.255.0
 ip rip receive version 2
 no ip split-horizon
 no keepalive
!
interface GigabitEthernet1/0/0
 no ip address
 negotiation auto
!
```

```
interface GigabitEthernet2/0/0
 no ip address
 negotiation auto
!
interface Cable5/1/0
!
!  This is the Protect interface for the first group.  Remember to configure the
!  Protect interface(s) last; after the Working interfaces are configured.
!
 no ip address
!
!  There is no need to set the IP address because it comes from the Working card via SNMP.
!
 no keepalive
!
!  This is set by default to 10 seconds with the N+1 IOS code, but should be disabled
!  on the Protect interface or set to be relatively high.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
!
!  The DS modulation and Interleave depth must be same on Protect and Working interfaces
!  of the same group.
!
 cable upstream 0 shutdown
!
!  This automatically becomes "no shut" (enabled) when a switchover occurs.
!
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
 hccp 1 protect 1 10.10.10.1
!
!  This is the HCCP first group and it is protecting member 1 with member 1's
!  FE IP address.  If it's intra-chassis, you can use the Loopback0 IP address.
!
 hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
!  This is the IP address of upconverter and its module 2 (B) that is backing
!  module 16 (P) of the upconverter.  This shows that one upconverter could have
!  a module backing up a module in a different chassis with a different IP address
!  if need be.  If this statement is not present when using 15BC2 IOS and above,
!  IF-Muting is assumed and an external upconverter with snmp capability is not needed.
!
 hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of the Switch and it is protecting member 1, which has a
!  bitmap of AA200000 in Switch slot 1.
!
 hccp 1 protect 2 10.10.10.1
!
!  This is the HCCP first group and it is protecting member 2 with its IP address.
!
 hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14
!
!  This is the IP address of the upconverter and its module 2 (B) that's backing
!  module 14 (N).
!
 hccp 1 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 AA200000 2
!
!  This is the IP address of the Switch and it is protecting member 2, with a
!  bitmap of AA200000 in Switch slot 2.
!
 hccp 1 protect 3 10.10.10.1
 hccp 1 channel-switch 3 uc wavecom-hd 10.97.1.21 2 10.97.1.21 12
 hccp 1 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 AA200000 3
 hccp 1 protect 4 10.10.10.1
 hccp 1 channel-switch 4 uc wavecom-hd 10.97.1.21 2 10.97.1.21 10
 hccp 1 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 AA200000 4
 hccp 1 protect 5 10.10.10.1
 hccp 1 channel-switch 5 uc wavecom-hd 10.97.1.21 2 10.97.1.21 8
 hccp 1 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 AA200000 5
 hccp 1 protect 6 10.10.10.1
 hccp 1 channel-switch 6 uc wavecom-hd 10.97.1.21 2 10.97.1.21 6
 hccp 1 channel-switch 6 rfswitch rfswitch-group 10.97.1.20 AA200000 6
 hccp 1 protect 7 10.10.10.1
 hccp 1 channel-switch 7 uc wavecom-hd 10.97.1.21 2 10.97.1.21 4
 hccp 1 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 AA200000 7
 hccp 1 timers 5000 15000
!
!  Cisco IOS command = hccp 1 timers <hellotime> <holdtime>
!  This is mostly for inter-chassis communication, so set it high for the uBR10012 router
!  as this can create extra CPU load.
!
interface Cable5/1/1
!
!  This is the Protect interface for the second group.
!
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
!
 hccp 2 protect 1 10.10.10.1
 hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
 hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
!  Because this MAC domain is on right side of header, the bitmap in hexadecimal code
!  is 55100000.
!
 hccp 2 protect 2 10.10.10.1
 hccp 2 channel-switch 2 uc wavecom-hd 10.97.1.21 1 10.97.1.21 13
 hccp 2 channel-switch 2 rfswitch rfswitch-group 10.97.1.20 55100000 2
 hccp 2 protect 3 10.10.10.1
 hccp 2 channel-switch 3 uc wavecom-hd 10.97.1.21 1 10.97.1.21 11
 hccp 2 channel-switch 3 rfswitch rfswitch-group 10.97.1.20 55100000 3
 hccp 2 protect 4 10.10.10.1
 hccp 2 channel-switch 4 uc wavecom-hd 10.97.1.21 1 10.97.1.21 9
 hccp 2 channel-switch 4 rfswitch rfswitch-group 10.97.1.20 55100000 4
 hccp 2 protect 5 10.10.10.1
 hccp 2 channel-switch 5 uc wavecom-hd 10.97.1.21 1 10.97.1.21 7
 hccp 2 channel-switch 5 rfswitch rfswitch-group 10.97.1.20 55100000 5
 hccp 2 protect 6 10.10.10.1
 hccp 2 channel-switch 6 uc wavecom-hd 10.97.1.21 1 10.97.1.21 5
 hccp 2 channel-switch 6 rfswitch rfswitch- group 10.97.1.20 55100000 6
 hccp 2 protect 7 10.10.10.1
 hccp 2 channel-switch 7 uc wavecom-hd 10.97.1.21 1 10.97.1.21 3
 hccp 2 channel-switch 7 rfswitch rfswitch-group 10.97.1.20 55100000 7
 hccp 2 timers 5000 15000
!
interface Cable8/1/0
!
!  This is the Working interface for the first group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.1.1 255.255.255.0
!
!  Interface bundling is supported also as well as subinterfaces.
!
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
!
!  The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
!
!  This is DS frequency, which used to be informational only when using an external
!  upconverter.  This must be set when doing N+1, so the Protect upconverter knows
!  which frequency to use.
!
 cable upstream 0 frequency 24000000
!
!  If doing dense mode combining, the upstream frequencies need to be different.
!  If no two US ports are shared, the same frequency can be used.
!
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
!
!  This tells cable modems to get an IP address from the primary scope and CPEs
!  to use the secondary scope.
!
 hccp 1 working 1
!
!  This is Working member 1 of HCCP Group 1.
!
 hccp 1 channel-switch 1 uc wavecom-hd 10.97.1.21 2 10.97.1.21 16
!
!  This is the IP address of the upconverter and its module 2 (B) that's backing
!  module 16 (P).
!
 hccp 1 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 AA200000 1
!
!  This is the IP address of the Switch & member 1, which has a bitmap of
!  AA200000 in Switch slot 1.
!
 hccp 1 reverttime 120
!
!  This is the time in minutes (+ 2 minute suspend) for the card to switch back to
!  normal mode if the fault has cleared.  If a fault was initiated by a keepalive
!  and you had a fault on the Protect card, it would revert back after the suspend
!  time and not await the full revert time.
!
interface Cable8/1/1
!
!  This is the Working interface for the second HCCP group.
!
 ip address 10.192.5.1 255.255.255.0 secondary
 ip address 172.25.2.1 255.255.255.0
 ip rip send version 2
 ip rip receive version 2
 keepalive 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable upstream 0 frequency 24000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable dhcp-giaddr policy
 hccp 2 working 1
!
!  This is Working member 1 of HCCP Group 2.
!
 hccp 2 channel-switch 1 uc wavecom-hd 10.97.1.21 1 10.97.1.21 15
 hccp 2 channel-switch 1 rfswitch rfswitch-group 10.97.1.20 55100000 1
!
!  This is the IP address of the Switch & Member 1 of Group 2, which has a bitmap of
!  55100000 in Switch slot 1.
!
 hccp 2 reverttime 120
!
ip classless
no ip http server
!
no cdp run
snmp-server community private RW
!
!  This does not affect the HCCP communications between the Upconverter, Switch,
!  the and uBR10012.
!
snmp-server enable traps cable
no cdp run
snmp-server manager
tftp-server server
tftp-server ios.cf alias ios.cf
!
line con 0
 logging synchronous
line aux 0
 no exec
 transport input all
!
!  The three lines above were used to console from the Auxiliary port of the uBR10012
!  to the Switch.
!
line vty 0 4
 session-timeout 400
 password xx
 login
endBuilding configuration...
```

Example: Virtual Interface Bundling

Example of Previously Supported Cable Line Card Interface Configuration Compared With Virtual Interface Bundling Configuration

The following example shows an older cable line card interface configuration with IP addressing:

```
interface cable 5/0/0
ip address 10.10.10.1 255.255.255.0
ip address 10.10.11.1 255.255.255.0 secondary
```

If previously configured on your router, this older cable line card interface configuration is automatically replaced by the following virtual interface bundling configuration, where no IP addressing is supported at the cable line card interface:

```
interface cable 5/0/0
no ip address
cable bundle 1
interface bundle 1
ip address 10.10.10.1 255.255.255.0
ip address 10.10.11.1 255.255.255.0 secondary
```

Example of Previously Supported Master/Slave Bundle Configuration with Virtual Interface Bundling Configuration

The following example shows the older cable line card interface configuration with IP addressing and master/slave bundling:

```
interface cable 5/0/0
ip address 10.10.10.1 255.255.255.0
cable bundle 5 master
interface cable 5/0/1
no ip address
cable bundle 5
```

If previously configured on your router, this older cable line card interface configuration is automatically replaced by the following virtual interface bundling configuration, where no IP addressing is supported at the cable line card interface:

```
interface cable 5/0/0
no ip address
cable bundle 5
interface cable 5/0/1
no ip address
cable bundle 5
interface bundle 5
ip address 10.10.10.1 255.255.255.0
Additional Information
```

Additional References

For additional information related to N+1 redundancy, the Cisco RF switch, and the Cisco uBR10012 routers, refer to the following references.

Related Documents

Related Topic	Document Title
Command References	• *Cisco IOS CMTS Cable Command Reference, 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html • *Cisco RF Switch Firmware Command Reference Guide* http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html
Cisco RF Switches	• Cisco RF Switch Documentation Home Page (complete documentation set) http://www.cisco.com/en/US/products/hw/cable/ps2929/tsd_products_support_series_home.html

Related Topic	Document Title
High Availability References for Cisco Broadband Cable	• *Bitmap Calculator for N+1 Configuration with the Cisco RF Switch* (Microsoft Excel format)
Additional Broadband Cable Technical Reference	• *Cisco Multiservice Broadband Cable Guide* http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_brochure09186a008014eeb0.pdf • *Cable Radio Frequency (RF) FAQs* http://www.cisco.com/en/US/tech/tk86/tk319/technologies_q_and_a_item09186a0080134faa.shtml

Standards

Standard	Title
DOCSIS	Data-Over-Cable Service Interface Specifications
EuroDOCSIS	European Data-Over-Cable Service Interface Specifications

MIBs

MIB	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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for N+1 Redundancy

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 7: Feature Information for N+1 Redundancy

Feature Name	Releases	Feature Information
HCCP N+1 Redundancy	12.1(10)EC	**HCCP support introduced on the Cisco uBR7200 series routers.**
HCCP N+1 Redundancy	12.2(4)XF1, 12.2(4)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router.

Feature Name	Releases	Feature Information
HCCP N+1 Redundancy	12.2(15)BC2a	• HCCP N+1 Redundancy support introduced for the Cisco uBR7246VXR router and the Cisco uBR 3x10 RF Switch. • CLI Usability—Synchronizes HCCP interface command-line interface (CLI) configuration between working and protect interfaces. • Support for N+1 redundancy for the Cisco UBR10-MC 5X20 BPE on the Cisco uBR10012 router. • IF Muting on the Cisco CMTS for non-SNMP-Capable Upconverters, on page 64 — enables N+1 redundancy on CMTS headends that do not use SNMP-enabled upconverters.
Global N+1 Line Card Redundancy	12.3(13a)BC	HCCP N+1 redundancy on the Cisco 7200 series routers is no longer supported. The following enhancements were introduced to HCCP N+1 redundancy support on the Cisco uBR10012 router: • Global N+1 Line Card Redundancy, on page 63 • Automatic running of the show hccp channel switch command for Background Path Testing for HCCP N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router.

Feature Name	Releases	Feature Information
HCCP Switchover Enhancements	12.3(21)BC	The following support has been removed: • HCCP N+1 redundancy support is removed for the Cisco uBR7246VXR router. • Tracking of HCCP interfaces is removed. The **hccp track** command is obsolete. The HCCP Switchover Enhancements feature is introduced on the Cisco uBR10012 router, with the following new support: • Performance improvements for traffic recovery during line card switchover under certain scalability limits. Within the required network scalability limits, the HCCP Switchover Enhancements feature provides the following switchover benefits: ◦ Less than 1-second voice call recovery. ◦ Less than 20-second data recovery. • To prevent false switchovers, the keepalive failure logic is modified. • For faster line card switchovers, the **member subslot protect** command has been modified to add the [**config** *slot/subslot*] option. When using the new **config** option, you can preload upstream connectors on an HCCP protected interface to emulate the most common line card connector assignments.

Feature Name	Releases	Feature Information
N+1 Redundancy	12.2(33)SCC	• HCCP N+1 redundancy support introduced on the Cisco uBR10012 router for Cisco uBR-MC 20X20V broadband processing engine (BPE). • Support for Legacy HCCP configurations has been removed. • Enabling Service Internal on HCCP Protect and Standby Working Interfaces, on page 78—The service internal command enables configuration of the protect and standby working cable interfaces for the following line cards: ◦ Cisco uBR10-MC5X20S, Cisco uBR10-MC5X20U, Cisco uBR10-MC5X20H and Cisco UBR-MC20X20V line cards.
N+1 Redundancy	12.2(33)SCE	The config option in the member subslot protect command is made the default. When more than one working card is configured, this option is automatically applied to the first working card.
N+1 Redundancy	12.2(33)SCF	This release supports configuration of a card with a lower license as protect for a working card with a higher license. However, when a switchover occurs, this protect card does not become active until it is upgraded and reloaded with a higher license.
N+1 Redundancy	12.2(33)SCG	Support for the new Cisco uBR Advanced RF Switch was added.

CHAPTER 3

Route Processor Redundancy for the Cisco uBR10012 Universal Broadband Router

First Published: February 14, 2008

Last Updated: January 28, 2013

The Route Processor Redundancy feature for the Cisco CMTS Routers is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. Route Processor Redundancy (RPR) reduces unplanned downtime. RPR enables a quicker switchover between active and standby PRE modules in the event of a fatal error on the active PRE module. When you configure RPR, the standby PRE is synchronized with the active PRE. In the event of a fatal error on the active PRE, the system switches to the standby PRE, which reinitializes itself and functions as the active PRE, reducing downtime of the 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 Route Processor Redundancy

- Two PRE modules must be installed in the Cisco uBR10012 chassis.
- The two processor modules must be of the same type. Both modules must be PRE2 modules or both modules must be PRE4 modules. You cannot mix PRE2 and PRE4 modules in the same chassis.
- Both PRE modules must be running identical software releases.
- For full redundancy, the FastEthernet port on the standby PRE module must have its own connection to the network. The console port on the standby PRE module must also be connected to a terminal, either by connecting it to a second terminal or by using a terminal server or other device to connect it to the same terminal used by the PRE module.
- Both PRE modules must be configured with the same amount of onboard SDRAM. A standby PRE cannot come online as the active PRE if the standby PRE has a smaller amount of SDRAM than the active PRE module.

Table below shows the hardware compatibility prerequisites for this feature.

Note Support for Route Processor Redundancy features in Cisco IOS Releases before 12.2BC; however, several of these releases and hardware have since reached End-of-Life (EOL) and therefore only the latest Cisco IOS software release trains are shown in the hardware compatibility table. For more information about the complete feature history, see the Feature Information for Route Processor Redundancy, on page 161.

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

Table 8: Route Processor Redundancy for Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine
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

Restrictions for Route Processor Redundancy

- Both PRE modules must be running Cisco IOS Release 12.2(33)SCA or Cisco IOS Release 12.2 SC releases to support the RPR feature.

Information About Route Processor Redundancy

Cisco IOS Release 12.2(4)XF and Cisco IOS Release 12.2(4)BC introduce support for Route Processor Redundancy (RPR) on the Cisco uBR10012 universal broadband router. The RPR feature enables the Cisco uBR10012 to use two PRE modules in a redundant configuration, so that if the active PRE module fails or becomes inactive, the system automatically performs a *switchover* , where the standby PRE module takes over and assumes full responsibility for systems operations.

Note From Cisco IOS release 12.2SC onwards, Nonstop Forwarding (NSF) and Stateful Switchover (SSO) are recommended and supported on the Cisco uBR10012 router. For SSO configuration details, see the "Configuring SSO" section in the *Stateful Switchover* guide at the following link: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html.

Note Unless otherwise indicated, all references to a PRE module in this document also include the PRE2 or PRE4 modules. However, when using redundant PRE modules, they cannot be mixed but must both be of the same type: both must be PRE2 modules or both must be PRE4 modules.

The RPR feature does not require a full reboot of the system to perform a switchover. When the system is originally initialized, the standby PRE module performs an abbreviated initialization routine—the PRE module performs all self-checks and loads the Cisco IOS software, but instead of performing normal systems operations it begins monitoring the active PRE module. If the standby PRE module detects a failure in the primary module, it can quickly assume the primary responsibility for systems operations.

Each PRE module contains all the resources required to operate the router, such as bootflash memory, Flash disks, Ethernet ports, and console port. In the default operation, the standby PRE module also synchronizes the major systems files, such as the Cisco IOS startup configuration file, so that during a switchover, the standby PRE module can duplicate the active PRE module's configuration. This process also resets the cable and network uplink interfaces.

Note Resetting the Gigabit Ethernet and OC-12 POS line cards will interrupt traffic for approximately 45 seconds. Because of DOCSIS requirements, a reset of the cable interface line cards requires all cable modems to go offline and reregister with the Cisco uBR10012 router. This will interrupt traffic on the cable network for 10 to 15 minutes, depending on the number of customers actually online at the time. A side-effect of this process is that when the cable modems come online again, they will not necessarily be assigned the same Service IDs (SIDs) that they had before the switchover.

Because the standby PRE module is partially initialized, you can use Cisco IOS CLI commands to access its resources, such as the Flash disks and bootflash. For example, you can use the **dir** command to list the contents of a device, or use the **copy** command to transfer files between the primary and standby PRE modules. (See the Using Redundant File Systems, on page 143 for more information on this feature.)

Switchover Procedure

A switchover occurs when the standby PRE module takes over responsibilities from the active PRE module. The switchover can occur automatically if the standby PRE module has determined that the active PRE module has failed, or an operator can initiate a manual switchover whenever desired.

A switchover triggers the following events:

1. If this is a manual switchover, the active PRE module verifies that the standby PRE module is present and is running Cisco IOS software that supports the RPR feature. If so, it instructs the standby PRE module to begin switchover procedures, and the active PRE module either attempts to reload its configured Cisco IOS software image or enters ROM monitor mode, depending on the setting of its configuration register.
2. The standby PRE module completes its initialization procedures, which includes completely loading the Cisco IOS software, verifying the physical components of the Cisco uBR10012 chassis, and parsing the startup configuration file. The standby PRE module is configured identically to the previous active PRE module, including the IP address for its onboard FastEthernet management interface.
3. The standby PRE assumes responsibility as the active PRE module and brings the Cisco uBR10012 chassis into a known state, which includes resetting all installed and enabled line cards and respective interfaces.

Note Resetting the Gigabit Ethernet and OC-12 POS line cards will interrupt traffic for approximately 45 seconds. Because of DOCSIS requirements, the reset of the cable interface line cards requires all cable modems to go offline and reregister with the Cisco uBR10012 router. This will interrupt traffic on the cable network for 10 to 15 minutes, depending on the number of customers actually online at the time. A side-effect of this process is that when the cable modems come online again, they will not necessarily be assigned the same Service IDs (SIDs) that they had before the switchover.

1. The new active PRE module begins normal systems operations, including passing traffic.

Note Depending on the setting of the PRE module's config register, it either reloads the Cisco IOS software or is left in the ROM monitor state. If the PRE module is in the ROM monitor state, it does not begin functioning as a standby PRE module until it is reloaded with the **hw-module sec-cpu reset** command.

Is PRE Switchover Failing?

The usual phenomenon for a PRE switchover to be affected is when the active PRE has these issues:

- PRE module hangs
- Login to PRE console or Tenet to chassis fails
- Line cards unable to connect to active PRE module, hence crashing
- Cable modems drop offline
- Chassis reload required
- Reset of active PRE module requires to restore service

One of the reasons may be because the active PRE may not be able to release its control to the standby PRE, thus both the PRE modules behave as the primary PRE modules.

In Cisco IOS Release 12.2(33)SCE5, the PRE high-availability is enhanced to address the PRE switchover issue. The line card uses a link loop mechanism when both the PRE modules behave as primary PRE modules.

In this mechanism, the line card checks the packet sent from the active PRE module, and automatically does a switchover to the real active PRE. The link loop mechanism automatically connects to the real active PRE module based on the MAC address, thus increasing robustness. This mechanism activates before the IPC keepalive timeout mechanism between the route processor and the line card does.

Note The PRE high-availability enhancement applies to both SSO and RPR redundancy modes on the Cisco uBR10012 router. For information on configuring SSO, see *Stateful Switchover* document at: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html.

Note If you are using the Break key to collect information, ensure that it is performed within 36 seconds (36s Enhanced High System Availability. Redundancy (EHSA) keepalive timeout) to prevent a reset of the active PRE module.

Note In case there is hardware issue with the PRE module, do not reinsert the faulty PRE in the chassis. Inserting a faulty PRE (although a standby PRE) may cause the line card to switch to the faulty PRE causing the line card to crash and cable modems to go offline.

Using Redundant File Systems

Both the primary and standby PRE modules have active file systems that can be accessed to store and transfer files. Table below lists the available file systems, the filenames that you can use with CLI commands to access the file systems, and a short description of each.

Table 9: Cisco uBR10012 Router File Systems

File System	Filename for CLI Commands	Description
Bootflash Secondary bootflash	bootflash: sec-bootflash:	Stores image and dump files.
NVRAM Secondary NVRAM	nvram: sec-nvram:	Typically stores the system default configuration file and startup configuration file.
System	system:	Stores the running configuration and other system files.

File System	Filename for CLI Commands	Description
Disk 0 Disk 1 Slot 0 Slot 1 Secondary Disk 0 Secondary Disk 1 Secondary Slot 0 Secondary Slot 1	disk0: disk1: slot0: slot1: sec-disk0: sec-disk1: sec-slot0: sec-slot1:	Disk refers to an ATA Flash disk (48 or 128 MB). Slot refers to a Flash memory card (8, 16, or 20 MB).[6] 0 refers to the left slot on the PRE module. 1 refers to the right slot on the PRE module. The **sec** prefix refers to the Flash disk or card in the standby PRE module.
FTP TFTP RCP	ftp: tftp: rcp:	Protocols used to transfer files to and from remote devices.

[6] Because of the small file system, the slot devices are not typically used on the Cisco uBR10012 router. The disk and sec-disk file systems are typically used instead.

You can use the Privileged EXEC commands **dir**, **del**, and **copy** to manage the contents of the file systems. You can also use the commands **mkdir** and **rmdir** to create and remove directories on Flash disks. You cannot use the commands **squeeze** and **undelete** on Flash disks.

Note For more information about using these file systems, see the *File Management* section in the Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide .

Console Port Usage After a PRE Module Switchover

When an active PRE module fails, and the standby PRE module becomes the active PRE module, you must use the console port on the new active PRE module to give CLI commands and display statistics for the router. If you have connected your PC or terminal to the console port on an active PRE module and a switchover occurs, you will no longer be able to access the console. The display will show the following error message:

```
Router#
Secondary console disabled
Router#
```

To access the console, move the PC or terminal's serial cable to the console port on the other PRE module, which is now acting as the active PRE module.

Reload PXF in the Standby PRE

Introduced in Cisco IOS Release 12.2(33)SCG2, the Reload PXF in the Standby PRE feature fixes most of the double-hit IRAM parity errors by reloading the Parallel Express Forwarding (PXF) in the standby PRE. The PXF can be reloaded periodically, or by a process based on timeout events, in the standby PRE. For the

Reload PXF in the Standby PRE feature, both the PRE modules should run the same Cisco IOS Release 12.2(33)SCG2 or later releases.

When Toasters (PXF Network Processing ASICs) continue to run for more than six months, Instruction RAM (IRAM) of the Toasters could encounter parity error where some bits of the IRAM are inversed. If a packet that is injected into the Toasters reaches the affected memory bits, the PRE will crash. If the IRAM parity error occurs in the standby PRE, it could remain undetected for a long time. During this period, if the active PRE crashes, the standby PRE will also crash after switchover, leading to collapse of the Cisco CMTS. This is called a double-hit IRAM parity error.

Restrictions

- Services may be affected when switchover and periodic reload of the PXF occur at the same time. The probability of this coincidence can be calculated by the following formula: 10s/(30*6*24*3600) * A = 1/1555200 *A = A * 6.43e-7 A is the probability of IRAM parity error of toasters on one PRE board.
- Standby PRE crashes on Reload failure

For benefits of the Reload PXF in the Standby PRE feature, see the Reload PXF in the Standby PRE ensures Enhanced Stability, on page 145.

Benefits

PRE Modules are not a Single Point of Failure

The PRE module is no longer a single point of hardware failure. If a permanent hardware failure in the active PRE module occurs, the standby PRE module recovers the system, increasing the level of network service and reliability.

PRE Switchover Occurs Without Operator Intervention

The standby PRE module can become the active PRE module without the manual intervention of a system operator. This increases the recovery time and reduces the need for an instant response from the network administrators.

Protection Against Software Failure

The RPR feature does not operate as a hot standby system, in which the standby PRE module continually duplicates the state of the primary module. Instead, during a switchover, the standby PRE module begins operations from a known state, thereby protecting the system from the possible software or operations failures that might have affected the active PRE module.

Reload PXF in the Standby PRE ensures Enhanced Stability

The Reload PXF in the Standby PRE feature ensures enhanced stability of the Cisco uBR10012 router by providing the following enhancements:

- Prevent double-hit IRAM parity errors.
- Reloading the PXF in the standby PRE when a timeout event is generated.

- Prevents the standby PRE crash and subsequent crashing of the Cisco CMTS. If the current PRE is in standby mode, the Toasters and Cobalt3 are reset.
- Interval of periodic reload is set at six months.
- Reload is scheduled at 3 a.m. (0300) local time, which is estimated as low traffic time, for minimal performance impact.

Toaster IRAM Parity Improvement

Starting from Cisco IOS Release 12.2(33)SCJ1a, the system shuts down the TMC cores which has Toaster IRAM parity error, and keeps other cores running. It can avoid the PXF crush and PRE switch over.

This feature is enabled by default, it can be disabled using **no cable toaster-iram-recover** command, to re-enable it, use **cable toaster-iram-recover** command.

Restrictions

- TMC core shutting down can only initiate once. The second occurrence of the Toaster IRAM parity error will trigger PXF crush.
- PRE5 PXF consists of five Toasters, this solution is effective only on the first four, which are T0, T1, T2 and T3.

How to Configure Route Processor Redundancy

See the following sections for configuration tasks for the RPR feature.

Tip These procedures refer to primary and standby PRE modules. Under normal circumstances when the Cisco uBR10012 router starts up, the PRE module in slot A becomes the active PRE module. However, the PRE module in slot B could can also function as the active PRE module at any time. When using these procedures, be aware that the term active PRE module refers to whichever PRE module is active at the current time, not necessarily to a PRE module in a particular physical slot.

Note All CLI commands shown in these procedures must be given at the console for the active PRE module. You do not normally need to configure the standby PRE module because the RPR feature automatically synchronizes the configuration files between the primary and standby PRE modules. If you have connected your PC or terminal to the console port on a active PRE module and a switchover occurs, you will no longer be able to access the console, and the display will read “Secondary console disabled”. To access the console, move the PC or terminal's serial cable to the console port on the other PRE module, which is now acting as the active PRE module.

Configuring Route Processor Redundancy

The RPR feature on the Cisco uBR10012 router is automatically enabled when two PRE modules are installed in the Cisco uBR10012 chassis. By default the two PRE modules are also configured to automatically synchronize all critical system files.

Use the following procedure to change how the PRE modules synchronize the system files.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **main-cpu**
5. **auto-sync** *option*
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**main-cpu** **Example:** `Router(config-red)# main-cpu`	Enters the main CPU configuration mode. • This configures the active PRE module, not the standby PRE module.
Step 5	**auto-sync** *option* **Example:** `Router(config-r-mc)#` **auto-sync***option*	Specifies the files to be synchronized. The *option* parameter can be one of the following: • **startup-config —**(Specifies that the PRE modules should synchronize the startup configuration files.

	Command or Action	Purpose
		• **config-register** —(Specifies synchronization of the configuration register values. • **bootvar** —(Specifies synchronization of the following boot variables: ◦ BOOT ◦ CONFIG_FILE ◦ BOOTLDR • **standard**—(Default) Specifies synchronization of all the system files.

Step 6	**end**
	Example:
	`Router(config-r-mc)# end`
		Returns to privileged EXEC mode.

Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the current configuration as the default startup configuration.

Configuring Reload PXF in the Standby PRE

The Reload PXF in the Standby PRE feature on the Cisco uBR10012 router is disabled by default. Use the following procedure to enable the Reload PXF in the Standby PRE feature.

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.

	Command or Action	Purpose
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**periodic-rel-pxf enable** **Example:** `Router(config-red)# periodic-rel-pxf enable`	Enables the periodic PXF reload. **Note** This configuration enables the PXF to reload periodically in the standby PRE module.

Step 5	**end**
	Example:
	`Router(config-red)# end`
		Returns to privileged EXEC mode.

Verifying Route Processor Redundancy

Use the following procedure to verify that RPR is configured on the Cisco uBR10012 router.

Step 1 Display the startup configuration and verify that the lines configuring redundancy appear:

Example:

```
Router# show startup-config

...
redundancy
 main-cpu
  auto-sync standard
...
```

Note If the **auto-sync** line contains anything other than **standard**, it indicates that only some of the required system files are being synchronized between the two PRE modules. Verify that this is the desired configuration, and if necessary, use the procedure given in the Configuring Route Processor Redundancy, on page 147 to reconfigure the router for **auto-sync standard** operation.

Step 2 Display the current RPR state using the **show redundancy** command. The Active PRE typically is shown in slot A:

Example:

```
Router# show redundancy

 PRE A (This PRE)    : Primary
 PRE B               : Secondary

 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED

 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
```

If a switchover has occurred, the **show redundancy** command will produce a display similar to the following, showing that the Active PRE has changed slots (in this case, moving from slot A to slot B):

Example:

```
Router# show redundancy

 PRE A              : Secondary
 PRE B (This PRE)   : Primary

 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED

 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
Router#
```

If the standby PRE module is not installed or is not operational, the **show redundancy** command will produce a display similar to the following:

Example:

```
Router# show redundancy

 PRE A (This PRE)   : Primary
 PRE B              : Secondary
 Redundancy state is REDUNDANCY_PEERSECONDARY_NONOPERATIONAL
 Secondary PRE information....
 Secondary PRE is not up
```

What to Do Next

Note The **show redundancy** command shows whether the PRE A slot or PRE B slot contains the active (**Primary**) PRE module. The other PRE slot will always be marked as **Secondary**, even if a second PRE module is not installed.

Forcing Switchover

To manually force a switchover, so that the standby PRE module becomes active, use the **redundancy force-failover main-cpu** command in Privileged EXEC mode. Manually forcing a switchover is useful in the following situations:

- You need to remove, replace, or upgrade the currently active PRE module.
- A previous switchover has activated the standby PRE module and you now want to restore the previously active PRE module.

Tip Simply removing the active PRE module would also trigger a switchover, but using the **redundancy force-failover main-cpu** command does not generate a hardware alarm.

The following procedure shows the procedure to force a switchover from the primary to the standby PRE module.

Step 1 Use the **redundancy force-failover main-cpu** command to force the switchover:

Example:

```
Router# redundancy force-failover main-cpu
Proceed with switchover to standby PRE? [confirm]

 00:38:09: %SYS-5-RELOAD: Reload requested
 System Bootstrap, Version 12.0(9r)SL1, RELEASE SOFTWARE (fc1)
 Copyright (c) 2000 by cisco Systems, Inc.

 Reset Reason Register = RESET_REASON_RESET_REG (0x74)
 C10000 platform with 524288 Kbytes of main memory
...
```

Step 2 After the switchover has occurred, the standby PRE module becomes the active PRE module, and the previous active PRE module is put into the ROM monitor mode. To enable that module to become the new standby PRE module, use the **hw-module sec-cpu reset** command so that the module will initialize and begin monitoring the health of the active PRE module:

Example:

```
Router# hw-module sec-cpu reset

Router#
11:55:09: %REDUNDANCY-5-PEER_MONITOR_EVENT: Primary detected a secondary crash
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
```

Verifying the PRE Switchover

Use the following procedure to verify that the switchover has occurred:

Step 1 Check that the Status LED on the new active, active PRE module is lighted with a steady green to indicate that it has initialized and is acting as the active PRE module. The alphanumeric display should also show a series of dashes to indicate that the PRE module is running without problems.

Step 2 Check that the Status LED on the new standby PRE module is OFF and that the alphanumeric display shows the message **IOS STBY** to indicate that the module is now acting as the standby PRE module.

Note After a failure, the non-active PRE module will either reload the Cisco IOS software image or enter ROM monitor mode, depending on the setting of its configuration register. If it loads the Cisco IOS software, it will automatically begin functioning as a standby PRE module. If it enters ROM monitor mode, it will become the standby PRE module only if it is reloaded using the **hw-module sec-cpu reset** command.

Step 3 To verify that a switchover has occurred, use the **show redundancy** command. Assuming that the original PRE module had been in slot A, and that the standby PRE module is in slot B, the **show redundancy** command would display the following:

Example:

```
Router# show redundancy

 PRE A              : Secondary
 PRE B (This PRE)   : Primary

 Redundancy state is REDUNDANCY_PEERSECONDARY_INITED

 Secondary PRE information....
 Secondary is up.
 Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
 Secondary CONFIG_FILE variable =
 Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
 Secondary Configuration register is 0x2
Router#
```

Verifying Reload PXF in the Standby PRE

To verify that the Reload PXF in the Standby PRE feature is enabled, use the **show running-config | include periodic** command in privileged EXEC mode.

```
Router# show running-config | include periodic

periodic-rel-pxf enable

Router#
```

Upgrading Cisco IOS Software on the PRE Modules

This section describes how to upgrade the software on redundant PRE modules in the Cisco uBR10012 router. This procedure requires that all PRE system files be synchronized, using the default synchronization setting (**auto-sync standard**).

Note The following CLI and ROM monitor commands must be given through the console port on the active PRE module. Although the CLI commands can be given through a Telnet connection to the active PRE module, this is not recommended because the ROM monitor commands require a connection to the active PRE module’s serial console port.

Step 1 If not already done, copy the new Cisco IOS software image from the TFTP server to the Flash disk in slot 0 of the active PRE module:

Example:

```
Router# copy tftp disk0:
```

```
Address or name of remote host [ ]? 192.168.100.10

Source filename [ ]? ubr10k-k8p6-mz.122-4.XF

Source filename [ubr10k-k8p6-mz.122-4.XF]?
Accessing tftp://192.168.100.10/ubr10k-k8p6-mz.122-4.XF
Loading ubr10k-k8p6-mz.122-4.XF from
192.168.100.10 (via FastEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
[OK - 5717476/11433984 bytes]
5717476 bytes copied in 250.840 secs (22869 bytes/sec)
Router#
```

Step 2 Copy the same image to the Flash disk in slot 0 of the standby PRE module:

Example:

```
Router# copy disk0:ubr10k-k8p6-mz.122-4.XF sec-disk0:
```

Step 3 Configure the system to use the new software image. In the following example, the Cisco uBR10012 router will use the software image named **ubr10k-k8p6-mz.122-4.XF** on the Flash disk in slot 0 of the active PRE module:

Example:

```
Router(config)# boot system flash disk0:ubr10k-k8p6-mz.122-4.XF
```

Step 4 If necessary, save the running configuration to the startup configuration:

Example:

```
Router# copy running-config startup-config
```

Step 5 Reset the standby PRE module so that it reboots and uses the new image.:

Example:

```
Router# hw-module sec-cpu reset
```

Step 6 Force a cutover to the standby PRE module, which forces the active PRE module to reboot and use the new image:

Example:

```
Router# redundancy force-failover main-cpu
```

Verifying the Software Upgrade

Use the following procedure to verify that the Cisco uBR10012 router is running the new upgraded Cisco IOS software image.

Step 1 Connect a PC or terminal to the console port of the active PRE module and give the **show version** command, which displays the version number and image name of the currently running software image:

Example:

```
Router# show version
 Cisco Internetwork Operating System Software
```

Example:

```
 Copyright (c) 1986-2001 by cisco Systems, Inc.
 Compiled Wed 1-Nov-01 22:36 by abc
 Image text-base: 0x600089C0, data-base: 0x61330000

 ROM: System Bootstrap, Version 12.0(9r)SL2, RELEASE SOFTWARE (fc1)
 BOOTLDR: 10000 Software (C10K-EBOOT-M), Version 12.0(16.6)ST2, RELEASE SOFTWARE
 Router uptime is 0 hours, 4 minutes
 System returned to ROM by power-on
```

Example:

Step 2 Connect a PC or terminal to the console port of the standby PRE module and give the **show version** command. This command should display the same name and version information as shown on the active PRE module.

Changing the System Boot Behavior

This section describes how to change the Cisco IOS software configuration register to modify how the system behaviors at power-on or reboot. The software configuration register is a 16-bit register in NVRAM that controls the following boot functions:

- Specifies the source of the Cisco IOS software image to be loaded
- Specifies whether the Cisco IOS software should ignore the contents of the saved configuration file in NVRAM memory
- Enables or disables the use of the Break function

Use the following procedure to change the software configuration register settings:

Step 1 Enter global configuration mode and use the **config-register** command to set the contents of the software configuration register to a new value. You must specify the new value as a 16-bit hexadecimal bitmask, using the values shown in the Table below.

Table 10: Definition of Bits in the Software Configuration Register

Bit No.	Hex Value	Meaning/Function
00 to 03	0x0000 to 0x000F	Defines the source of a default Cisco IOS software image required to run the router: • 00—On powerup, the system remains at the ROM monitor prompt (rommon>), awaiting a user command to boot the system manually by means of the rommon **boot** command. • 01—On powerup, the system automatically boots the first system image found in the Flash memory single inline memory module (SIMM) on the PRE. • 02 to 0F—On powerup, the system automatically boots from a default Cisco IOS software image stored on a TFTP server in the network. For this setting, the Fast Ethernet port on the PRE must be configured and operational. This setting also enables boot system commands that override the default filename.
06	0x0040	Causes system software to ignore the contents of the NVRAM configuration file.
07	0x0080	Enables the original equipment manufacturer (OEM) bit.
08	0x0100	Disables the Break function after 30 seconds.
09	0x0200	Not used.
10	0x0400	Specifies that broadcast packets are based on the 0.0.0.0 IP address.
11 and 12	0x0800 to 0x1000	Defines the console baud rate (the default setting is 9600 baud).

Bit No.	Hex Value	Meaning/Function
13	0x2000	Boots an image from the Flash memory.
14	0x4000	Specifies that broadcast packets use the subnet broadcast address.
15	0x8000	Enables diagnostic messages and ignores the contents of the NVRAM configuration file.

For example, to configure the router to boot to the ROM monitor prompt, set the configuration register to **0x2100** with the following commands:

Example:

```
Router#
config t

Router(config)#
config-register 0x2100

Router(config)#
```

Tip The typical bitmask for normal use is 0x2102, which specifies that the router loads the Cisco IOS software from the Flash memory and boots to the Cisco IOS CLI prompt. The Break key is enabled for only 30 seconds, so that the user can break to the ROM monitor prompt if desired.

Step 2 Exit the global configuration mode by entering the **exit** command.

Example:

```
Router(config)# exit

Router#
```

Step 3 Display the new software configuration register setting using the **show version** command. The last line shows the settings of the configuration register:

Example:

```
Router#
show version

Cisco Internetwork Operating System Software
 IOS (tm) 10000 Software (UBR10K-K8P6-MZ), Released Version 12.2(4)XF
 Copyright (c) 1986-2001 by cisco Systems, Inc.
...
```

Example:

Note When you change the configuration register, the **show version** command shows both the current value of the register, as well as the value that will be used on the next reboot or reload.

Step 4 Save the configuration file to preserve the new software configuration register settings.

Example:

```
Router# copy running-config startup-config
```

Step 5 The changes to the software configuration register will take effect the next time the router is rebooted or restarted. To manually reboot the router, use the **reload** command:

Example:

```
Router# reload

System configuration has been modified. Save? [yes/no]: yes

Proceed with reload? [confirm]
```

What to Do Next

Note For detailed information about setting and using the configuration register, see the *Rebooting* chapter in the *File Managemen*t manual, which is part of the *Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*.

Moving a Configuration File to the Flash Disk

This section describes how to copy a configuration file to a Flash disk and configure the Cisco uBR10012 router so that it loads the configuration file from the Flash disk. This typically is necessary when the configuration file is approaching the 512KB maximum size that is allowed for configuration files that are stored in NVRAM.

Use the following procedure to copy and run the startup configuration off a Flash disk.

Step 1 The configuration file must fit within one complete buffer on the Flash disk. The default buffer size is 512 KB, so if the configuration file is larger than this, or if you ever expect the file to be larger than this, you will need to change the buffer size. To do so, enter global configuration mode and change the buffer size with the **boot buffersize** command.
The following shows the buffer being changed to 1 MB in size:

Example:

```
Router# configure terminal

Router(config)# boot buffersize 1024000

Router(config)# exit

Router#
```

Step 2 Copy the configuration file to the Flash disks in both PRE modules. The following example assumes the configuration file is still small enough to exist in NVRAM and is being copied to the first Flash disk in each PRE module:

Example:

```
Router# copy nvram:ubr10012-config disk0:ubr10012-config

Router# copy nvram:ubr10012-config sec-disk0:ubr10012-config

Router#
```

If the configuration file is currently on a TFTP server, the following commands copy the file to the first Flash disk in each PRE module:

Example:

```
Router# copy tftp://192.168.100.10/router-config disk0:ubr10012-config

Router# copy disk0:ubr10012-config sec-disk0:ubr10012-config

Router#
```

Step 3 Specify the new location of the configuration file by setting the CONFIG_FILE boot variable with the **boot config** command in global configuration mode. For example, the following specifies

Example:

```
Router# config t

Router(config)# boot config disk0:ubr10012-config

Router(config)# exit

Router#
```

Step 4 When you have finished changing the running-configuration, save the new configuration:

Example:

```
Router# copy running-config startup-config
```

What to Do Next

When the Cisco uBR10012 router next restarts or reboots, the router will use the configuration file on the first Flash disk in the active PRE module.

Verifying the Configuration File Setting

To verify that the Cisco uBR10012 router is configured to use the startup configuration file on the Flash disk, use the following procedure:

Step 1 Display the directory of the Flash disk in the active PRE module:

Example:

```
Router# dir disk0:
```

```
Directory of disk0:/
    1  -rw-    10705784   May 30 2001 20:12:46  ubr10k-k8p6-mz.122-4.XF
    2  -rw-      484772   Jun 20 2001 19:12:56  ubr10012-config
128094208 bytes total (116903652 bytes free)
Router#
```

Step 2 Display the directory of the Flash disk in the standby PRE module:

Example:

```
Router# dir sec-disk0:

Directory of sec-disk0:/
    1  -rw-    10705784   May 30 2001 20:12:46  ubr10k-k8p6-mz.122-4.XF
    2  -rw-      484772   Jun 20 2001 19:12:56  ubr10012-config
128094208 bytes total (116903652 bytes free)
Router#
```

Note The contents of the Flash disk in the standby PRE module should be similar or identical to the contents of the Flash disk in the active PRE module.

Step 3 Display the setting of the CONFIG_FILE boot variable using the **show bootvar** command:

Example:

```
Router# show bootvar

BOOT variable =
CONFIG_FILE = disk0:ubr10012-config
BOOTLDR variable =
Configuration register is 0x2102
```

Configuration Examples for Route Processor Redundancy

The following example shows the relevant portion of the Cisco IOS configuration file for the default configuration for the RPR feature, which should be used for most applications:

```
redundancy
  main-cpu
    auto-sync standard
```

The following example shows the relevant portion of the Cisco IOS configuration file for the configuration that could be used when the two PRE modules are running different Cisco IOS software images and require different configuration files:

```
redundancy
  main-cpu
    no auto-sync startup-config
    auto-sync config-register
    auto-sync bootvar
```

Additional References

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
CMTS Hardware Installation Guide	Cisco uBR10012 Series Hardware Installation Guide
CMTS Software Installation Guide	Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC
CMTS Troubleshooting Guide	Cisco uBR10012 Series Troubleshooting Guide
Route Processor Performance Routing Engines	Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module
Route Processor Redundancy Plus for Cisco CMTS	Route Processor Redundancy Plus for the Cisco uBR10012 Universal Broadband Router
Stateful Switchover	Stateful Switchover
In Service Software Upgrade	Cisco IOS In Service Software Upgrade

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

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

Feature Information for Route Processor Redundancy

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 11: Feature Information for Route Processor Redundancy

Feature Name	Releases	Feature Information
Route Processor Redundancy	12.2(4)XF	This feature was introduced on the Cisco uBR10012 universal broadband router.
	12.2(4)BC1	Support for this feature was added to Cisco IOS Release 12.2 BC for the Cisco uBR10012 universal broadband router.

Feature Name	Releases	Feature Information
	12.2(11)CY, 12.2(11)BC3	Support for the PRE module was removed. Only the PRE1 module can be used with the Cisco uBR10012 router**.**
	12.2(33)SCA	This feature was intergrated in Cisco IOS Release 12.2(33)SCA for Cisco uBR10012 router.
	12.2(33)SCE5	PRE high availability was enhanced. A link loop mechanism was added to the PRE switchover.
Reload PXF in the Standby PRE	12.2(33)SCG2	This feature is introduced on Cisco uBR10012 universal broadband router. The following were introduced or modified: **periodic-rel-pxf enable**

CHAPTER 4

Route Processor Redundancy Plus for the Cisco uBR10012 Broadband Router

First Published: February 14, 2008

This document describes the Route Processor Redundancy Plus (RPR+) feature on the Cisco uBR10012 universal broadband router. RPR+ and DOCSIS Stateful Switchover (DSSO) support in Cisco IOS® Software for fast route processor failover without DOCSIS line card reboot.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

With RPR+ and DOCSIS SSO, the Cisco uBR10012 can rapidly fail over from the active route processor to the standby processor without the reloading of the cable line cards. However, even though the cable line cards are not reset, the new active route processor needs to perform certain recovery procedures in order for cable line card traffic-flow to resume. A Cisco implementation provides priority-recovery procedures for those modems carrying voice, providing more rapid recovery of voice services.

Note From Cisco IOS release 12.2SC onwards, NSF and SSO is recommended and supported on the Cisco uBR10012 router. For SSO configuration details, see the "Configuring SSO" section in the Stateful Switchover guide at the following link: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/sso26s.html#wp1338159

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 Route Processor Plus Redundancy

- You must have the same image on both the active and standby RPs to support RPR+. If one or more RPs does not have an RPR+ image, the router reverts to RPR mode on both RPs.
- Two PRE1 or PRE2 modules must be installed in the Cisco uBR10012 chassis. The order number for the PRE1 module is UBR10-PRE1. You cannot mix PRE modules with PRE1 or PRE2 modules in the same chassis.

Note The PRE module no longer ships with the Cisco uBR10012 chassis.

- For full redundancy, the Fast Ethernet port on the standby RP must have its own connection to the network. The console port on the standby RP must also be connected to a terminal, either by connecting it to a second terminal or by using a terminal server or other device to connect it to the same terminal used by the PRE1 or PRE2 module.
- Both PRE1 or PRE2 modules must be configured with the same amount of onboard SDRAM. A standby RP cannot come online as the active RP if the standby RP has a smaller amount of SDRAM than the active RP.

Restrictions for Route Processor Plus Redundancy

ARP Filtering Statistics

The Cisco uBR10012 router maintains ARP filtering statistics on the Performance Routing Engine (PRE) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in RPR+ Redundancy, these ARP filtering statistics are reset to zero.

For additional information about ARP filtering, refer to the following document on Cisco.com:

- *Cable ARP Filtering*

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

Command-line Interface Synchronization and SNMP

Command-line interface (CLI) configuration commands are synchronized only with the standby Performance Routing Engine (PRE) module. Simple Network Management Protocol (SNMP) persistence is not supported through a PRE1 or PRE2 switchover. Any configuration that is done with SNMP commands is not synchronized with the standby PRE module.

Console Port Usage After a PRE1 or PRE2 Module Switchover

When an active RP fails, and the standby RP becomes the active RP, you must use the console port on the new active RP to give command-line interface (CLI) commands and display statistics for the system. If you have connected your PC or terminal to the console port on an active RP and a switchover occurs, you no longer are able to access the console and the display shows "Standby console disabled."

To access the console, move the PC or terminal's serial cable to the console port on the other PRE1 or PRE2 module, which is now acting as the active RP.

Encrypted Multicast

Encrypted multicast is not supported during a line card switchover nor during a PRE1 or PRE2 switchover.

External Management Stations

External management stations lose connectivity with the cable modem termination system (CMTS) during PRE1 or PRE2 switchover. Stations must reestablish connectivity after the switchover between PRE1 or PRE2 modules is complete.

Flap Detection on WAN Interfaces During Switchover

Neighboring routers detect flapping on WAN interfaces during a switchover. The neighboring routers reconverge after the switchover is complete.

Note Cable interfaces do not flap during a switchover. Service may be temporarily suspended for approximately 30 seconds during a switchover and reinitialization, but service to cable interfaces does not stop.

Link States Reinitialized After Switchover

The synchronization of link states is not maintained between the active and standby RP. Link states are reinitialized after switchover

MIB Variables Reinitialized After Switchover

All MIB variables will be re-initialized following a switchover.

Telnet Sessions Disconnected During Switchover

A switchover automatically disconnects any Telnet sessions on the active (failed) RP.

Information About Route Processor Plus Redundancy

When two route processors (RPs) are installed in a Cisco uBR10012 router chassis, one RP acts as the active RP, and the other acts as a backup, or standby, RP. If the active RP fails, or is removed from the system, the standby RP detects the failure and initiates a switchover. During a switchover, the standby RP assumes control of the router, connects with the network interfaces, and activates the local network management interface and system console.

Using the RPR+ feature, the standby RP is fully initialized and configured. This allows RPR+ to dramatically shorten the switchover time if the active RP fails, or if a manual switchover is performed. Because both the startup configuration and running configuration are continually synchronized from the active to the standby RP, line cards are not reset during a switchover. The interfaces remain up during this transfer, so neighboring routers do not detect a link flap (that is, the link does not go down and back up).

Each RP contains all the resources required to operate the router, such as bootflash memory, Flash disks, Ethernet ports, and console port. In the default operation, the secondary RP also synchronizes the major systems files, such as the Cisco IOS startup configuration file, so that during a switchover, the secondary RP can duplicate the active RP's configuration. This process also resets the cable and network uplink interfaces.

This section describes the switchover process with RPR+, including synchronization between the active and standby RPs, and includes the following topics:

Benefits

DOCSIS Stateful Switchover (DSSO)

DOCSIS stateful switchover (DSSO) increases service uptime by instantaneously switching over between dual route processors should one processor fail. Switchover takes place without resetting or reloading line cards or affecting related subsystems or processes. The advantage of DOCSIS Stateful Switchover (DSSO) (with RPR+) is that a switchover between the primary and standby RP will not require the cable interfaces to be reset, nor do the modems reregister or go offline. Furthermore, the cable modems retain their service IDs (SIDs) through the switchover.

Standard RPR

In standard RPR, the system implemented Extended High System Availability (EHSA) redundancy, wherein the standby RP suspended its initialization midway through the startup process. To complete the initialization during a switchover, all line cards were reset and the switch fabric was reinitialized. Because initialization of the standby RP was suspended before configuration was parsed, chassis discovery and startup configuration parsing were conducted during the switchover.

Improved Switchover Time with RPR+

RPR+ provides a faster switchover by fully initializing and fully configuring the standby RP. The configuration data on the standby RP is fully synchronized with the active RP. With RPR+, the communication with line cards is reinitialized, but the line cards are not reset.

Supported Cable Interface Line Cards and Interface Modules

Beginning with Cisco IOS Release 12.2(11)BC3, the Cisco uBR10012 router supports the following cable interface line cards and interface modules with RPR+ and PRE1 or PRE2 modules:

- Cisco uBR10-LCP2-MC16C/MC16E/MC16S Line Card
- Cisco uBR10-LCP2-MC28C/B Line Card
- Cisco uBR10-MC5X20S Cable Interface Line Card

- Cisco uBR10-SRP-OC12SML/SMI DPT Adapter Card
- Cisco uBR10012 OC-48 DPT/POS Interface Module

Terminology Changes with Cisco IOS Release 12.2(11)BC3

In Cisco IOS Release 12.2(11)BC3 and later, the following High Availability terms for the Cisco uBR10012 universal broadband router have been changed:

Old Term	New Term
Failover	Switchover
N+1 Redundancy	1:n Redundancy
Primary RP	Active RP
Secondary RP	Standby RP

Synchronization

To achieve the benefits of RPR+, the chassis and slot configuration information is synchronized from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. This synchronization occurs in two separate phases:

1. When a standby RP first comes online, the configuration information is synchronized in bulk from the active RP to the standby RP.
2. When configuration changes occur, an incremental synchronization from the active RP to the standby RP is conducted. Incremental synchronizations contain either the modifications to the shelf configuration or the trigger that caused the modification.

Synchronization During Initialization

When a system with RPR+ is initialized, the active RP performs a chassis discovery (discovery of the number and type of line cards and fabric cards in the system) and parses the startup configuration file.

The active RP then synchronizes this data to the standby RP and instructs the standby RP to complete its initialization. This method ensures that both RPs contain the same configuration information.

Note Even though the standby RP is fully initialized, it interacts only with the active RP to receive incremental changes to the configuration files as they occur. CLI commands on the standby RP are not supported.

Synchronization of Startup Configuration

The startup configuration is a text file stored in the RP's NVRAM. During system startup, the startup configuration file is copied from the active RP to the standby RP. Any existing startup configuration file on the standby RP is overwritten.

The startup configuration file is also synchronized whenever you perform the following operations:

- CLI command: copy system:running-config nvram:startup-config
- CLI command: copy running-config startup-config
- CLI command: write memory
- CLI command: copy filename nvram:startup-config
- SNMP SET of MIB variable ccCopyEntry in CISCO_CONFIG_COPY MIB
- System Configuration Saved on reload command.
- System Configuration Saved on redundancy force-failover command.

Note Synchronization of the startup configuration file is enabled by default in RPR+ mode. Because this is necessary for RPR+ functionality, the command [no] auto-sync startup-config is not available in RPR+ mode. This command is available only in standard RPR mode. For additional information on the use of [no] auto-sync startup-config with standard RPR, see the Route Processor Redundancy for the Cisco uBR10012 Universal Broadband Router .

Incremental Synchronization of the Running Configuration

When both RPs are fully initialized, any further changes to the running configuration are synchronized to the standby RP as they occur.

CLI commands

CLI changes to the running configuration are synchronized from the active RP to the standby RP. In effect, the CLI command is run on both the active and the standby RP.

SNMP SET Commands

Configuration changes caused by an SNMP SET are also synchronized on a case-by-case basis. Currently only two SNMP configuration SETs are supported on the Cisco uBR10012 router:

- shut/no-shut (of an interface)
- link up/down trap enable/disable

Changes to Chassis State

- Any changes to the chassis state because of line card insertion or removal are synchronized over to the standby RP.

- Changes to the chassis state because of switch card insertion or removal, or from configuration changes to the alarm or power supply cards, are not synchronized to the standby RP. The standby learns these configuration changes using a discovery and reconciliation process during a switchover.
- Information regarding line card states is not synced. Line cards that are not on line at the time of a switchover (that is, any cards not running the Cisco IOS software and not communicating with the active RP) are reset and reloaded during a switchover. This process does not add downtime.

The RPR+ Switchover Process

A switchover occurs when the standby RP takes over responsibilities from the active RP. The switchover can occur automatically if the standby RP has determined that the active RP has failed, or an operator can initiate a manual switchover whenever desired.

A switchover triggers the following events:

1. If this is a manual switchover, the active RP verifies that the standby RP is present and is running Cisco IOS software that supports the RPR feature. If so, it instructs the standby RP to begin switchover procedures, and the active RP either attempts to reload its configured Cisco IOS software image or enters ROM monitor mode, depending on the setting of its configuration register.
2. The standby RP completes its initialization procedures, which includes completely loading the Cisco IOS software, verifying the physical components of the Cisco uBR10012 chassis, and parsing the startup configuration file. The standby RP is configured identically to the previous active RP, including the IP address for its onboard Fast Ethernet management interface.
3. The standby RP assumes responsibility as the active RP and brings the Cisco uBR10012 chassis into a known state, which includes resetting all installed and enabled line cards and respective interfaces.

Note Resetting the Gigabit Ethernet and OC-12 Packet Over SONET (POS) line cards will interrupt traffic for approximately 30 seconds. The cable interface is not reset, and in support of DOCSIS requirements, the cable modems do not go offline.

Note Depending on the network configuration and on the configuration of the Ethernet/Fast Ethernet interfaces, the network could take between 3 to 25 seconds after an RPR+ switchover before all end-to-end connections are fully restored. During that time it is possible that some packets might be dropped.

1. The new active RP begins normal systems operations, including passing traffic.

Note Depending on the setting of the PRE1 or PRE2 module's configuration register, it either reloads the Cisco IOS software or is left in the ROM monitor state. If the PRE1 or PRE2 module is in the ROM monitor state, it does not begin functioning as a standby RP until it is reloaded with the hw-module sec-cpu reset command.

Note The backup PRE1 or PRE2 module starts forwarding traffic immediately to cable modems, presuming that the interfaces are up, and that all the FIB, adjacency, service flow, classifiers, and Virtual Traffic Management System (VTMS) queue information are correctly configured.

Redundant File Systems

Both the active and standby RPs have active file systems that can be accessed to store and transfer files. Table 1 lists the available file systems, the filenames that you can use with CLI commands to access the file systems, and a short description of each.

Table 12: Cisco uBR10012 Router File Systems

File System	Filename for CLI Commands	Description
Bootflash Secondary bootflash	bootflash: sec-bootflash:	Stores image and dump files.
NVRAM Secondary NVRAM	nvram: sec-nvram:	Typically stores the system default configuration file and startup configuration file.
System	system:	Stores the running configuration and other system files.
Disk 0 Disk 1 Slot 0 Slot 1 Secondary Disk 0 Secondary Disk 1 Secondary Slot 0 Secondary Slot 1	disk0: disk1: slot0: slot1: sec-disk0: sec-disk1: sec-slot0: sec-slot1:	Disk refers to an ATA Flash disk (48 or 128 MB). Slot refers to a Flash memory card (8, 16, or 20 MB).[7] 0 refers to the left slot on the PRE1 or PRE2 module. 1 refers to the right slot on the PRE1 or PRE2 module. The sec prefix refers to the Flash disk or card in the standby RP.
FTP TFTP RCP	ftp: tftp: rcp:	Protocols used to transfer files to and from remote devices.

[7] Because of the small file system, the slot devices are not typically used on the Cisco uBR10012 router. The disk and sec-disk file systems are typically used instead.

You can use the privileged EXEC commands dir, del, and copy to manage the contents of the file systems. You can also use the commands mkdir and rmdir to create and remove directories on Flash disks. You cannot use the commands squeeze and undelete on Flash disks.

Note For more information about using these file systems, see the “File Management” manual in the Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide.

DSX Messages and Synchronized PHS Information

Cisco IOS Release 12.3(17a)BC introduces support for PHS rules in a High Availability environment. In this release, and later releases, PHS rules synchronize and are supported during a switchover event of these types:

- Route Processor Redundancy Plus (RPR+) for the Cisco uBR10012 router, with Active and Standby Performance Routing Engines (PREs)
- HCCP N+1 Redundancy, with Working and Protect cable interface line cards

For further information about DSX messages and Payload Header Suppression (PHS) information on the Cisco CMTS, refer to these documents, and additional DOCSIS PHS information:

- *Cable DOCSIS 1.1 FAQs* , Cisco TAC Document 12182

http://www.cisco.com/en/US/tech/tk86/tk168/technologies_q_and_a_item09186a0080174789.shtml

- DOCSIS 1.1 for the Cisco CMTS

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

High Availability Support for Encrypted IP Multicast

Cisco IOS Release 12.3(17a)BC introduces support for IP Multicast streams during switchover events in a High Availability environment. This feature is supported for Route Processor Redundancy Plus (RPR+), N+1 Redundancy, and encrypted BPI+ streams.

For additional information about IP Multicast and High Availability, refer to these documents on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*

http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html

- *Dynamic Shared Secret for the Cisco CMTS*

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

- *IP Multicast in Cable Networks,* White Paper

http://www.cisco.com/en/US/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun.html

How to Configure, Verify, and Troubleshoot Route Processor Plus Redundancy

This section provides the following procedures to configure and verify RPR+ and high availability on the Cisco uBR10012 router.

Configuring RPR+ on the Cisco uBR10012 Universal Broadband Router

The default redundancy mode in the Cisco uBR10012 router is standard Route Processor Redundancy (RPR). Perform the steps below to enable RPR+ on the Cisco uBR10012 router.

Before You Begin

To enable RPR+, both route processors must be running the same version of Cisco IOS software.

Note If necessary, refer to the "Upgrading Cisco IOS Software Images" section on page 14 to change the image on the Cisco uBR10012 router. Reload is required.

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	**main-cpu** **Example:** `Router(config)# main-cpu`	Enters the main CPU configuration mode. (This configures the active RP, not the standby RP.) Refer to **main-cpu** command, for additional command syntax information.
Step 4	auto-sync option **Example:** `Router(config-r-mc)# auto-sync standard`	Specifies the files to be synchronized. Refer to **auto-sync** command, for additional command syntax information. **Note** Cisco strongly recommends that you use the auto-sync standard command to ensure that all system files remain synchronized between the two PRE1 or PRE2 modules.
Step 5	**no auto-sync** *option* **Example:** `Router(config-r-mc)# no auto-sync standard`	(Optional) Specifies that one or more files should not be synchronized. Option can be any of the values specified previously. **Note** The **no auto-sync** command is not typically used in production plants.
Step 6	**CTRL-Z** **Example:** `Router(config-r-mc)# CTRL-Z`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the current configuration as the default startup configuration.

Verifying RPR+ Configuration

Perform the steps below to verify that RPR+ is configured on the Cisco uBR10012 router:

DETAILED STEPS

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

Step 2	**show startup-config**
	Example:
	`Router# show startup-config`
	`...`
	`redundancy`
	`main-cpu`
	`auto-sync standard`
	`...`
		Displays the startup configuration and verify that the lines configuring redundancy appear.
		Note If the auto-sync line contains anything other than standard, it indicates that only some of the required system files are being synchronized between the two PRE1 or PRE2 modules. Verify that this is the desired configuration. If necessary, refer to the Configuring RPR+ on the Cisco uBR10012 Universal Broadband Router, on page 172 to reconfigure the router for auto-sync standard operation.

Step 3	**show redundancy**
	Example:
	`Router# show redundancy`
	`PRE1 A (This PRE1) : Primary`
	`PRE1 B : Secondary`
	`...`
		Displays the current RPR state. The active RP typically is shown in slot A.

If a switchover has occurred, the show redundancy command displays information similar to the following, showing that the active RP has changed slots (in this case, moving from slot A to slot B):

```
Router# show redundancy
PRE1 A : Secondary
PRE1 B (This PRE1) : Primary
Redundancy state is REDUNDANCY_PEERSECONDARY_INITED
```

```
Secondary RP information....
Secondary is up.
Secondary BOOT variable = bootflash:ubr10k-k8p6-mz
Secondary CONFIG_FILE variable =
Secondary BOOTLDR variable = bootflash:c10k-eboot-mz
Secondary Configuration register is 0x2
Router#
```

If the standby RP is not installed or is not operational, the show redundancy command displays information similar to the following:

```
Router# show redundancy
PRE1 A (This PRE1) : Primary
PRE1 B : Secondary
Redundancy state is REDUNDANCY_PEERSECONDARY_NONOPERATIONAL
Secondary RP information....
Secondary RP is not up
```

Note The show redundancy command shows whether the PRE1 A slot or PRE1 B slot contains the active (Primary) PRE1 module. The other PRE1 slot will always be marked as Secondary, even if a second PRE1 module is not installed.

Upgrading Cisco IOS Software Images

RPR+ is enabled by default with the Cisco IOS Release 12.2(11)BC3 and later releases. Use this set of procedures when you need to upgrade your Cisco IOS to a release that supports RPR+ on the Cisco uBR10012 router.

Cisco IOS software upgrade involves these three procedures:

Prerequisites

Note You are required to have the same image on both the active and standby RPs to support RPR+. If one or more RPs does not have an RPR+ image, the router reverts to RPR mode on both RPs.

Creating Additional Disk Space (Optional)

(Optional) To create additional disk space in preparation for the RPR+ image, issue the following commands from global configuration mode on the active and standby RPs (where slot is the RP slot number and filename is the RPR+ image file name).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • delete slot 0:filename • delete sec-slot 0:filename	Deletes an old file from the active or standby RP to make room for the new file.

	Command or Action	Purpose
	Example: Router(config)# **delete slot 0:ubr10k-p6-mz** or Router(config)# delete sec-slot 0:ubr10k-p6-mz	
Step 2	squeeze flash: **Example:** Router(config)# squeeze flash:	Permanently deletes all files marked "delete" on a Flash memory device, recovering space on the device.

Copying the Cisco IOS Image

To copy the Cisco IOS image from a TFTP server, and to set the boot variable on the active RP, issue the following commands in global configuration mode (where filename is the RPR+ image fil name).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • copy tftp://tftp-server/filename bootflash:filename • • copy tftp://tftp-server/filename sec-bootflash:filename **Example:** Router# **copy tftp://tftp-server/ubr10k-p6-mz bootflash:ubr10k-p6-mz** or **Router# copy tftp://tftp-server/ubr10k-p6-mz sec-bootflash:ubr10k-p6-mz**	Copies the Cisco IOS image from a TFTP server to the bootflash of the active or standby RP. This command allows you to change software images without requiring access to the TFTP monitor mode. The image you download is made available to the Cisco uBR10012 router on the next reload (reboot).
Step 2	boot system bootflash:filename **Example:** Router# **boot system bootflash:ubr10k-p6-mz**	Sets the BOOT environment variable. This variable specifies the location and name of the system image file to use when automatically booting the system.

	Command or Action	Purpose
Step 3	write memory **Example:** `Router# write memory`	Saves the configuration.
Step 4	**show bootvar** **Example:** `Router# show bootvar`	Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.

Resetting a PRE1 or PRE2 Module or Line Card After Upgrade

To reset a particular route processor (RP) or a particular line card, use the hw-module reset command in privileged EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**hhw-module sec-cpu reset** **Example:** `Router# hw-module sec-cpu reset`	Resets the specified RP or line card slot. **Note** Refer to **hw-module reset command** for additional command syntax information.

Reloading Cisco IOS (Restarting the System)

To reload the operating system, use the reload command in privileged EXEC mode.

Note This reload is required if you are reloading an RPR+ image, but optional otherwise. The reload command restarts the entire system, including both the active and standby RPs.

SUMMARY STEPS

1. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**reload** **Example:** `Router# reload`	Reloads the operating system and restarts the router.

What to Do Next

Note If you are upgrading from a Cisco IOS image previously configured with RPR+ to a newer image with RPR+, the procedure is now complete. When the new active RP comes up, it will automatically configure RPR+ from the configuration information in the startup configuration (synchronized from the old active RP).

Performing a Manual Route Processor Switchover

For testing or maintenance, you may need to perform a manual switchover in which your standby RP becomes your active RP. Perform the following steps to force a manual switchover between RPs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show cable modem** **Example:** `Router> show cable modem`	Displays information for the registered and unregistered cable modems supported by the active RP. The output from this command provides information that confirms successful switchover in pending steps.
Step 2	**redundancy force-failover main-cpu** **Example:** `Router# configure terminal`	Forces a switchover on the active RP. The standby RP becomes the active RP with a switchover time of approximately 30 seconds or less. **Note** The modems do not redefine their ranges and the line cards do not reset during switchover.
Step 3	**show cable modem** **Example:** `Router> enable`	Displays information for the registered and unregistered cable modems supported by the newly active RP (formerly the standby RP).

Troubleshooting Route Processor Redundancy Plus

If RPR+ is not enabled after mode rpr-plus is run, verify that both the active and standby RPs are running Cisco IOS Release 12.2(11)BC3 or a later release.

Note If the active RP detects a different version of the image on the standby RP, the system automatically reverts to standard RPR behavior.

Configuration Examples for Route Processor Plus Redundancy

This section provides the following command examples that display the configuration and status of RPR+ on a Cisco uBR10012 router chassis with active and standby RPs. These commands all illustrate the same Cisco uBR10012 chassis:

- show redundancy
- show running configuration
- show version

The following show redundancy command displays the slots for the primary RP (PRE in slot 15), the secondary RP (PRE in slot 7), and additional redundancy mode information.

```
Router# show redundancy
Primary PRE in slot 15:
Secondary PRE in slot 7:
Preferred PRE: 15
Operating Redundancy Mode: RPR Plus
Auto synch: startup-config running-config
switchover timer 8 seconds [default]
```

The following show running configuration command displays RPR+ information such as main-cpu and auto-sync status.

```
Router# show run
Building configuration...
Current configuration : 10895 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
!
hostname "Router"
!
boot system flash bootflash:ubr10k-k8p6-mz.999-99.122BC_UB_030303
redundancy
 no keepalive-enable
 main-cpu
  auto-sync standard
no logging rate-limit
enable password cisco
!
facility-alarm intake-temperature major 49
```

```
facility-alarm intake-temperature minor 40
facility-alarm intake-temperature critical 57
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
facility-alarm core-temperature critical 60
card 1/0 1gigethernet-1
card 1/1 2cable-tccplus
card 3/0 1oc12pos-1
card 4/0 1gigethernet-1
card 5/0 2cable-mc28c
card 5/1 cable-lcp
card 6/0 2cable-mc28c
card 7/0 2cable-mc28c
card 8/0 1cable-mc16s
card 8/1 1cable-mc16s
cable modem max-cpe unlimited
cable spectrum-group 1 band 8000000 20000000
cable modulation-profile 1 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 1 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 1 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 1 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable service flow inactivity-threshold
cable time-server
ip subnet-zero
ip cef table resolution-timer 1
no ip domain lookup
ip host abrick 223.255.254.254
ip dhcp relay information option
!
ip dhcp pool modems-c6
   network 1.6.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.10.41.3
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.6.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c5
   network 1.5.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.5.1.65
   default-router 1.5.1.65
   option 7 ip 1.5.1.65
   option 4 ip 1.5.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c7
   network 1.7.1.64 255.255.255.224
   bootfile up2-down2-nobpi.cm
   next-server 1.10.41.3
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.7.1.65
   option 2 hex ffff.8f80
!
ip dhcp pool modems-c8
   network 1.8.1.64 255.255.255.224
   bootfile schcfr_new.cm
   next-server 1.8.1.65
   default-router 1.8.1.65
   option 7 ip 1.8.1.65
   option 4 ip 1.8.1.65
   option 2 hex ffff.8f80
```

```
!
ip dhcp pool modems-c51
   network 1.9.1.64 255.255.255.224
   bootfile config.cm
   next-server 1.10.41.3
   default-router 1.10.41.3
   option 7 ip 1.10.41.3
   option 4 ip 1.9.1.65
   option 2 hex ffff.8f80
!
ip multicast-routing
!
!
interface Loopback1
 ip address 222.1.1.1 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 1.10.41.3 255.255.0.0
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no cdp enable
!
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.0.0
 no negotiation auto
 no cdp enable
!
interface POS3/0/0
 ip address 200.200.0.1 255.255.0.0
 shutdown
 crc 32
 no cdp enable
 pos ais-shut
!
interface GigabitEthernet4/0/0
 no ip address
 negotiation auto
 no cdp enable
!
interface Cable5/0/0
 no ip address
 load-interval 30
 no keepalive
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 no cable upstream 0 concatenation
 cable upstream 0 data-backoff automatic
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 working 5
 hccp 1 channel-switch 5 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 1 channel-switch 5 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 1 reverttime 6
!
interface Cable5/0/0.1
 ip address 111.111.111.1 255.255.255.0 secondary
 ip address 1.5.1.65 255.255.255.224
 ip pim sparse-mode
 ip helper-address 1.10.41.3
 ip igmp static-group 239.0.0.11
 ip igmp static-group 239.0.0.12
 ip igmp static-group 239.0.0.14
 ip igmp static-group 239.0.0.16
 ip igmp static-group 239.0.0.32
 ip igmp static-group 239.0.0.35
 ip igmp static-group 239.0.0.36
 cable source-verify dhcp
 cable dhcp-giaddr policy
!
interface Cable5/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable6/0/0
 no ip address
 no keepalive
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 70
 cable upstream 0 frequency 12000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 working 6
 hccp 1 channel-switch 6 uc wavecom-ma 1.10.41.6 2 1.10.41.5 2
 hccp 1 channel-switch 6 nru rfswitch-group 1.10.41.7 80080000 2
!
interface Cable6/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable7/0/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 power-level 0
 no cable upstream 0 concatenation
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 hccp 1 protect 5 222.1.1.1
 hccp 1 channel-switch 5 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 1 channel-switch 5 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 1 protect 6 222.1.1.1
 hccp 1 channel-switch 6 uc wavecom-ma 1.10.41.6 2 1.10.41.5 2
 hccp 1 channel-switch 6 nru rfswitch-group 1.10.41.7 80080000 2
 hccp 1 timers 5000 15000
!
interface Cable7/0/1
 no ip address
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
!
interface Cable8/0/0
 no ip address
 ip access-group 99 in
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 spectrum-group 1
 cable upstream 0 power-level 0
 cable upstream 0 modulation-profile 2 1
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 threshold  cnr-profile1 21 cnr-profile2 11 Corr-Fec 11 Uncorr-Fec 21
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
 hccp 2 working 8
 hccp 2 channel-switch 8 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 2 channel-switch 8 nru rfswitch-group 1.10.41.7 80080000 1
!
interface Cable8/0/0.1
 ip address 1.8.1.65 255.255.255.224
 cable source-verify dhcp
!
interface Cable8/1/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 60
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 power-level 0
 cable upstream 1 shutdown
 cable upstream 2 power-level 0
 cable upstream 2 shutdown
 cable upstream 3 power-level 0
 cable upstream 3 shutdown
 cable upstream 4 power-level 0
 cable upstream 4 shutdown
 cable upstream 5 power-level 0
 cable upstream 5 shutdown
 hccp 2 protect 8 222.1.1.1
 hccp 2 channel-switch 8 uc wavecom-ma 1.10.41.6 2 1.10.41.5 1
 hccp 2 channel-switch 8 nru rfswitch-group 1.10.41.7 80080000 1
 hccp 2 timers 5000 15000
 no hccp 2 revertive
!
ip default-gateway 1.10.0.1
ip classless
ip route 1.9.0.0 255.255.0.0 1.10.0.1
ip route 2.6.0.0 255.255.0.0 200.200.0.2
ip route 223.255.254.254 255.255.255.255 1.10.0.1
no ip http server
ip pim bidir-enable
!
ip access-list standard XYZ
 permit any
ip access-list standard pqRS
 permit any
no logging linecard
access-list 3 permit 210.221.55.46
access-list 99 permit any
access-list 110 permit ip any any
access-list 110 permit udp any eq bootps any
access-list 111 permit udp any eq bootps any
arp 1.10.41.6 0020.4a51.1776 ARPA
arp 1.10.41.5 0020.4a51.00ea ARPA
no cdp run
snmp-server manager
tftp-server bootflash:up2-down2-nobpi.cm alias up2-down2-nobpi.cm
tftp-server bootflash:tony11.cm alias tony11.cm
tftp-server bootflash:up2-down2.cm alias up2-down2.cm
tftp-server bootflash:new-privacy.cm alias new-privacy.cm
tftp-server bootflash:10.cm alias 10.cm
tftp-server bootflash:att-10plus.cm alias att-10plus.cm
tftp-server bootflash:schcfr_new.cm alias schcfr_new.cm
tftp-server bootflash:test11.cm alias test11.cm
tftp-server bootflash:4us16ds.cm alias 4us16ds.cm
!
alias exec scm show cable modem
alias exec sqos show cable qos profile
alias exec shc show hccp
alias exec nd no debug all
alias exec sr show running-config
alias exec sip show ip interface b
alias exec dc debug hccp channel-switch
alias exec spm sh proc mem | in HCCP
alias exec de debug hccp event
alias exec ds debug hccp sync
alias exec dp debug hccp plane
alias exec dt debug hccp timing
alias exec dipc debug cr10k-rp ipc
alias exec dpm debug hccp plane message
alias exec dpp debug hccp plane packet
alias exec sib show ip int br
alias exec shb show hccp br
alias exec scs show cable spectrum-group
!
line con 0
 exec-timeout 0 0
line aux 0
 stopbits 1
 speed 19200
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 length 0
!
end
```

The following show version command displays active and standby RP status.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K-K8P6-M), Version 12.2(122BC.030303.)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 03-Mar-03 21:23 by
Image text-base: 0x60008954, data-base: 0x61B00000
ROM: System Bootstrap, Version 12.0(9r)SL2, RELEASE SOFTWARE (fc1)
amit-rp2 uptime is 57 minutes
```

```
System returned to ROM by reload at 02:05:40 UTC Sun Nov 26 2000
System image file is "bootflash:ubr10k-k8p6-mz.999-99.122BC_UB_030303"
cisco uBR10000 (PRE1-RP) processor with 393215K/131072K bytes of memory.
Processor board ID TBA05191959
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
Backplane version 1.0, 8 slot
Last reset from other pre
Toaster processor tmc0 is running.
Toaster processor tmc1 is running.
1 OC12 POS controller (1 POS)
1 TCCplus card(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Gigabit Ethernet/IEEE 802.3 interface(s)
1 Packet over SONET network interface(s)
8 Cable Modem network interface(s)
509K bytes of non-volatile configuration memory.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
32768K bytes of Flash internal SIMM (Sector size 256KB).
Secondary is up.
Secondary has 524288K bytes of memory.
Configuration register is 0x0
```

Additional References

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
CMTS Software Configuration Guide Guide	Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC
Cisco High Availability Initiatives	

Technical Assistance

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