



## CHAPTER 12

# N+1 Redundancy for the Cisco Cable Modem Termination System

---

**Revised: November 10, 2008, OL-1467-08**

This chapter provides procedures and commands by which to configure the N+1 Redundancy feature on the Cisco Cable Modem Termination System (CMTS), using the Cisco uBR10012 universal broadband routers with the Cisco 3x10 RF Switch.

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. N+1 redundancy, of which 4+1 redundancy is one version, is made possible with the addition of a single Cisco RF Switch to your cable headend network. Together with the Cisco uBR10012 router, the Cisco RF Switch provides a fully redundant system that enables cable operators to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

N+1 redundancy is an important step toward 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.

Beginning with Cisco IOS Release 12.2(15)BC2a, 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.

Global N+1 Line Card Redundancy, or HCCP Rapid Configuration, is a feature that 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 with the Cisco UBR-MC5X20S, Cisco UBR10-MC5X20U, and Cisco UBR10-MC5X20H broadband processing engines (BPEs). Support for global 7+1 redundancy was introduced in Cisco IOS Release 12.3(13a)BC. In Cisco IOS Release 12.3(17a)BC, global N+1 redundancy was extended to support 4+1 configurations.

Beginning in Cisco IOS Release 12.3(21)BC, the Cisco uBR10012 universal broadband router supports the HCCP Switchover Enhancements feature that implements performance improvements for traffic recovery during line card switchover under certain scalability limits. For networks with less than 5000 cable modems per line card, and less than 1000 voice calls per line card, these switchover improvements include under 1-second recovery for voice calls, and under 20-second recovery for data traffic. In addition, the keepalive failure logic is modified to improve false switchovers.

### 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 Firmware when configured in N+1 Redundancy.



**Note** The Cisco IOS CLI now synchronizes configurations between HCCP Working and Protect interfaces. Preconfiguration of the Protect interfaces is no longer required in most circumstances.

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

Both command-line interfaces above are required for configuration and testing of N+1 Redundancy.

### Cisco IOS Feature Specifications for N+1 Redundancy on the Cisco Cable Modem Termination System

Release	Modification
12.1(10)EC	HCCP support introduced on the Cisco uBR7200 series routers.
12.2(4)XF1, 12.2(4)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router and UBR10-LCP2-MC28C cable interface line card.
12.2(8)BC2	HCCP N+1 Redundancy support was added for the Cisco uBR10012 router and Cisco uBR10-LCP2-MC16x cable interface line cards.
12.2(11)BC1	HCCP N+1 Redundancy support was added for the Cisco uBR7246VXR router and Cisco uBR-LCP-MC16x cable interface line cards.
12.2(15)BC1	HCCP N+1 Redundancy support introduced for the Cisco uBR10012 router and Cisco UBR10-MC 5X20U or -S broadband processing engine (BPE).
12.2(15)BC2a	<ul style="list-style-type: none"> <li>• HCCP N+1 Redundancy support introduced for the Cisco uBR7246VXR router and the Cisco uBR 3x10 RF Switch.</li> <li>• CLI Usability—Synchronizes HCCP interface command-line interface (CLI) configuration between Working and Protect interfaces.</li> <li>• Support for N+1 Redundancy for the Cisco UBR10-MC 5X20U or -S BPE on the Cisco uBR10012 router.</li> <li>• <a href="#">IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters</a> — enables N+1 Redundancy on CMTS headends that do not use SNMP-enabled upconverters.</li> </ul>
12.3(13a)BC	<p>HCCP N+1 Redundancy on the Cisco 7200 series routers is no longer supported.</p> <p>The following enhancements were introduced to HCCP N+1 redundancy support on the Cisco uBR10012 router:</p> <ul style="list-style-type: none"> <li>• <a href="#">Global N+1 Line Card Redundancy</a></li> <li>• Automatic running of the <b>show hccp channel switch</b> command for <a href="#">Background Path Testing for HCCP N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router</a></li> </ul>

---

12.3(17a)BC	<p>The following High Availability enhancements were introduced for the Cisco CMTS:</p> <ul style="list-style-type: none"> <li>• Enhanced globally-configured N+1 Redundancy on the Cisco uBR10012 router: <ul style="list-style-type: none"> <li>– Added global 4+1 redundancy support to the existing global 7+1 redundancy on the Cisco uBR10012 router.</li> <li>– Supporting redundancy and <b>show</b> command enhancements</li> </ul> </li> <li>• Encrypted IP Multicast is supported during High Availability switchover events.</li> <li>• PHS rules synchronize and are supported during High Availability switchover events.</li> </ul>
12.3(21)BC	<p>The following support has been removed:</p> <ul style="list-style-type: none"> <li>• HCCP N+1 Redundancy support is removed for the Cisco uBR7246VXR router.</li> <li>• Tracking of HCCP interfaces is removed. The <b>hccp track</b> command is obsolete.</li> </ul> <p>The HCCP Switchover Enhancements feature is introduced on the Cisco uBR10012 router, with the following new support:</p> <ul style="list-style-type: none"> <li>• 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: <ul style="list-style-type: none"> <li>– Less than 1-second voice call recovery.</li> <li>– Less than 20-second data recovery.</li> </ul> </li> <li>• To prevent false switchovers, the keepalive failure logic is modified.</li> <li>• For faster line card switchovers, the <b>member subslot protect</b> command has been modified to add the [<b>config slot/subslot</b>] option. When using the new <b>config</b> option, you can preload upstream connectors on an HCCP protected interface to emulate the most common line card connector assignments.</li> </ul>

---

### Feature History for Cisco RF Switch Firmware

Several performance and configuration enhancements have been added to Cisco RF Switch firmware, released in the following most recent versions:

- Version 2.50—SNMPv1 Upconverters and Traps, Default Gateway for Remote TFTP Transfer
- Version 3.30—Improved switchover times, DHCP Server, several new commands or command enhancements for slot configuration and system information
- Version 3.50—Further improved switchover times, optimized ARP cache feature, ARP timeout configuration, and additional **show** command enhancements for ARP and configuration status
- Version 3.60 includes the following enhancements:
  - Changes to the network buffering to allocate a larger pool (number) of buffers, with a new number of 100 buffers total, to help handle an increase in SNMP traffic.
  - Reduction of the maximum packet size to 600 bytes. This combination of a larger number of buffers with smaller maximum packet size helps with handling large bursts of inbound packets that were discarded in previous versions of Cisco RF Switch Firmware.
  - Resolution of a problem in the SNMP agent to help further with the above items. In prior versions of Cisco RF Switch firmware, the SNMP agent blocked traffic just after packet reception, waiting to allocate a buffer in which to place the output response. If no buffer was available (as would be the case if a large burst of incoming packets occurred), the agent would

timeout, and the system would generate a watchdog timeout. Now, the agent uses a private buffer for the output response, and only requests a packet buffer after completing the snmp operation. If no buffer is available, the output response is discarded, and the agent continues processing inbound packets.

- Addition of the **noverify** option to the copy command, enabling you to override the file type verification, and place a file in either the flash (FL:) or bootflash (BF:) device. Version 3.60 updates the online help to reflect this new option. This new option provides the ability to place a copy of the main application into the bootflash, so that normal system operation is restarted in the case of a system crash, instead of having the "sys>" prompt as in previous versions of Firmware.
- Version 3.60 resolves a previous issue in which concurrent access to the RF switch modules via the command-line interface and SNMP would cause random errors and crashes. The firmware now allows simultaneous usage of telnet, console, and SNMP operation. This issue was observed primarily if the show version and test module commands were used at the same time that SNMP status polling operations were occurring. This previous issue also affected a number of additional commands.

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.

#### **Additional Cisco Broadband Cable High Availability Features**

Cisco High Availability (HA) for Broadband Cable products includes these and additional features:

- N+1 HCCP Redundancy
- DOCSIS Stateful Switchover (DSSO)
- Gigabit Ethernet
- PacketCable Support
- Route Processor Redundancy Plus (RPR+)

These and additional HA features are described further in the Cisco White Paper, *Cisco Cable IP Solutions for High-Availability Networks*, available on Cisco.com.

#### **Finding Support Information for Platforms and Cisco IOS Software Images**

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

## Contents

This chapter provides the following procedures and commands to configure, test and debug the N+1 Redundancy scheme on your Cisco universal broadband router CMTS:

- [Prerequisites, page 12-5](#)
- [Restrictions and Limitations, page 12-5](#)
- [Information About N+1 Redundancy and the Cisco Universal Broadband CMTS, page 12-9](#)
- [Manual RF Switch Configuration Tasks for N+1 Redundancy, page 12-20](#)
- [Global N+1 Line Card Redundancy, page 12-26](#)
- [How to Configure N+1 Redundancy on the Cisco CMTS, page 12-31](#)
- [Switchover Testing Tasks for N+1 Redundancy, page 12-48](#)

- [Configuration Examples for Cisco N+1 Redundancy, page 12-57](#)
- [Additional References, page 12-91](#)

## Prerequisites

To use N+1 HCCP 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 DOCSIS 1.1 requirements.
- Customer cable modems must meet requirements for your network and server offerings. All third-party cable modems must be DOCSIS 1.0- or DOCSIS 1.1-compliant and configured for two-way data communication.

## 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 prior to Cisco IOS Release 12.3(13a)BC, line card redundancy is configured at the interface configuration level using **hccp** commands. Beginning in Cisco IOS Release 12.3(13a)BC and later, enhancements to the N+1 line card redundancy configuration include a newer command-line interface (CLI) at the global configuration level, that replaces the legacy **hccp** interface command configuration. The newer feature is referred to as Global N+1 Line Card Redundancy, or Rapid HCCP Configuration. 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 and Limitations

These restrictions apply to N+1 Redundancy on the Cisco uBR10012 and Cisco uBR7246VXR routers in Cisco IOS Release 12.3(9a)BC and earlier Cisco IOS releases.

- When using the **show hccp channel switch** Cisco IOS command, the system communicates with each module in the RF Switch that comprises the bitmap. This requires a much longer period for timeout—contrasted with the lesser timeout required for the system to verify connectivity. Use the **show hccp g m channel** command to view each individual member of an HCCP group.

Cable upstream configuration commands are described in the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

- **HCCP interface configuration can be removed** from either Working or Protect Interfaces. However, the following HCCP restrictions apply to HCCP N+1 Redundancy on either the Cisco uBR10012 or Cisco uBR7246VXR router:
  - Before removing HCCP configurations from an active Working interface, either shut down the Protect or lockout switchover functions using the **hccp group lock member-id** command in global configuration mode. Otherwise the Protect interface may declare the Working interface to have failed and may attempt to switch over.

- Do not remove HCCP configurations from an active Protect interface. The active HCCP group member should be restored to its corresponding Working interface (revertback) 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.

For information about modifying HCCP configuration, refer to the section titled [“Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces”](#) section on page 12-45.

- **Downstream (DS) modulation, interleave depth and DOCSIS Annex mode** must be the same for all members in the same HCCP group. For configuration information, refer to the [“Preconfiguring HCCP Protect Interfaces for N+1 Redundancy”](#) section on page 12-33.
- **When using external, non-SNMP upconverters**, DS frequencies must be set to be the same across all cable interface line cards that are protected by the same Protect line card.

## N+1 Redundancy Restrictions and Requirements for the Cisco uBR7246VXR Router



**Note** As of Cisco IOS Release 12.3(21)BC, N+1 redundancy is no longer supported on the Cisco uBR7246VXR router.

- Cisco IOS Release 12.3(17a)BC support 4+1 redundancy on the Cisco uBR7246VXR router with the uBR-MC28C, uBR-MC16S and uBR-MC16C line cards only.
- Global N+1 redundancy configuration is not supported on the Cisco uBR7246VXR router.
- Cisco Systems recommends that the lowest slot interface be the master when configuring cable interface bundling on the Cisco uBR7246VXR router.
- Cisco uBR7246VXR CMTS interfaces that are bundled in IP switch over together.

## N+1 Redundancy Restrictions and Requirements for the Cisco uBR10012 Router

### Restrictions for Cisco IOS Release 12.2(15)BC2a

If you use DOCSIS 1.1 provisioned cable modems in your network and you are considering deploying Cisco IOS Release 12.2(15)BC2a, Cisco Systems recommends that you disable HCCP N+1 Redundancy until further notification, or that you reduce instances of manual switchover from HCCP Working to Protect via the command line interface (CLI).

Cable interface line cards in HCCP Working or Protect status may reload or experience intermittent failure during HCCP N+1 switchover in Cisco IOS Release 12.2(15)BC2a:

- Cable interface line cards that are in HCCP Working status may reload during N+1 switchover from HCCP Working to Protect status.
- You may experience HCCP memory overrun when cable interface line cards in HCCP Working status switch over to HCCP Protect status.

**General Requirements for the Cisco uBR10012 Router with All Cable Interface Line Cards**

- 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 TCC+ card, refer to the *Cisco uBR10012 Universal Broadband Router TCC+ Card* document available on Cisco.com:  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/installation/tcc5094.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/installation/tcc5094.html)
- Use the **IP address from the local loopback interface** as the Working interface IP address when configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router. Cisco strongly recommends 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.
- 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.
- **Cisco IOS downgrade** can be performed while retaining N+1 functionality, as supported by earlier Cisco IOS releases. However, when downgrading your Cisco IOS software from release 12.2(15)BC2a to an earlier release, N+1 Redundancy requires that you preconfigure the Protect interface(s) with the **cable upstream connector** command. Without this HCCP preconfiguration, the upstream channel does not come up again after a switchover.



**Note** Be careful if you plan to downgrade from Cisco IOS Release 12.3(13a)BC, when the Global N+1 Line Card Redundancy feature was introduced. The global N+1 configuration is not supported in earlier Cisco IOS software releases.

- The HCCP Switchover Enhancements feature in Cisco IOS Release 12.3(21)BC has the following restrictions:
  - The feature is supported on the Cisco uBR10012 router with the Cisco Performance Routing Engine 2 (PRE2) only.
  - The feature is supported by the following line cards on the Cisco uBR10012 router: Cisco UBR10-MC5X20S, Cisco UBR10-MC5X20U, and Cisco UBR10-MC5X20H
  - 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. For more information about configuring virtual interface bundling, see the “[Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS](#)” chapter.
  - Tracking of HCCP interfaces is removed. The **hccp track** command is obsolete.
  - In prior releases, a switchover could be triggered due to a keepalive failure regardless of how many cable modems were online for an upstream. This resulted in false switchovers. In Cisco IOS Release 12.3(21)BC, keepalive failure detection is now 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.

#### Restrictions with the Cisco UBR10-MC 5X20U or -S BPE

- **MAC domains and corresponding DS interface pairs switch over together.** Each ASIC processor on the Cisco UBR10-MC 5X20U or -S BPE 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.




---

**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.

---

#### Disabling HCCP Revertive on Protect Cable Interfaces

The cable interface line cards pair up interfaces that share the same JIB (ASIC processor) as explained in the restriction immediately above.

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 back automatically to active state. This is desirable behavior because it prevents revertback to active state prematurely—before the cause of an external failure is confirmed and remedied.



**Note**

---

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 back 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, Cisco Systems recommends 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 5X20U or -S in N+1 configuration, disable the revertive function on both Protect interfaces.

To disable the HCCP revertive function on Protect interfaces, use the **no hccp group revertive** command in cable interface configuration mode. Disable revertive on each HCCP Protect interface:

```
no hccp group revertive
```

**Syntax Description**

group	The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.
-------	---

For additional information about configuring or removing HCCP, refer to the “[How to Configure N+1 Redundancy on the Cisco CMTS](#)” section on page 12-31, and to the **hccp revertive** command in the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Information About N+1 Redundancy and the Cisco Universal Broadband CMTS

This section describes the following concepts that relate to N+1 Redundancy:

- [The Components and Terminology of N+1 Redundancy](#)
- [IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters](#)
- [DSX Messages and Synchronized PHS Information](#)
- [High Availability Support for Encrypted IP Multicast](#)

### The Components and Terminology of N+1 Redundancy

N+1 Redundancy is made possible with the addition of the Cisco RF Switch to your cable headend network. 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 router chassis.

N+1 Redundancy is available for these Cisco Cable Modem Termination System (CMTS) platforms:

**Table 1 Cisco CMTS Platforms Supporting N+1 Redundancy**

CMTS Platform/N+1	Line Cards or BPEs	Supported Upconverters	Cisco RF Switch
Cisco uBR10012	<ul style="list-style-type: none"> <li>• UBR10-LCP2-MC16C</li> <li>• UBR10-LCP2-MC16C=</li> <li>• UBR10-LCP2-MC16E</li> <li>• UBR10-LCP2-MC16E=</li> <li>• UBR10-LCP2-MC16S</li> <li>• UBR10-LCP2-MC16S=</li> <li>• UBR10-LCP2-MC28C</li> <li>• UBR10-LCP2-MC28C</li> <li>• UBR10-MC5X20U, -S, or -H</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP with RF Muting</li> <li>• Non-SNMP<sup>1</sup> with IF Muting</li> </ul>	Cisco 3x10 RF Switch (one or multiple)
Cisco uBR7246VXR	<ul style="list-style-type: none"> <li>• UBR-MC28C</li> <li>• UBR-MC16S</li> <li>• UBR-MC16C</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP with RF Muting</li> <li>• Non-SNMP<sup>1</sup> with IF Muting</li> </ul>	Cisco 3x10 RF Switch (two)

1. Non-SNMP upconverters are supported beginning with Cisco IOS Release 12.2(15)BC2a.

N+1 Redundancy refers to Working cable interface line cards (N) being protected by one additional line card (+1). The two types of Cisco N+1 configuration are as follows:

- 8+1 (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. This redundancy scheme is also referred to as 7+1 redundancy, which 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.

Upconverters may reside between the Cisco RF Switch and the downstream (DS) interface on the Cisco CMTS. Cisco IOS supports both SNMP and non-SNMP-capable upconverters.

## N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router

The eight-card 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, each featuring one to five downstream and six to 20 upstream cable interfaces for a total of up to 40 downstream and 160 upstream interfaces in the chassis.

A single Cisco RF Switch can then be connected to this Cisco uBR10012 CMTS, 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.

The Cisco uBR10012 router supports N+1 Redundancy on the following Cisco uBR10012 cable interface line cards (broadband processing engines—BPEs):

Cable Interface Line Card	N+1 Redundancy Introduced
Cisco UBR10-MC5X20H	Cisco IOS Release 12.3(17a)BC2
Cisco UBR10-MC 5X20U or -S	Cisco IOS Release 12.2(15)BC2a
Cisco UBR10-MC 5X20U or -S	Cisco IOS Release 12.2(15)BC1
Cisco uBR10-LCP2-MC16C, Cisco uBR10-LCP2-MC16E, Cisco uBR10-LCP2-MC16S	Cisco IOS Release 12.2(8)BC2 <b>Note</b> Beginning in Cisco IOS Release 12.2(15)BC2a, these cable line card interfaces are end-of life (EOL).
UBR10-LCP2-MC28C	Cisco IOS Release 12.2(4)XF1, 12.2(4)BC1

The Cisco uBR10012 router contains eight slots, numerated as shown in [Figure 1](#), using the slot/port CLI convention (for example, slot 8/0).

A Cisco uBR10012 router identifies a subinterface addresses by slot number, subslot number, and downstream (DS) port number, in the format slot/subslot/DS port. For example, the address of a subinterface could be 5/1/0 (slot 5, subslot 1 and DS port 0).

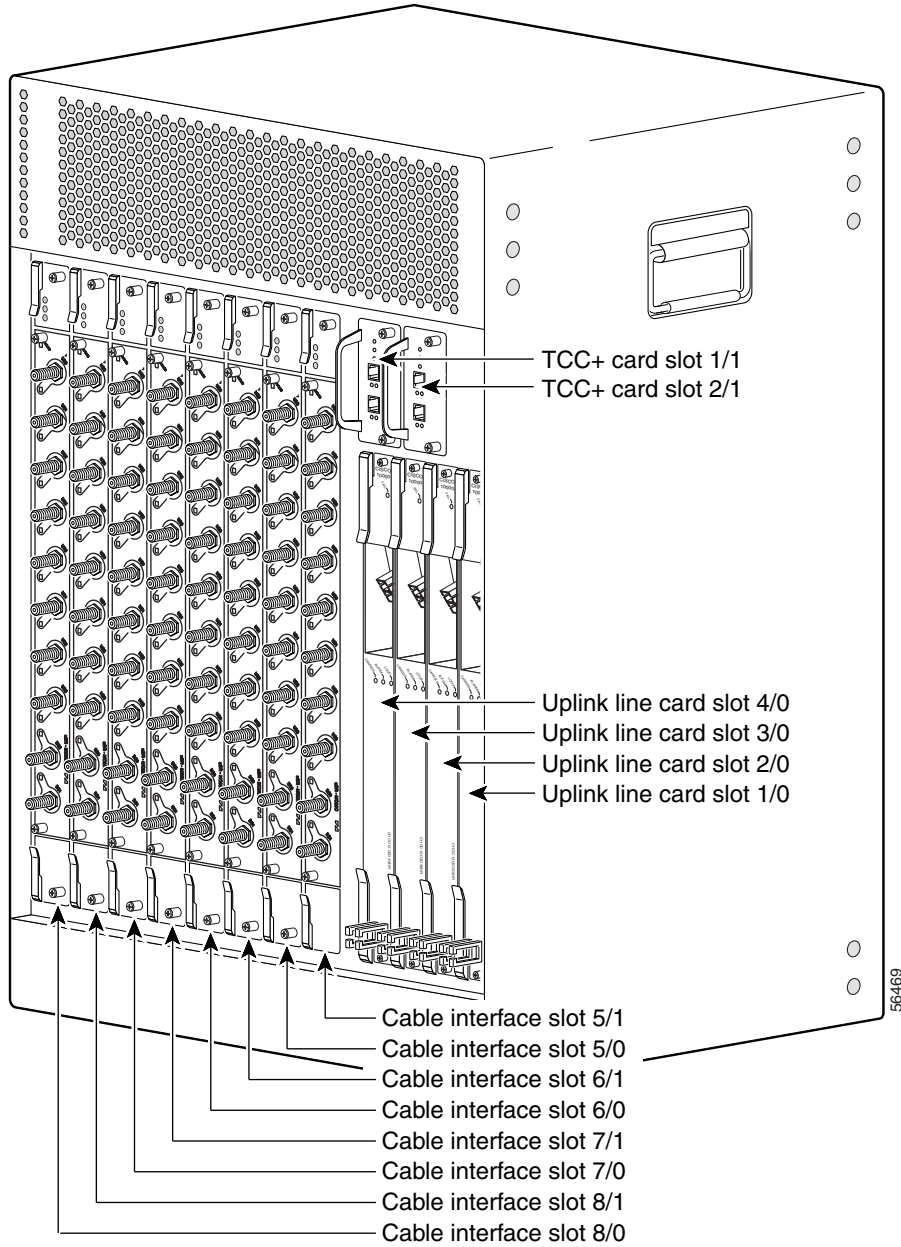
Cisco IOS command line syntax is unique when selecting or defining slots, subslots and ports for the Cisco uBR10012 router. For example, the syntax of the Cisco IOS command **interface cable slot/subslot/port** identifies a cable interface on the Cisco uBR10012 router. The following are the valid values for this and similar such commands:

- *slot* = 5 to 8
- *subslot* = 0 or 1
- *port* = 0 to 4 (depending on the cable interface)

Figure 1 illustrates the numeration of these cable interfaces on the Cisco uBR10012 router chassis.

**Chassis Slot Numeration and Selection on the Cisco uBR10012 Router**

**Figure 1 Cisco uBR10012 Chassis Slot Numeration –Rear View**



## N+1 Redundancy on the Cisco uBR7246VXR Universal Broadband Router

The 4+1 redundancy scheme for the Cisco uBR7246VXR router supports redundancy for the cable interface line cards installed in four fully populated router chassis.



### Note

Cisco Systems recommends using the chassis with the most memory, network processing engine (NPE) power and additional resources as the Protect chassis.

Each Cisco uBR7246VXR can support up to four Cisco cable interface line cards, each featuring one or two downstream and six or eight upstream cable interfaces, for a total of up to eight downstream and 32 upstream interfaces in the chassis.

Two Cisco RF Switches can be connected to four Working and one Protect Cisco uBR7246VXR routers, allowing you to deploy an N+1 Redundancy scheme in which one protecting cable interface line card in the Working uBR7246VXR supports one Working cable interface line card in each of the four Working chassis.

The Cisco uBR7246VXR router supports N+1 Redundancy on the following cable interface line cards:

Cable Interface Line Card	N+1 Redundancy Introduced
Cisco uBR-MC16S/C	Cisco IOS Release 12.2(15)BC2a
Cisco uBR-MC28C	Cisco IOS Release 12.2(15)BC2a

### Chassis Slot Numeration on the Cisco uBR7246VXR Router

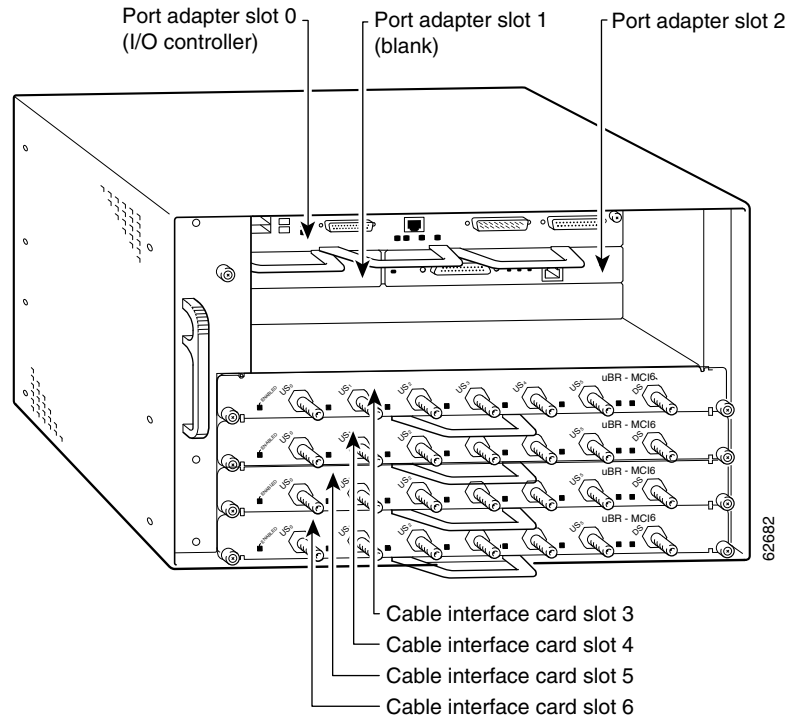
For Cisco uBR7200 series components, the slot number is the chassis slot in which a port adapter or a cable interface card is installed. The logical interface number is the physical location of the interface port on a port adapter. Numbers on a Cisco uBR7200 series router begin with 0.

Using a Cisco uBR7246VXR router chassis to illustrate, slot/port positioning is as follows:

- Slot 0—I/O controller
- Slot 1-2—Cisco port adapters
- Slot 3-6—Cisco cable interface line cards; the upstream ports on the card start with port 0.

For the Cisco uBR7246VXR reference design discussed in this guide, line card (LC) 1 in Cisco uBR7246VXR 5 protects the Working LC 1 in router chassis 1, 2, 3, and 4. LC 2 in chassis 5 protects the Working line card 2 in chassis 1, 2, 3, and 4, and so forth.

Figure 2 Cisco uBR7246VXR Router Chassis Slot Numbering—Rear View



## N+1 Redundancy and the Cisco RF Switches

The Cisco RF Switch can be operated in two separate modes, either in 8+1 configuration, or in 4+1 configuration as two RF Switches.



### Note

The default N+1 Redundancy mode for the Cisco RF Switch is 8+1. This does not require change when configuring N+1 Redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20U or -S BPE.

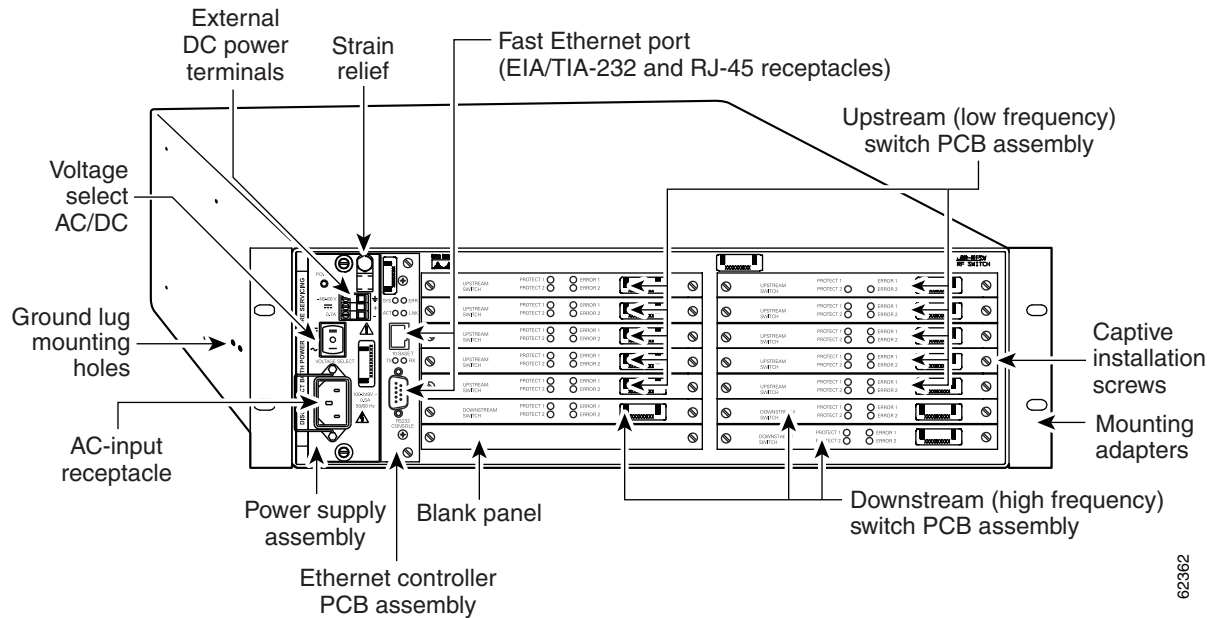


### Note

The **show configuration** command and other Cisco RF Switch commands contain 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.

## Cisco 3x10 RF Switch Chassis Overview

**Figure 3** Cisco RF Switch Chassis—Front View



62362

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 MAC-layer or hardware address is a standardized data link layer address that is required for certain network interface types. The Cisco RF Switch uses a specific method to assign and control the MAC-layer addresses of its Ethernet controller.

The Ethernet controller and upstream and downstream assembly slots maintain the same slot number regardless of whether other Ethernet controllers or upstream or downstream cards have been installed or removed. However, when you move an upstream or downstream card to a different slot, the logical interface number changes to reflect the new slot number. The Ethernet card is always installed in the same slot.

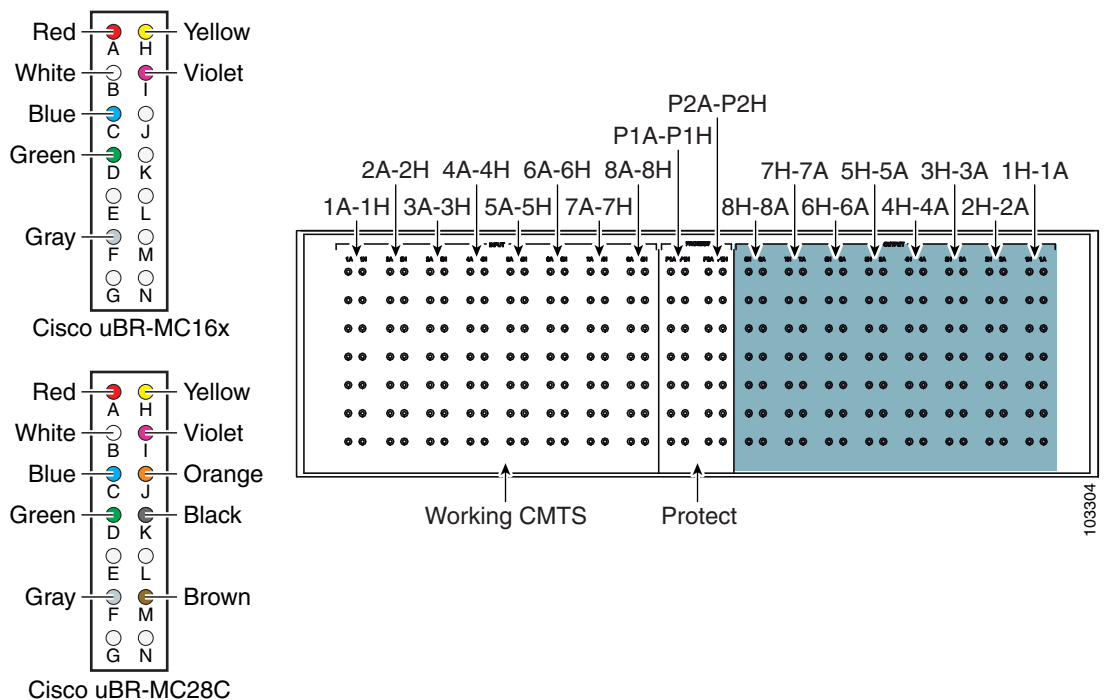
All LAN interfaces (ports) require unique MAC-layer addresses, also known as hardware addresses. Typically, the MAC address of an interface is stored on a memory component that resides directly on the interface circuitry; however, the OIR feature requires a different method.

The OIR feature allows you to remove an Ethernet controller or an upstream or downstream assembly and replace it with another identically configured one. If the new controller or assembly matches the controller or assembly you removed, the system immediately brings it online. In order to allow OIR, an address allocator with a unique MAC address is stored in an EEPROM on the Cisco RF Switch midplane. Each address is reserved for a specific port and slot in the switch, regardless of whether an Ethernet controller or an upstream or downstream assembly resides in that slot.

The MAC addresses are assigned to the slots in sequence. The first address is assigned to Ethernet controller slot 0, and the next addresses are assigned to upstream and downstream assembly slots 1 through 14. This address scheme allows you to remove the Ethernet controllers or assemblies and insert them into other switches without causing the MAC addresses to move around the network or be assigned to multiple devices.

Cisco RF Switch Modules

Figure 4 Cisco RF Switch Modules, Rear View



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.

The RF Switch header block has 14 ports labeled with letters. Each header screws into a slot in the Cisco RF Switch. A Cisco RF Switch module contains all the active relays for a particular port for all slots.

Cisco uBR 3x10 RF Switch Slot Information

Table 2 lists the RF modules and the ports assigned to each module, as illustrated in Figure 4.



Tip

The modules are listed as seen from the front of the RF switch.

Table 2 Switching Matrix for the Cisco uBR 3x10 RF Switch (Upstream and Downstream Modules)

RFS Module	Working Ports	PROTECT Ports	Type	RFS Module	Working Ports	PROTECT Ports	Type
2	1H—8H	P1H, P2H <sup>1</sup>	upstream	1	1A—8A	P1A, P2A	upstream
4	1I—8I	P1I, P2I	upstream	3	1B—8B	P1B, P2B	upstream
6	1J—8J	P1J, P2J	upstream	5	1C—8C	P1C, P2C	upstream
8	1K—8K	P1K, P2K	upstream	7	1D—8D	P1D, P2D	upstream
10	1L—8L	P1L, P2L	upstream	9	1E—8E	P1E, P2E	upstream
12	1M—8M	P1M, P2M	downstream	11	1F—8F	P1F, P2F	downstream
14	not used	—	—	13	1G—8G	P1G, P2G	downstream

1. P2 is used only when the switch is in 4 + 1 mode.

**Example:**

Modules 1-10 below are upstream (US) modules in the Cisco uBR 3x10 RF Switch.

The remainder of the modules are either assigned to downstream functions or are not used.

- Module 1 uses Port a for slots 1-8 on the Working, and it uses Port a of Protect slot 1 and/or Protect slot 2.
- Module 2 uses CMTS Ports 1h through 8h, and Protect Port 1h and Protect Port 2h.
- Module 3 uses port b.
- Module 4 uses port i.
- Module 5 uses port c.
- Module 6 uses port j.
- Module 7 uses port d.
- Module 8 uses port k.
- Module 9 uses port e.
- Module 10 uses port l.
- Module 11 uses port f.
- Module 12 uses port m.
- Module 13 uses port g.
- Module 14 uses port n, which is not used on the Cisco uBR 3x10 RF Switch.

The Cisco uBR 3x10 RF Switch works with the Cisco uBR10012 router and supports three downstream modules and 10 upstream modules. Each RF switch module supports the full frequency range specified by DOCSIS and EuroDOCSIS standards.

## IF Muting on the Cisco CMTS for non-SNMP-capable Upconverters

Beginning with Cisco IOS Release 12.2(15)BC2a, Cisco supports IF Muting with both SNMP and non-SNMP-capable upconverters 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 headends.
- IF Muting offers the additional benefit of being faster than RF Muting.
- IF Muting is enabled by default. The Cisco CMTS automatically enjoys the benefits and availability of IF Muting.

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:

- Case 1—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.

- This type of Cisco CMTS is newly supported with Cisco IOS Release 12.2(15)BC2a. Previously, such customers could not enable N+1 Redundancy in the Cisco CMTS headend because they use upconverters that previously could not be controlled from the Cisco CMTS.
- 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), as with the Cisco UBR10-MC 5X20U or -S BPE. 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.

For additional details, refer to the procedures in these sections:

- [Manual RF Switch Configuration Tasks for N+1 Redundancy, page 12-20](#)
- [How to Configure N+1 Redundancy on the Cisco CMTS, page 12-31](#)

## 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.

**cable downstream frequency** *down-freq-hz*

**no cable downstream frequency**

The **no** form of this command is supported only on the Cisco uBR-MC28U/X cable interface line card and the UBR10-MC 5X20U or -S.

- *down-freq-hz*—The known center frequency of the downstream carrier in Hz (the valid range is 55 MHz to 858 MHz). 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.

For additional information about this command, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## 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.

## 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](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](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/reference/guide/mibv5ubr.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/tech/tk828/technologies\\_case\\_study0900aecd802e2ce2.shtml](http://www.cisco.com/en/US/tech/tk828/technologies_case_study0900aecd802e2ce2.shtml)
- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/u10krprp.html>

# Manual RF Switch Configuration Tasks for 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. You must also configure HCCP Working interfaces and groups.

Perform these procedures in sequence when configuring N+1 Redundancy on the Cisco RF Switch.

	Procedure	Purpose
Step 1	<a href="#">“Configuring the Cisco RF Switch for N+1 Redundancy” procedure on page 12-20</a>	(Required) Provides required and optional configurations on the Cisco RF Switch, including MAC and IP addressing, SNMP configurations, and switchover interface groups.
Step 2	<a href="#">“Creating Cisco RF Switch Module Bitmaps” procedure on page 12-23</a>	(Required) Provides required configuration of hexadecimal-format module bitmaps that indicate which upstream (US) and downstream (DS) modules belong to a switchover group.

## Configuring the Cisco RF Switch for N+1 Redundancy

### SUMMARY STEPS

1. **set mac address** *mac-address* (optional)
2. **set ip address** *ip-address netmask* (optional)
3. **set slot config** { *upstreamslots* | *downstreamslots* } (optional)
4. **set snmp community read-write private** (optional)
5. **set snmp host** *ip-address* (optional)
6. **set snmp traps** (optional)
7. **set protection** {4|8} (required)
8. **set password** *text* (optional)
9. **set tftp-host** *ip-address* (optional)
10. **set switchover-group** *group-name module-bitmap* | **all** (required)

## DETAILED STEPS

	Command	Purpose
Step 1	<p><b>set mac address</b> <i>mac-address</i></p> <p><b>Example:</b>  <pre>rfswitch&gt; set mac address 0000.8c01.1111</pre></p>	<p>(Optional) To specify the MAC address of the Ethernet port on the Cisco RF Switch (used to connect to the LAN), use the <b>set mac address</b> command at the Cisco RF Switch command line interface.</p> <p>The MAC address must be specified using a trio of hexadecimal values. For example, <b>set mac address</b> <i>hex.hex.hex</i>. To negate the existing MAC address assignment and specify a new one, use the <b>no</b> form of this command. If no MAC address is specified, the Cisco RF Switch assumes the default OUI MAC address value.</p>
Step 2	<p><b>set ip address</b> <i>ip-address</i> <i>netmask</i> [ <b>dhcp</b> ]</p> <p><b>Example:</b>  <pre>rfswitch&gt; set ip address 172.16.10.3 255.255.255.0</pre></p>	<p>(Optional) To specify a static IP address and relative netmask of the Ethernet interface on the Cisco RF Switch, use the <b>set ip address</b> command in User mode. To restore the default setting, use the <b>no</b> form of this command.</p> <p>Default setting differs according to your Firmware Version:</p> <ul style="list-style-type: none"> <li>• The default IP configuration for Version 3.30 and 3.50 is DHCP enabled.</li> <li>• The <b>dhcp</b> keyword enables the specified IP address as the address for DHCP services on the network. This keyword also produces the same result as the <b>no</b> form of this command for Version 3.30 and 3.50—it enables DHCP.</li> <li>• The default IP configuration for Version 2.50 is the static IP address of 10.0.0.1 255.255.255.0.</li> </ul>
Step 3	<p><b>set slot config</b> { <i>upstreamslots</i>   <i>downstreamslots</i> }</p> <p><b>Example:</b></p> <p><b>Cisco 3x10 RF Switch (default)</b>  <pre>rfswitch&gt; set slot config 0x03ff 0x1c00</pre></p>	<p>(Optional) Sets the chassis slot-to-line card configuration. The command <b>no set slot config</b> restores the default, which is a 3x10 configuration.</p> <p>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 <i>upstreamslots</i> and <i>dnstreamslots</i> 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.</p> <p>For additional bitmap conversion information, refer to the <i>Bitmap Calculator for N+1 Configuration with the Cisco RF Switch</i> (Microsoft Excel format)</p> <p><a href="http://www.cisco.com/warp/public/109/BitMap.xls">http://www.cisco.com/warp/public/109/BitMap.xls</a></p> <p>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.</p> <p><b>Note</b> Changes made to the slot configuration on the Cisco RF Switch do not take effect until the system is rebooted (<b>reload</b> command), or an event occurs which causes the enumeration of the chassis line cards to reset.</p>

Step 4	<pre>set snmp community read-write private</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set snmp community read-write private</pre></p>	<p>(Optional) To specify the Simple Network Management Protocol (SNMP) community string on the Cisco RF Switch, use the <b>set snmp community</b> command at the Cisco RF Switch command line interface.</p> <p>This command enables you to gain read and write access to the Cisco RF Switch. The <i>community</i> string must be entered as a string of text. To negate the existing <i>community</i> string and make way for a new one, use the <b>no</b> form of this command. If no SNMP string is entered, the SNMP string assumes the default value <b>private</b>.</p> <p><b>Note</b> Currently, the <b>private</b> keyword is the only SNMP community string supported on communication between the Cisco RF Switch and the Cisco uBR10012 router. The default value of <b>private</b> is the proper setting under normal circumstances.</p>
Step 5	<pre>set snmp host ip-address</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set snmp host 172.16.10.3</pre></p>	<p>(Optional) To specify the IP address that receives SNMP notification messages, use the <b>set snmp host</b> 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 <b>no</b> form of this command. If no SNMP IP address is specified, the Cisco RF Switch does not transmit any SNMP notification messages.</p>
Step 6	<pre>set snmp traps</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set snmp traps</pre></p>	<p>(Optional) To enable SNMP reporting for all modules on the Cisco RF Switch, use the <b>set snmp traps</b> command in the Cisco RF Switch User mode. To deactivate SNMP reporting, use the <b>no</b> form of this command. SNMP reporting is enabled by default on the Cisco RF Switch.</p>
Step 7	<pre>set protection {4 8}</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set protection 8</pre></p>	<p>(Required) To set the line card protection scheme, specifying the N+1 protection scheme under which the Cisco RF Switch operates, use the <b>set protection</b> command in Cisco RF Switch User mode.</p> <ul style="list-style-type: none"> <li>• <b>set protection 4</b>—Specifies that the Cisco RF Switch operate using a 4+1 protection scheme.</li> <li>• <b>set protection 8</b>—Specifies that the Cisco RF Switch operate using an 8+1 protection scheme.</li> </ul> <p>To negate the existing protection scheme specification, use the <b>no</b> form of this command. The default protection scheme for the Cisco RF Switch is 8+1.</p>
Step 8	<pre>set password text</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set password cisco</pre></p>	<p>(Optional) To specify an access password for the Cisco RF Switch command line interface, use the <b>set password</b> command at the Cisco RF Switch command line interface. To negate the existing access password, use the <b>no</b> form of this command.</p>
Step 9	<pre>set tftp-host ip-address</pre> <p><b>Example:</b>  <pre>rfswitch&gt; set tftp host 172.16.10.17</pre></p>	<p>(Optional) To specify the host IP address of the TFTP server through which the Cisco RF Switch enables file transfer, use the <b>set tftp-host</b> command at the Cisco RF Switch command line interface. To negate an existing host IP address specification for the remote TFTP server, use the <b>no</b> form of this command. (No default TFTP server IP address is supported on the Cisco RF Switch.)</p>

<p><b>Step 10</b> <code>set switchover-group</code> <code>group-name module-bitmap   all</code></p> <p><b>Example:</b> rfswitch&gt; set switchover-group a12345 0xAA200000</p>	<p>(Required) To specify a new or existing switchover group name (to which a Cisco RF Switch module is assigned), use the <b>set switchover group</b> 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.</p> <ul style="list-style-type: none"> <li>• <i>group-name</i> — Can be an alpha-numeric string beginning with a non-numeric character.</li> <li>• <i>module-bitmap</i> — Defines a Cisco RF Switch module, and must be specified as an eight-character hexadecimal identifier or assigned the <b>all</b> keyword.</li> </ul> <p><b>Note</b> Refer to the “<a href="#">Creating Cisco RF Switch Module Bitmaps</a>” section on <a href="#">page 12-23</a> for instructions on creating an appropriate hexadecimal module bitmap.</p> <ul style="list-style-type: none"> <li>• <b>all</b> — Keyword instructs the Cisco RF Switch to automatically switch over all upstream and downstream interfaces connected to the switch module in question.</li> </ul> <p><b>Note</b> When setting bit maps on the RF Switch, type <b>0x</b> 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.</p> <p>To negate an existing switchover group, use the <b>no set switchover-group</b> command at the Cisco RF Switch command line interface.</p> <p><b>Note</b> You do not need to specify <i>module-bitmap</i> when negating an existing switchover group. For example, the command <b>no set switchover-group a12345</b> will eliminate the switchover group named “a12345.”</p> <p>Once a switchover group containing one or more Cisco RF Switch modules has been defined, you can use the <b>switch</b> command to enable N+1 Redundancy behavior on the Cisco RF Switch, as described in the following section, “<a href="#">Switchover Testing Tasks for N+1 Redundancy</a>.”</p>
<p><b>Step 11</b> <code>save config</code></p> <p><b>Example:</b> rfswitch&gt; save config</p>	<p>This command saves the latest configuration or image upgrade changes in both Flash and Bootflash, and synchronizes Backup and Working copies in each.</p>
<p><b>Step 12</b> <code>reboot</code> or <code>reload</code></p> <p><b>Example:</b> rfswitch&gt; reload</p>	<p>This command restarts the Cisco RF Switch so that all changes above take effect.</p>

## 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.





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**

Cisco Systems recommends 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” section on page 12-8](#).

## Global N+1 Line Card Redundancy

Cisco IOS release 12.3(13a)BC introduces the Global N+1 Line Card Redundancy (or, HCCP Rapid Configuration) feature on the Cisco uBR10012 router to streamline the configuration of N+1 line card redundancy. The feature implements a simpler command-line interface (CLI) to establish the working and protect line card relationships, which no longer requires configuration of the legacy **hccp** interface configuration commands.

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.

For installations in which maximum granularity is required for downstream-based switchover capabilities on a line card (and not the full line card switchover supported by global N+1 redundancy), Cisco IOS Release 12.3(13a)BC continues to support manual configuration of **hccp** commands for 7+1

and 4+1 Redundancy, as in prior Cisco IOS Releases, and as described elsewhere throughout this document. However, globally-configured N+1 line card redundancy and the legacy form of HCCP line card redundancy configurations are mutually exclusive.

This section, supported only for Cisco IOS Release 12.3(13a)BC and later 12.3 BC releases, contains the following information about globally-configured N+1 line card redundancy:

- [Configuring the Cisco uBR10012 Universal Broadband Router for Global N+1 Line Card Redundancy, page 12-27](#)
- [Default Line Card and Bitmap Settings on the Cisco RF Switch for Global 7+1 Line Card Redundancy, page 12-28](#)
- [Changing Default RF Switch Subslots for N+1 Line Card Redundancy, page 12-28](#)
- [Displaying Global N+1 Line Card Redundancy Configuration, page 12-28](#)
- [Configuring DHCP on the Cisco uBR10012 Universal Broadband Router to Assign IP Addresses on the Cisco RF Switch, page 12-29](#)
- [Using Optional RF Switch Settings with Global N+1 Redundancy, page 12-30](#)
- [Using Line Card Switchover and Revertback Commands for Global N+1 Redundancy, page 12-31](#)
- [Using HCCP Lock and Unlock for Global N+1 Redundancy, page 12-31](#)

## Configuring the Cisco uBR10012 Universal Broadband Router for Global N+1 Line Card Redundancy

Cisco IOS Release 12.3(13a)BC introduces the following set of simpler CLI on the Cisco uBR10012 universal broadband router to configure global N+1 line card redundancy:

- **redundancy** command in global configuration mode
- **linecard-group 1 cable** command in redundancy configuration mode

The command immediately above auto-enables line card redundancy configuration mode.



---

**Note** The *group\_num* value of 1 is the only option for global configuration.

---

- **member subslot slot/subslot working [rfs-sw-slot n]** command in line card redundancy configuration mode
- **member subslot slot/subslot protect** command in line card redundancy configuration mode



---

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

---

For information about how to configure global N+1 line card redundancy, see the “[Configuring Global HCCP 4+1 and 7+1 Line Card Redundancy on the Cisco uBR10012 Router](#)” section on page 12-39.

## Default Line Card and Bitmap Settings on the Cisco RF Switch for Global 7+1 Line Card Redundancy

The Cisco 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 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
<b>RFSw-Slot 7+1 mode</b>	7	0	5	6	3	4	1	2



**Note**

Value 0 signifies by default the Protect slot.



**Note**

RFSw-Slot header and RFSwitch slot # refer to the same thing.

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

To change the factory configuration of subslot mapping to a custom (non-default) mapping, use the following optional command in line card redundancy mode. This command specifies a non-default rf-switch subslot:

```
member subslot X/Y working rfsw-slot [1 | 2 | 3 | 4... | 8 ]
```

This 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 (rfsw-slot). For example, interface 7/0 might need to be wired to rfsw-slot 7 (instead of the default 3).

## Displaying Global N+1 Line Card Redundancy Configuration

When you configure redundancy-level commands on the Cisco uBR10012 router for global N+1 line card redundancy, the running configuration shows only the line card redundancy configuration commands.

To display the corresponding interface-level HCCP configuration that results from your global line card redundancy configuration, use the **show redundancy linecard all** command in privileged EXEC mode.

For example, in the following global configuration of 7+1 line card redundancy, interface 8/0 is configured as the Working line card, and interface 7/0 is configured as the Protect line card:

```
Router# show redundancy linecard all
  Interface Config  Grp Mbr RfSw-Name  RfSw-IP-Addr  RfSw-Slot Bitmap
-----
Ca5/1/0  Protect   1  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca5/1/1  Protect   2  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca5/1/2  Protect   3  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca5/1/2  Protect   3  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF
Ca5/1/3  Protect   4  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF
Ca5/1/4  Protect   5  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF

Ca8/0/0  Working   1  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca8/0/1  Working   2  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca8/0/2  Working   3  80  rfsw-2    10.10.107.201  1      0xFFFFFFFF
Ca8/0/2  Working   3  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF
Ca8/0/3  Working   4  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF
Ca8/0/4  Working   5  80  rfsw-1    10.10.107.202  1      0xFFFFFFFF
```

This command shows what the associated interface-level HCCP configuration is, with automatically assigned values like rfsw-name, rfsw-slot and bitmap used, and so forth.

## Configuring DHCP on the Cisco uBR10012 Universal Broadband Router 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.bbccc.ddee.ff
!
ip dhcp pool rfsw-2 [ DHCP MAC->IP mapping for RF-switch # 2 ]
  host b.c.d.f <mask>
  client-id 01aa.bbccc.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 rfs-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 rfs-1 only gets IP address 10.10.107.202, and rfs-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.

## Using Optional RF Switch Settings with Global N+1 Redundancy

The following optional command syntax can be used in redundancy and line card redundancy configuration mode:

```

Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# ?
linecard group configuration commands:
exit          Exit from linecard group configuration mode
member        Add or remove a LC member into redundancy group
no            Negate a command or set its defaults
rf-switch     Specify/Change RF-switch parameters (Optional Command)

Router(config-red-lc)# rf-switch ?
name          new name string
protection-mode RF-Switch protection mode {7+1 or ...}
snmp-community SNMP community name
```

**Syntax Description**

<i>name</i>	Alphanumeric name to replace the default name of the Cisco RF Switch.
-------------	---

Cisco IOS Release 12.3(13a)BC uses default names for the Cisco RF-switch names ("rfs-1" for switch 1 and rfs-2 for switch 2). These default names 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 of rfs-1" and rfs-2, then enter the new RF Switch name as part of line card redundancy configuration using the following optional configuration commands:

```
Router(config-red-lc)# [no] rf-switch name {1|2} name
```

b. community string

To configure a non-default snmp-community string, use the following command in line card redundancy configuration mode:

```
Router(config-red-lc)# [no] rf-switch snmp-community community-name
```

This string can only be configured under config priv level 15.

This command updates the uBR10K 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. So configuring new community on the RF-switch, is user's responsibility.

## Using Line Card Switchover and Revertback Commands for Global N+1 Redundancy

Cisco IOS Release 12.3(13a)BC enables the switchover on an entire line card at one time, instead of one interface at a time. To switch over a cable interface line card, 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 back 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 back 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.

## Using HCCP Lock and Unlock for Global N+1 Redundancy

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

```
Router# redundancy linecard-group [un]lockout <working-slot>/<working-subslot>
```

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.

## How to Configure N+1 Redundancy on the Cisco CMTS

You must configure and activate both the Cisco RF Switch and the Cisco CMTS to ensure that N+1 Redundancy operates correctly. Several factory-configured options are available.

**Note**

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.

Perform these procedures when configuring N+1 Redundancy on the Cisco CMTS. Procedures vary in applicability, according to your equipment of choice and Cisco IOS release. You do not require every procedure, but selected procedures depending on your installation.

**Note**

Global configuration procedures introduced in Cisco IOS Release 12.3(13a)BC render previous interface-level configuration of **hccp** commands obsolete. Legacy HCCP configuration and the newer global N+1 redundancy configuration are mutually exclusive. N+1 redundancy configuration commands prior to release 12.3(13a)BC can not be supported with a global N+1 redundancy configuration.

Procedure	Purpose
<a href="#">Preconfiguring HCCP Protect Interfaces for N+1 Redundancy</a>	(Required for interface-level configuration) Defines three functions on the HCCP Protect interfaces: DS modulation, DS interleave depth, and DOCSIS Annex mode.
<a href="#">Operating DHCP with the Cisco RF Switch</a>	(Optional in all cases) Provides instructions for using the DHCP client. DHCP operation is enabled by default, unless you have set a static IP address from the RF Switch command-line interface (CLI). Commands have been added or enhanced to support DHCP operation.
<a href="#">Configuring HCCP Groups for Legacy N+1 Line Card Redundancy</a>	(Required for interface-level configuration) Defines HCCP Working and Protect interfaces, Cisco RF Switch commands, and upconverter statements (optional) on the Cisco CMTS as the first step in N+1 configuration.
<a href="#">Enabling HCCP Protect Interfaces for N+1 Redundancy</a>	(Required for interface-level configuration) Enables HCCP Protect interfaces, making ready for N+1 switchover from HCCP Working interfaces in the case of their failure.
<a href="#">Configuring Global HCCP 4+1 and 7+1 Line Card Redundancy on the Cisco uBR10012 Router</a>	(Required for quick global configuration) Configures HCCP 4+1 Redundancy for the Cisco uBR10012 router and either one or two Cisco RF Switches in 4+1 or 7+1 redundancy. Supported in Cisco IOS Release 12.3(17a)BC.
<a href="#">Enabling the HCCP Switchover Enhancements Feature</a>	(Automatically supported) Implements performance improvements for traffic recovery during line card switchover under certain scalability limits.
<a href="#">Maintaining Online Cable Modem Service When Removing HCCP Configuration from Working HCCP Interfaces</a>	(Optional for Interface-level Configuration) Prevents cable modems from going offline during removal of HCCP configuration from Working interfaces.

## Preconfiguring HCCP Protect Interfaces for N+1 Redundancy

There are three specific HCCP functions that do not synchronize between Working and Protect interfaces. Therefore, each HCCP interface should be configured in identical fashion for the following functions. These functions require manual configurations on HCCP Protect interfaces, as follows:

- 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)

These manual preconfigurations prevent HCCP Protect interfaces from inheriting unexpected or non-standard configurations from HCCP Working interfaces during switchover. Each of these three preconfigurations must be the same for all members of each HCCP group.

To define downstream modulation, interleave depth and downstream annex mode on your HCCP Protect interfaces, perform these steps at the Cisco IOS command-line interface (router console).

### SUMMARY STEPS

1. **enable**
2. **config terminal**
3. **interface cableslot/subslot/port**
4. **cable downstream modulation { 64qam | 256qam }**
5. **cable downstream interleave-depth { 8 | 16 | 32 | 64 | 128 }**
6. **cable downstream annex { A | B }**
7. **Ctrl-Z**
8. **write memory**

### DETAILED STEPS

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

Step 3	<pre>interface cableslot/subslot/port</pre> <p><b>Example:</b> Router# interface cable8/1/0 </p>	<p>Enters interface configuration mode.</p> <p><b>Note</b> Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the <i>Cisco Broadband Cable Command Reference Guide</i> for complete command information.</p>
Step 4	<pre>cable downstream modulation {64qam   256qam}</pre> <p><b>Example:</b> Router(config-if)# cable downstream modulation 256qam </p>	<p>Sets the modulation format for a downstream port on a cable interface line card. The default setting is <b>64qam</b>.</p> <ul style="list-style-type: none"> <li>• <b>64qam</b>—Modulation rate is 6 bits per downstream symbol.</li> <li>• <b>256qam</b>—Modulation rate is 8 bits per downstream symbol.</li> </ul>
Step 5	<pre>cable downstream interleave-depth {8   16   32   64   128}</pre> <p><b>Example:</b> Router(config-if)# cable downstream interleave-depth 128 </p>	<p>Sets the downstream interleave depth. A higher interleave depth provides more protection from bursts of noise on the HFC network by interleaving downstream symbols. The default setting is <b>32</b>.</p> <ul style="list-style-type: none"> <li>• <b>{8   16   32   64   128}</b>—Indicates the downstream interleave depth in amount of symbols.</li> </ul>
Step 6	<pre>cable downstream annex { A   B }</pre> <p><b>Example:</b> Router(config-if)# cable downstream annex a </p>	<p>Sets the Motion Picture Experts Group (MPEG) framing format for a downstream port on a cable interface line card to either Annex A (Europe) or Annex B (North America). The default setting for Annex mode varies according to the cable interface line card or BPE in use. Refer to the corresponding configuration feature module for your specific modules.</p> <ul style="list-style-type: none"> <li>• <b>A</b>—Annex A. The downstream uses the EuroDOCSIS J.112 standard.</li> <li>• <b>B</b>—Annex B. The DOCSIS-compliant cable plants that support North American channel plans use ITU J.83 Annex B downstream radio frequency.</li> </ul>
Step 7	<pre>Ctrl-Z</pre> <p><b>Example:</b> Router(config-if)# Ctrl^Z </p>	<p>When you have included all of the configuration commands to complete the configuration, enter <b>^Z</b> (press the Control key while you press Z) to exit configuration mode.</p>
Step 8	<pre>write memory</pre> <p><b>Example:</b> Router# write mem [OK] Router# </p>	<p>Writes the new configuration to nonvolatile random access memory (NVRAM).</p> <p>The system displays an OK message when the configuration has been stored.</p>

For additional information about the commands in this section, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## Operating DHCP with the Cisco RF Switch

The latest Cisco IOS software release in support of the Cisco RF Switch includes full support for a DHCP client. DHCP operation is enabled by default, unless the user has set a static IP address defined at the command-line interface (CLI). Commands have been added/enhanced to support DHCP operation.

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

- **set ip address dhcp**
- **set ip address** *ip-address subnet-mask*
- **no set ip address** (to set the default, with DHCP now the default)



### Note

The RF Switch Firmware no longer assumes a static IP address of 10.0.0.1 as in versions prior to 3.00.

If enabled, the Cisco RF Switch installs the DHCP client and attempts to locate a DHCP server to request a lease. By default, the client requests a lease time of 0xffffffff (infinite lease), but this can be changed using the **set dhcp lease** *leasetime* command in User mode at the `rfswitch>` prompt, where *leasetime* is seconds. Because the actual lease time is granted from the server, this command is primarily used for debugging and testing purposes, and should not be required for normal operation.

When a server is located, the client requests settings for IP address and subnet mask, a gateway address, and the location of a TFTP server. The gateway address is taken from Option 3 (Router Option). The TFTP server address can be specified in a number of ways. The client checks the next-server option (*siaddr*), Option 66 (TFTP server name) and Option 150 (TFTP server address). If all three of the above are absent, the TFTP server address defaults to the DHCP server address. If the server grants a lease, the DHCP client records the offered lease time for renewal, and continues with the boot process, installing the other network applications (Telnet and SNMP), and the CLI.

When a server is not located within 20-30 seconds, the DHCP client is suspended and the CLI runs. The DHCP client will run in the background attempting to contact a server approximately every five seconds until a server is located, a static IP is assigned via the CLI, or the system is rebooted.

The CLI allows the user to override any of the network settings that may be received via the server, and assign static values for these settings. All of the “SET xxx” parameters are stored in `nvmem`, and are used across reboots. Because the current network settings now may come from either DHCP or the CLI, a few changes/new commands have been implemented. First, the existing SHOW CONFIG command has been changed to show the settings of all the `nvmem` parameters, which are not necessarily the ones in effect at the time.

To obtain the current network parameters in use, the new command SHOW IP has been added. In addition to the network settings, this command also shows the current IP mode (static versus DHCP), the status of the DHCP client, and the status of the Telnet and SNMP applications (which are only started if a valid IP exists).

An additional command, SHOW DHCP, has been added for informational purposes. This command shows the values received from the DHCP server, as well as the status of the lease time. The time values shown are in the format HH:MM:SS, and are relative to the current system time, which is also displayed.

Assignment of static values for any of the definable network parameters should go into effect immediately, and override the current setting without further action. This allows some of the parameters to remain dynamic, while fixing others. For example, DHCP could be used to obtain the IP address, while retaining the setting for the TFTP server set via the CLI. The one exception to this is when going from using a static IP to DHCP. Since the DHCP client is only installed at boot-up as required, transitioning from a static IP to DHCP requires the system to be rebooted for DHCP to take effect.

## Configuring HCCP Groups for Legacy N+1 Line Card Redundancy



### Note

This procedure is not applicable for global N+1 line card redundancy, which is available in Cisco IOS Release 12.3(13a)BC and later.

In releases prior to Cisco IOS Release 12.3(13a)BC, once the Cisco RF Switch has been configured and enabled to support N+1 Redundancy, you must configure Cisco IOS and Cisco RF Switch Firmware to support the Cisco RF Switch. This procedure defines HCCP Working and Protect interfaces, Cisco RF Switch commands, and upconverter statements (optional) on the Cisco CMTS as the first step in N+1 configuration.



### Note

When the Cisco CMTS CLI descriptions include the term *channel switch*, this term refers to the Cisco RF Switch.



### Note

When configuring Hot-Standby Connection-to-Connection Protocol (HCCP) on the Cisco uBR10012 router, use the IP address from the local loopback interface as the Working interface IP address. Cisco strongly recommends 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.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *slot/subslot/port*
4. **hccp group working member**
5. **hccp group protect member ip-address**
6. **hccp group channel-switch member-id upconverter name wavecom-xx**  
*protect-upconverter-ip-address module (upconverter) working-ip-address its-module*
7. **hccp group channel-switch member-id channel-switch-name rswitch-group ip-address**  
*module-bitmap position*
8. **Ctrl-Z**
9. **write memory**

## DETAILED STEPS

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

Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# config t</p>	Enters global configuration mode.
Step 3	<pre>interface cable slot/subslot/port</pre> <p><b>Example:</b> Router# interface cable8/1/0</p>	<p>Enters interface configuration mode.</p> <p><b>Note</b> Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the <i>Cisco Broadband Cable Command Reference Guide</i> for complete command information.</p>
Step 4	<pre>hccp group working member-id</pre> <p><b>Example:</b> Router(config-if)# hccp 1 working 1</p>	<p>Designates a cable interface on a CMTS in the specified HCCP group to be a Working CMTS.</p> <p><b>Note</b> The <code>hccp group working member</code> command is to be used for Working line card interfaces only.</p> <ul style="list-style-type: none"> <li>• <i>group</i>—The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> <li>• <i>member-id</i>—The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> </ul>
Step 5	<pre>hccp group protect member-id ip-address</pre> <p><b>Example:</b> Router(config-if)# hccp 1 protect 2 10.10.10.1</p>	<p>Assigns the HCCP group number, defines the corresponding HCCP member, and defines the Working IP address of the interface used for HCCP communication.</p> <p><b>Note</b> The <code>hccp group protect member-id</code> command is to be used for Protect line card interfaces only.</p> <p><b>Note</b> The Working and Protect line cards are located on different chassis when using the Cisco uBR7246VXR router. Working and Protect line cards are located on the same Cisco uBR10012 router chassis. In the latter case, Cisco Systems recommends that you use the Loopback IP address in this configuration.</p>
Step 6	<pre>hccp group channel-switch member-id upconverter name wavecom-xx protect-upconverter-ip-address module (upconverter) working-ip-address its-module</pre> <p><b>Example:</b> Router(config-if)# hccp 1 channel-switch 2 uc wavecom-hd 10.97.1.21 2 10.97.1.21 14</p>	<p>Upconverter (optional). Configures the upconverter (UPx) topology so that the Vecima upconverter becomes part of the specified HCCP member in a particular HCCP group.</p> <p><b>Note</b> This procedure is not required when configuring N+1 Redundancy on the Cisco uBR10012 router with the Cisco UBR10-MC 5X20U or -S BPE.</p> <p><b>Note</b> Steps 6 and 7 of this procedure are required for both the Working and the Protect interfaces.</p>
Step 7	<pre>hccp group channel-switch member-id channel-switch-name rfswitch-group ip-address module-bitmap position</pre> <p><b>Example:</b> Router(config-if)# hccp 1 channel-switch 2 rfswitch-name rfswitch-group 10.97.1.20 AA200000 2</p>	<p>Configures the Cisco CMTS so that the specified Cisco RF Switch becomes part of the specified HCCP member in a particular HCCP group.</p> <ul style="list-style-type: none"> <li>• <i>ip address</i> — The IP address of the Cisco RF Switch.</li> <li>• <i>rf-switch-name</i> — Specifies the name of the Cisco RF Switch, and must also include the hexadecimal module-bitmap argument. Refer to the “<a href="#">Creating Cisco RF Switch Module Bitmaps</a>” section on <a href="#">page 12-23</a> for instructions on creating an appropriate hexadecimal module bitmap.</li> <li>• <i>position</i> — This value specifies the slot/header of the Cisco RF Switch—there are eight on the Cisco uBR10012.</li> </ul> <p><b>Note</b> Steps 6 and 7 of this procedure are required for both the Working and the Protect interfaces.</p>

<b>Step 8</b>  <b>Example:</b> Router(config-if)# <b>Ctrl^Z</b>	<b>Ctrl-Z</b>	Exits interface configuration mode, and returns you to global configuration mode.
<b>Step 9</b>  <b>Example:</b> Router# copy running-config startup-config or Router# write memory	<b>write memory</b>	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.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## Enabling HCCP Protect Interfaces for N+1 Redundancy

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.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cableslot/subslot/port**
4. **no shutdown**
5. Repeat steps 3-4.
6. **Ctrl-Z**
7. **write memory**

### DETAILED STEPS

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

<b>Step 3</b>	<code>interface cableslot/subslot/port</code>  <b>Example:</b> Router# interface cable8/1/0 Router(config-if)#	Enters interface configuration mode for the desired interface. Select the HCCP Protect interface.  <b>Note</b> Syntax for Interface Configuration mode differs between the Cisco uBR1012 and the Cisco uBR7246VXR routers. Refer to the <i>Cisco Broadband Cable Command Reference Guide</i> for complete command information.
<b>Step 4</b>	<code>no shutdown</code>  <b>Example:</b> Router(config-if)# no shut	Enables the HCCP Protect interface.
<b>Step 5</b>	Repeat	Repeat steps 3-4 for every HCCP Protect interface.
<b>Step 6</b>	<code>ctrl-z</code>  <b>Example:</b> Router(config-if)# <b>Ctrl^Z</b>	Exits interface configuration mode, and returns you to global configuration mode.
<b>Step 7</b>	<code>write memory</code>  <b>Example:</b> Router# write mem	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

## Configuring Global HCCP 4+1 and 7+1 Line Card Redundancy on the Cisco uBR10012 Router

Cisco IOS Release 12.3(17a)BC adds support for HCCP 4+1 line card redundancy to the existing 7+1 redundancy (supported in Cisco IOS Release 12.3(13a)BC) on the Cisco uBR10012 router. In this configuration, one Cisco router is configured with either one or two Cisco RF Switches using HCCP. Global configuration of the router in Cisco IOS Release 12.3(17a)BC makes this High Availability configuration quick and straightforward to implement.

With either redundancy scheme, perform these steps on the Cisco uBR10012 router. These are global configurations that govern all interfaces and line cards in the scheme, and override any previous HCCP configurations from releases prior to Cisco IOS Release 12.3(17a)BC.

Either form of N+1 Redundancy supports the Cisco uBR-MC5X20U/D or the Cisco uBR-MC5X20S broadband processing engines (BPEs) on the Cisco uBR10012 router, in any combination.



### Note

N+1 Redundancy supports two types of BPEs in the Cisco uBR10012 router. Any combination of the Cisco uBR-MC5X20U BPE and the Cisco uBR-MC5X20S BPE is supported.

Beginning in Cisco IOS Release 12.3(21)BC, 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** keyword option, you can preload upstream connectors on an HCCP protected interface to emulate the most common line card connector assignments.

**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 RF Switches 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.

**Prerequisites**

- Cisco IOS Release 12.3(17a)BC must be installed on each router for global 4+1 redundancy support. Global 7+1 redundancy is supported beginning in Cisco IOS Release 12.3(13a)BC.
- 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:

```
ip dhcp pool rfs witch-pool
  network
  <all other stuff>
!
ip dhcp pool rfs w-1 ! DHCP MAC->IP mapping for RF-switch # 1
host a.b.c.d <mask>
  client-id 01aa.bb cc.ddee.ff
!
ip dhcp pool rfs w-2 ! DHCP MAC->IP mapping for RF-switch # 2
host b.c.d.f <mask>
  client-id 01aa.bb cc.ddee.ff
```

- 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. For more information about the **rf-switch name** command, see the [“Using Optional RF Switch Settings with Global N+1 Redundancy”](#) section on page 12-30.

**Restrictions**

In Cisco IOS Release 12.3(17a)BC, when global 4+1 Redundancy is configured, earlier HCCP configuration commands are not supported. This document supports several such configuration commands, applicable to releases prior to Cisco IOS Release 12.3(17a)BC. This procedure describes global configuration of N+1 Redundancy on the Cisco CMTS.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip host rf-sw1 ip\_addr**
4. **ip host rf-sw2 ip\_addr**
5. **redundancy**

6. **linecard-group 1 cable**
7. **member subslot *slot/card* working**
8. **member subslot *slot/card* protect [config *slot/card*]**
9. **Ctrl-Z**
10. **write memory**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# config t Router(config)#	Enters global configuration mode.
Step 3	<b>ip host rf-sw1 ip_addr</b>  <b>Example:</b> 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	<b>ip host rf-sw2 ip_addr</b>  <b>Example:</b> 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.
Step 5	<b>redundancy</b>  <b>Example:</b> 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	<b>linecard-group 1 cable</b>  <b>Example:</b> 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	<b>member subslot <i>slot/card</i> working</b>  <b>Example:</b> 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.

<b>Step 8</b>	<pre>member subslot slot/card protect</pre> <p><b>Example:</b> Router(config-red)# member subslot 8/1 protect</p> <p>or</p> <pre>member subslot slot/card protect config slot/card</pre> <p><b>Example:</b> Router(config-red)# member subslot 8/1 protect config 8/0</p>	<p>Configures all interfaces on the specified line card to function as HCCP Protect interfaces in the redundancy scheme.</p> <p>or</p> <p>For faster switchover results, configures the protect interface for the most appropriate working interface configuration.</p>
<b>Step 9</b>	<pre>Ctrl-Z</pre> <p><b>Example:</b> Router(config-red)# Ctrl^Z Router#</p>	<p>Exits global and redundancy configuration modes and returns to Privileged EXEC mode.</p>
<b>Step 10</b>	<pre>write memory</pre> <p><b>Example:</b> Router# copy running-config startup-config</p> <p>or</p> <pre>Router# write memory</pre>	<p>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.</p>

## Examples

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

```
Router# show running config
...
redundancy
  main-cpu
    auto-sync standard
  linecard-group 1 cable
    rf-switch name 1 rf-switch-1
    rf-switch name 2 rf-switch-2
  rf-switch snmp-community private123
    member subslot 6/1 working
    member subslot 5/1 protect
  member subslot 8/0 working
...
```

The following example illustrates information supported by the **show redundancy linecard all** command in privileged EXEC mode. This redundancy configuration supports two Cisco 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 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca7/0/0 Protect 1 61 rfs-1 10.4.4.1 6 0xFFFFFFFF
Ca7/0/1 Protect 2 80 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca7/0/1 Protect 2 61 rfs-1 10.4.4.1 6 0xFFFFFFFF
Ca7/0/2 Protect 3 80 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca7/0/2 Protect 3 80 rfs-2 10.4.4.2 1 0xFFFFFFFF
Ca7/0/2 Protect 3 61 rfs-1 10.4.4.1 6 0xFFFFFFFF
Ca7/0/2 Protect 3 61 rfs-2 10.4.4.2 6 0xFFFFFFFF
Ca7/0/3 Protect 4 80 rfs-2 10.4.4.2 1 0xFFFFFFFF
Ca7/0/3 Protect 4 61 rfs-2 10.4.4.2 6 0xFFFFFFFF
Ca7/0/4 Protect 5 80 rfs-2 10.4.4.2 1 0xFFFFFFFF
Ca7/0/4 Protect 5 61 rfs-2 10.4.4.2 6 0xFFFFFFFF
Ca8/0/0 Working 1 80 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca8/0/1 Working 2 80 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca8/0/2 Working 3 80 rfs-1 10.4.4.1 1 0xFFFFFFFF
Ca8/0/2 Working 3 80 rfs-2 10.4.4.2 1 0xFFFFFFFF
Ca8/0/3 Working 4 80 rfs-2 10.4.4.2 1 0xFFFFFFFF
Ca8/0/4 Working 5 80 rfs-2 10.4.4.2 1 0xFFFFFFFF

```

In addition to the **show redundancy linecard all** command illustrated above, you can use the following two commands to display additional redundancy information for a specified slot. These examples illustrate slot-level syntax for the **show redundancy** command:

- **show redundancy linecard all | inc Ca8/0/**
- **show redundancy linecard all | inc 81**

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 RF Switches in either 4+1 or 7+1 Redundancy.

**Table 3 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

## What to Do Next

If not previously complete, refer to these additional sections to complete the N+1 Redundancy scheme:

- [“Configuring the Cisco RF Switch for N+1 Redundancy” section on page 12-20](#)
- [“Creating Cisco RF Switch Module Bitmaps” section on page 12-23](#)
- [“Configuring the Cisco uBR10012 Universal Broadband Router for Global N+1 Line Card Redundancy” section on page 12-27](#)
- [“Using Optional RF Switch Settings with Global N+1 Redundancy” section on page 12-30](#)

If this was the final required configuration of your redundancy scheme, refer to these additional sections:

- [“Switchover Testing Tasks for N+1 Redundancy”](#) section on page 12-48
- [“Configuration Examples for Cisco N+1 Redundancy”](#) section on page 12-57
- [“Additional References”](#) section on page 12-91

## Enabling the HCCP Switchover Enhancements Feature

Beginning in Cisco IOS Release 12.3(21)BC, the Cisco uBR10012 universal broadband router supports the HCCP Switchover Enhancements feature that 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.

## Virtual Interface Bundling

Virtual interface bundling configuration is required to enable the HCCP Switchover Enhancements feature. When you upgrade to Cisco IOS Release 12.3(21)BC, 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 more information about configuring virtual interface bundling, see the [“Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS”](#) chapter in this guide.

### 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
```

## Prerequisites for Enabling the HCCP Switchover Enhancements Feature

- Requires Cisco IOS Release 12.3(21)BC and later.
- Requires the PRE2 in the Cisco uBR10012 router.
- Supported with the Cisco UBR10-MC 5X20S, Cisco UBR10-MC 5X20U, and Cisco uBR10-MC5X20H line cards.
- 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.

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

The following HCCP restrictions apply to HCCP N+1 Redundancy on either the Cisco uBR10012 or Cisco uBR7246VXR router:

- Before removing HCCP configuration from an active Working interface, either shut down the protect or lockout switchover functions using the **hccp group lock member-id** 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 (revertback) 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), Cisco Systems recommends using one of the following three procedures as a best practice:

- [Shutting Down HCCP Protect Interfaces](#)  
or  
[Locking out HCCP Interface Switchover](#)
- [Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces](#)

## Shutting Down HCCP Protect Interfaces

### SUMMARY STEPS

1. **enable**
2. **config t**
3. **interface** *slot/subslot/port*
4. **shutdown**
5. Repeat the above steps 3 and 4 as required to shutdown all Protect HCCP interfaces.

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# config t	Enters global configuration mode.
Step 3	<b>interface cable</b> <i>slot/subslot/port</i>  <b>Example:</b> Router# interface cable8/1/0	Enters interface configuration mode.
Step 4	<b>shutdown</b>  <b>Example:</b> 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

### SUMMARY STEPS

1. **enable**
2. **hccp group lockout** *member-id*

3. Repeat above steps as required to lock out all Working HCCP interface switchover events.
4. **hccp group unlockout member**
5. **Ctrl-Z**
6. **write memory**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>hccp group lockout member-id</b>  <b>Example:</b> Router# hccp 1 lockout 1	To prevent a Working HCCP interface from automatically switching to a Protect interface in the same group, use the <b>hccp lockout</b> command in privileged EXEC mode. This command disables HCCP for the specified member of the specified group. <ul style="list-style-type: none"> <li>• <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> <li>• <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> </ul> <p><b>Note</b> 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 5X20U or -S.</p> <p><b>Note</b> With the Cisco uBR7246VXR CMTS, HCCP interface tracking occurs across all interfaces that share the same cable interface IP bundle. Therefore, if any one HCCP interface switches over, all interfaces in that bundle will switch over together, regardless of whether they are locked out or not.</p>
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	<b>hccp group unlockout member</b>  <b>Example:</b> Router# hccp 1 unlockout 1	Disables the HCCP lockout feature when desired (re-enabling N+1 Redundancy on the Working interface). <ul style="list-style-type: none"> <li>• <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> <li>• <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> </ul>

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## Removing HCCP Configuration from HCCP Working or HCCP Protect Interfaces

### SUMMARY STEPS

1. **enable**
2. **config t**
3. **interface** *slot/subslot/port*
4. **no hccp group** {**working** | **protect**} *member*
5. Repeat the above steps as required to remove all Protect HCCP interface configurations.

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# config t	Enters global configuration mode.
Step 3	<b>interface cable</b> <i>slot/subslot/port</i>  <b>Example:</b> Router# interface cable8/1/0	Enters interface configuration mode.
Step 4	<b>no hccp group</b> { <b>working</b>   <b>protect</b> } <i>member-id</i>  <b>Example:</b> Router(config-if)# no hccp 1 protect 1	Turns off HCCP, and removes the specified HCCP configuration from the specified interface.  <ul style="list-style-type: none"> <li>• <i>group</i> — The group number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> <li>• <i>member-id</i> — The member number for the specified interface. Valid values are any number from 1 to 255, inclusive.</li> </ul>
Step 5	Repeat.	Repeat the above steps as required to remove HCCP configuration from all desired HCCP Protect interfaces.

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## 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 or Cisco uBR7246VXR CMTS. 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, page 12-49](#)
- [Switchover Testing Procedures, page 12-53](#)

**Note**

To test route processor switchover functions on the Cisco uBR10012 router, refer to the document [Route Processor Redundancy Plus on the Cisco uBR10012 Universal Broadband Router](#) on Cisco.com.

## Pre-testing System Check Procedures

As a best practice, Cisco strongly recommends 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 Group Status on the Cisco CMTS, page 12-49](#)
- [Displaying HCCP Working and HCCP Protect Interface Status, page 12-51](#)
- [Displaying Cisco RF Switch Module Status on the Cisco RF Switch, page 12-52](#)

## Displaying HCCP Group Status on the Cisco CMTS

As a best practice, Cisco Systems recommends 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.

### SUMMARY STEPS

1. **enable**
2. **show hccp {group-member} channel-switch**
3. **show ip interface brief**

## DETAILED STEPS

Command	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>show hccp {group-member} channel-switch</code></p> <p><b>Example:</b> Router# show hccp channel-switch</p> <pre>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 . . .</pre> <p><b>Note</b> For a complete example of command output, refer to the <a href="#">“Example: Channel Switch Information from the Cisco uBR10012 Router”</a> section on page 12-71.</p>	<p>To display HCCP group status on the Cisco CMTS, including Cisco RF Switch information relevant to N+1 Redundancy behavior, use the <b>show hccp channel-switch</b> command in privileged EXEC mode. This command displays status for all channel switches belonging to the specified HCCP group and HCCP member.</p> <ul style="list-style-type: none"> <li><i>group-member</i>—Optionally specifies a specific HCCP group member. If you do not specify an HCCP group member, the CMTS displays status for all channel switches known to the router.</li> </ul> <p>Potential causes for a fault or an unknown state while using the <b>show hccp channel-switch</b> command are:</p> <ul style="list-style-type: none"> <li>SNMP misconfiguration on the Cisco RF Switch or CMTS</li> <li>misconfigured access lists</li> </ul> <p><b>Note</b> This command does not display HCCP interfaces that have been shut down (disabled).</p>
<p><b>Step 3</b> <code>show ip interface brief</code></p> <p><b>Example:</b> Router# show ip interface brief</p> <pre>Interface  IP-Address  OK? Method Status Protocol Ethernet0/0/0 127.0.0.254 YES unset up up FastEthernet0/0/0 1.8.22.13 YES NVRAM up up SRP2/0/0 200.1.1.10 YES NVRAM up up SRP4/0/0 202.1.1.10 YES NVRAM up up Cable5/0/0 130.1.1.1 YES NVRAM up up Cable5/0/1 unassigned YES NVRAM up up Loopback0 203.1.1.10 YES NVRAM up up</pre>	<p>Displays a summary of all interfaces, including the DPT WAN card.</p>

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## Displaying HCCP Working and HCCP Protect Interface Status

As a best practice, Cisco Systems recommends that you perform this test prior to performing any manual switchovers. This status check confirms the enabling of HCCP interfaces, and the direction of pending manual switchover tests.

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 RF Switch prompt.

### SUMMARY STEPS

1. **show hccp brief**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>show hccp brief</b>  <b>Example:</b> Router# <b>show hccp brief</b>  <pre> Interface Config  Grp Mbr Status Ca5/0/0    Protect  1  3  standby Ca7/0/0    Working  1  3  active           </pre>	To confirm that HCCP Working or Protect interfaces are configured and enabled, use the <b>show hccp brief</b> command in user EXEC or privileged EXEC mode.  <b>Note</b> This command does not display HCCP interfaces that have been shut down (disabled).  For complete information about the <b>show hccp</b> command, refer to the <i>Cisco Broadband Cable Command Reference Guide</i> on Cisco.com:  <a href="http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html">http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html</a>

### Examples

In Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases, the **brief** option also shows the amount of time left before the next re-synchronization and the time left before a restore:

```

Router# show hccp brief

      Interface Config  Grp Mbr Status          WaitToResync  WaitToRestore
      Ca5/0/0    Protect  1  3  standby          00:01:50.892
      Ca7/0/0    Working  1  3  active          00:00:50.892  00:01:50.892

Router#
  
```

## Displaying Cisco RF Switch Module Status on the Cisco RF Switch

As a best practice, Cisco Systems recommends 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 RF Switch itself.

To display current module status for one or more modules on the Cisco RF Switch, use the **show module all** command at Cisco RF Switch prompt.

### SUMMARY STEPS

1. **show module {*module* | *group-name* | all}**

### DETAILED STEPS

	Command	Purpose
Step 1	<pre>show module {<i>module</i>   <i>group-name</i>   all}</pre> <p><b>Example:</b>  <pre>rfswitch&gt; show module all</pre></p> <pre>Module Presence Admin Fault 1         online    0      ok 2         online    0      ok 3         online    0      ok 4         online    0      ok 5         online    0      ok 6         online    0      ok 7         online    0      ok 8         online    0      ok 9         online    0      ok 10        online    0      ok 11        online    0      ok 12        online    0      ok 13        online    0      ok</pre>	<p>This command displays current status with these options:</p> <ul style="list-style-type: none"> <li>• a single, specified module</li> <li>• a group of modules</li> <li>• all modules on the Cisco RF Switch</li> </ul> <p>The statistical output resulting from the <b>show module</b> command includes module administration state, module operation state, and module error state, if any.</p> <p>For an example of statistical output from the <b>show module</b> command, refer to the “<a href="#">Example: Cisco 3x10 RF Switch Modules in 8+1 Mode</a>” section on page 12-58.</p> <p>The Administrative State field (<code>Admin</code>) indicates the following potential states:</p> <ul style="list-style-type: none"> <li>• 0 — Indicates normal Working state.</li> <li>• 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 <code>Admin</code> 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 <code>Admin</code> state corresponds with the actual wiring on the Cisco RF Switch.</li> <li>• 9 — Indicates fault for the specified module.</li> </ul>

For additional information about the command in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## 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, page 12-53](#)
- [Testing HCCP Groups with Manual Switchover, page 12-55](#)
- [Using the show cable modem Command After a Manual Switchover, page 12-55](#)

### Testing Cisco RF Switch Relays with Manual Switchover

Cisco Systems recommends 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.

#### SUMMARY STEPS

1. **telnet**
2. **test module or switch** *group-name 1*
3. **switch** *group-name 0*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>telnet ip-address /noecho</pre> <p><b>Example:</b> Router# telnet 172.16.10.3 /noecho</p>	<p>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.</p> <p>If a Telnet password is set on the Cisco RF Switch, type <b>password string</b>, where <i>string</i> is the previously-defined password set on the RF Switch. The Telnet password is set using the separate <b>set password string</b> command in Cisco RF Switch User mode.</p> <p><b>Note</b> 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.</p> <p>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 <code>/noecho</code> option (as shown at left).</p> <p>Common Telnet disconnect methods are as follows:</p> <ul style="list-style-type: none"> <li>• Press <b>Ctrl+Break</b>.</li> <li>• Press <b>Ctrl+]</b>.</li> <li>• Type <b>quit</b> or <b>send break</b>.</li> </ul> <p>Another Telnet disconnect method is as follows:</p> <ol style="list-style-type: none"> <li>a. Press <b>Ctrl+Shift 6 6 x</b>.</li> <li>b. Type <b>disc 1</b> from the router CLI.</li> </ol> <p>For additional Telnet break sequences, refer to the document <a href="#">Standard Break Key Sequence Combinations During Password Recovery</a> on Cisco.com.</p>
Step 2	<pre>test module</pre> <p><b>Example:</b> rfswitch&gt; test module or <b>switch group-name x</b></p> <p><b>Example:</b> rfswitch&gt; switch 13 1</p>	<p>The <b>test module</b> command tests all the relays at once, and then returns to the normal Working mode.</p> <p> <b>Caution</b> Do not use the <b>test module</b> command while in the Protect mode.</p> <p>Alternately, you can test an entire bitmap with <b>switch group-name x</b>, where <i>x</i> is the RF Switch header number. For example, the <b>switch 13 1</b> tests port G on slot 1 of the Cisco RF Switch.</p>
Step 3	<pre>switch group-name 0</pre> <p><b>Example:</b> rfswitch&gt; switch 13 0</p>	<p>Use the command <b>switch group name 0</b> (or <code>idle</code>) to disable the relays, and to return to normal Working mode.</p>

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## 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	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><code>hccp group switch member</code></p> <p><b>Example:</b> Router# hccp 1 switch 1</p>	<p>Manually switches a Working CMTS with its Protect CMTS peer (or vice versa).</p>

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## 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.

### SUMMARY STEPS

1. `enable`
2. `show cable modem ip-address`
3. `ping ip-address`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>show cable modem ip-address</b></p> <p><b>Example:</b> Router# show cable modem 172.16.10.3</p> <pre>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</pre>	<p>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.</p>
Step 3	<p><b>ping ip-address</b></p> <p><b>Example:</b> Router# ping 172.16.10.3</p>	<p>Forces IP traffic by sending an ICMP ECHO packet.</p>

For additional information about the commands in this section, refer to the [Cisco Broadband Cable Command Reference Guide](#) on Cisco.com.

## Background Path Testing for HCCP N+1 Redundancy on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(13a)BC introduces automatic running of the **show hccp channel switch** command to do background path testing, where the Cisco uBR10012 router regularly communicates with each module in the Cisco RF switch to obtain status information. Beginning in Cisco IOS Release 12.3(13a)BC, the router automatically polls the RF switch every 10 seconds, and stores the SNMP response information in a cache. When you manually run the **show hccp channel switch** command, the router reports the information stored in this cache.

The switch can require from two to five seconds before reporting an SNMP response. If SNMP errors are detected in response to this command, the switch may require a significantly longer timeout period.

For additional information about HCCP N+1 Redundancy on the Cisco CMTS, refer to these documents on Cisco.com:

- Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

# 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.

**Table 4 Summary Table of N+1 Configuration Examples—Cisco IOS 12.2(15)BC2a, Firmware 3.50**

Example	Cisco RF Switch <sup>1</sup>	N+1 Mode	Cisco Router Chassis <sup>2</sup>	Cisco Cable Interface Line Cards	Upconverters
<b>Cisco RF Switch Module Examples</b>					
<a href="#">Example: Cisco 3x10 RF Switch Modules in 8+1 Mode</a>	3x10 RF	8+1 <sup>3</sup>	uBR10012	Not described	Not described
<a href="#">Example: Cisco 3x10 RF Switch Modules in 4+1 Mode</a>	3x10 RF	4+1	uBR7246VXR (five)	uBR10K-MC28C	Vecima HD4040 (three)
<b>Cisco uBR10012 Chassis Configuration Examples</b>					
<a href="#">Examples: Cisco 3x10 RF Switch with Cisco uBR10012 Chassis</a>	3x10 RF	8+1 <sup>3</sup>	uBR10012	UBR10-MC 5X20U or -S (five)	Not described
<a href="#">Example: Channel Switch Information from the Cisco uBR10012 Router</a>	3x10 RF	8+1 <sup>3</sup>	uBR10012	Not described	Not described
<a href="#">Example: Cisco 3x10 RF Switch and Cisco uBR10012 Chassis</a>	3x10 RF	8+1 <sup>3</sup>	uBR10012	UBR10-LCP2-MC28C (eight)	Not described
<a href="#">Example: Cisco 3x10 RF Switches and Cisco uBR10012 Chassis</a>	3x10 RF (two)	8+1 <sup>3</sup>	uBR10012	UBR10-MC 5X20U or -S	Not described
<b>Cisco uBR7246VXR Chassis Configuration Examples</b>					
<a href="#">Example: Cisco 3x10 RF Switches and uBR7246VXR Chassis</a>	3x10 RF (two)	4+1	uBR7246VXR (five)	uBR-MC28U/X (20)	Not described

1. Assume one Cisco RF Switch per example unless more are cited.
2. Assume one Cisco router chassis per example unless more are cited.
3. The term of "8+1 Redundancy" is often referred to as "7+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 8+1 Mode

The following is sample output for the **show module all** command from a Cisco RF Switch that has been configured for 8+1 Redundancy:

```
rfswitch> show module all

Module  Presence  Admin  Fault
      1  online      0      ok
      2  online      0      ok
      3  online      0      ok
      4  online      0      ok
      5  online      0      ok
      6  online      0      ok
      7  online      0      ok
      8  online      0      ok
      9  online      0      ok
     10  online      0      ok
     11  online      0      ok
     12  online      0      ok
     13  online      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 for the **show config** command from a Cisco 3x10 RF Switch configured in 8+1 Redundancy mode:

```
rfswitch> show config

IP addr: 172.18.73.3
Subnet mask: 255.255.255.0
MAC addr: 00-03-8F-01-04-13

Gateway IP: 172.18.73.1
TFTP host IP: 172.18.73.2
TELNET inactivity timeout: 600 secs
Password: (none)

SNMP Community: private
SNMP Traps: Enabled
SNMP Trap Interval: 300 sec(s)
SNMP Trap Hosts: 1
    172.18.73.165

Card Protect Mode: 8+1
Protect Mode Reset: Disabled
Chassis Config: 13 cards
Watchdog Timeout: 20 sec(s)

Group definitions: 3
ALL          0xffffffff
GRP1         0xaa200000
GRP2         0x55100000
```



### 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.

## Example: Cisco 3x10 RF Switch Modules in 4+1 Mode

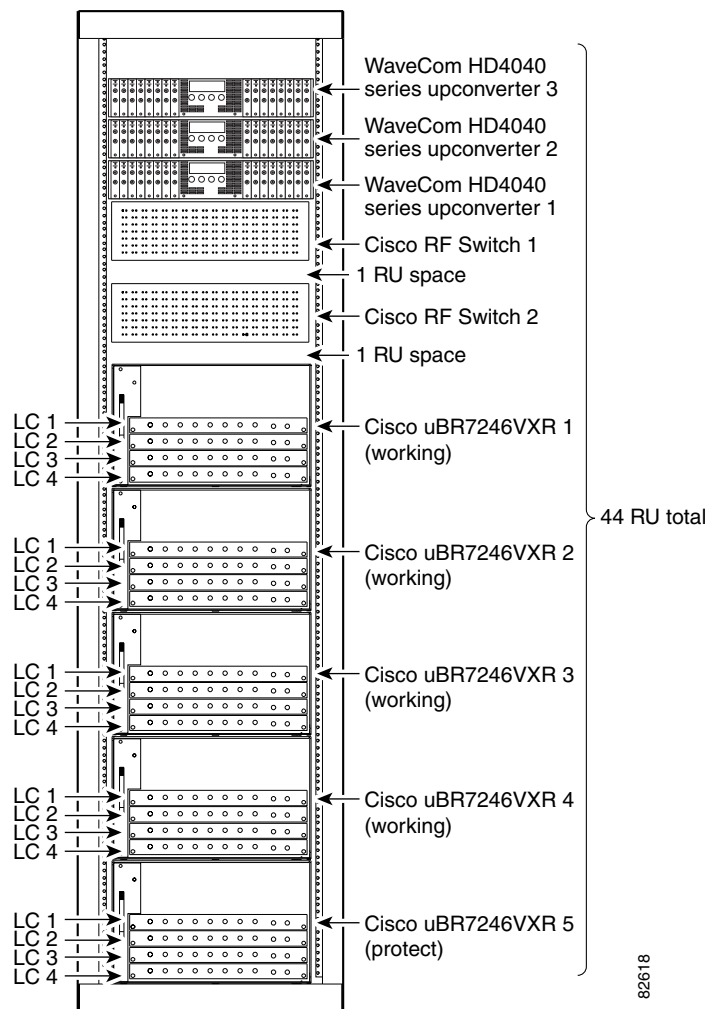
The following example configuration illustrates N+1 Redundancy using the following Cisco

- Two Cisco RF Switches (3x10) in 4+1 mode
- Five Cisco uBR7246VXR routers
- 20 Cisco uBR10K-MC28C cable interface line cards
- Three Vecima HD4040 chassis containing 40 modules.

The physical layout is shown in Figure 8-4. A cabling document can be found at:

<http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/installation/guide/310HIG.pdf>

**Figure 5** 4+1 Redundancy Using Cisco MC28C Line Cards & Two Cisco RF Switches



The following physical stacking is assumed:

- IP address assignments start with 192.168.1.2 at the top, and continuing downward in sequence.
- The first Cisco RF Switch is interpreted by the Cisco CMTS to be two switches, as it is in the 4+1 mode (a & b), where a is slots 1-4 and b is slots 5-8.
- The second Cisco RF Switch is also interpreted by the Cisco CMTS to be two switches (a & b).

## N+1 Configuration Example on the Working Cisco uBR7246VXR Router

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "WorkingVXR1"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxabcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
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
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.7 255.255.255.0
no keepalive
speed auto
full-duplex
!
! This interface is used for HCCP traffic.
!
interface FastEthernet0/1
ip address 192.168.2.5 255.255.255.0
keepalive 1
!
! This is set to 1 second so if the cable was disconnected, this interface will fail over
within 3 seconds.
!
speed auto

```

```

full-duplex
!
interface Cable3/0
ip address 10.11.12.1 255.255.255.0 secondary
ip address 192.168.3.5 255.255.255.0
load-interval 30
keepalive 1
!
! The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
load-interval 30
cable downstream channel-id 0
cable bundle 1 master
!
! Interface bundling is supported as well as subinterfaces.
! Note: Interface bundles failover together.
!
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 453000000
!
! This is downstream frequency, which used to be informational only when using an external
UPx. This must be set when using the MC28U cards with internal UPxs or when doing N+1
with MC28C cards, so that the Protect UPx knows which frequency to use.
!
cable upstream 0 frequency 24000000
!
! If doing dense mode combining, the upstream frequencies will need to be different. If
no two upstream ports are shared, the same frequency can be used.
!
cable upstream 0 power-level 0
cable upstream 0 channel-width 3200000
cable upstream 0 minislots-size 2
cable upstream 0 data-backoff automatic
cable upstream 0 modulation-profile 3
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 the Working first group, member 1.
!
hccp 1 channel-switch 1 rfs1a rfs1-switch-group 192.168.1.5 44440400 1
!
! This is IP add of Switch and it's protecting member 1 in the left side of Switch slot 1.
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
hccp 1 track FastEthernet0/1
!
! Tracking is enabled for the egress port in case the WAN-backhaul is disrupted. In this
instance, this cable interface would fail over to the Protect.
!
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 & not wait the full
revert time.
!
interface Cable3/1
hccp 2 working 1
hccp 2 channel-switch 1 rfs1a rfs1-switch-group 192.168.1.5 11110100 1
!
! This is the IP address of the Cisco RF Switch and its protecting member 1 in the right
side of Switch slot 1.
!
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 reverttime 120

interface Cable4/0
hccp 3 working 1
hccp 3 channel-switch 1 rfs1b rfs1-switch-group 192.168.1.5 88880800 1
!
! This is the IP address of the Cisco RF Switch and its protecting member 1 in the left
side of Switch slot 5.

```

```

!
 hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
 hccp 3 reverttime 120
!
interface Cable 4/1
 hccp 4 working 1
 hccp 4 channel-switch 1 rfswlb rfs switch-group 192.168.1.5 22220200 1
!
! This is IP address of the Cisco RF Switch and its protecting member 1 in the right side
of Switch slot 5.
!
 hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
 hccp 4 reverttime 120

interface Cable5/0
 hccp 5 working 1
 hccp 5 channel-switch 1 rfs2a rfs switch-group 192.168.1.6 44440400 1
 hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
 hccp 5 reverttime 120
!
interface Cable 5/1
 hccp 6 working 1
 hccp 6 channel-switch 1 rfs2a rfs switch-group 192.168.1.6 11110100 1
 hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
 hccp 6 reverttime 120

interface Cable 6/0
 hccp 7 working 1
 hccp 7 channel-switch 1 rfs2b rfs switch-group 192.168.1.6 88880800 1
 hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
 hccp 7 reverttime 120

interface Cable 6/1
 hccp 8 working 1
 hccp 8 channel-switch 1 rfs2b rfs switch-group 192.168.1.6 22220200 1
 hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
 hccp 8 reverttime 120

router eigrp 2500
 network 10.11.12.0 0.0.0.255
 network 192.168.1.0
 network 192.168.3.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
 cdp run
!
snmp-server community private RW
!
! This does not affect the HCCP communications between the Upconverter, Switch, and
Router.
!
snmp-server community public RO
snmp-server enable traps tty
snmp-server manager
tftp-server disk0:
tftp-server disk1:
tftp-server disk1:rfs250-f1-1935030e
tftp-server disk1:rfs250-bf-1935022d
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```

## N+1 Configuration Example on the Protect Cisco uBR7246VXR Router

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "ProtectVXR"
!
boot system disk0:ubr7200-ik8s-mz.BC.28Sept02
enable secret 5 $1$d1We$809Be9s21TGJ3IAV1X4Pa.
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
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
!
ip subnet-zero
ip cef
!
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool MODEMS2
network 192.168.5.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.5.6
default-router 192.168.5.6
option 7 ip 192.168.5.6
option 4 ip 192.168.5.6
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC2
network 10.11.13.0 255.255.255.0
default-router 10.11.13.1
dns-server 171.68.226.120
lease 10 1 11
!
ip dhcp pool PC1
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.11 255.255.255.0
no keepalive

```

```

speed auto
full-duplex
no cdp enable
!
interface FastEthernet0/1
ip address 192.168.2.11 255.255.255.0
keepalive 1
speed auto
full-duplex
no cdp enable
!
interface Cable3/0
no ip address
!
! There is no need to set the IP address because it'll come from the Working card via SNMP.
!
no keepalive
! This is set by default to 10 seconds with the N+1 IOS code, but recommended to 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 same on the Protect and Working of the same group.
!
no shut
!
! The interface must be activated to start HCCP functionality. Do this last.
!
cable upstream 0 shutdown
!
! This will automatically become "no shutdown" (enabled) when a failover occurs.
!
hccp 1 protect 1 192.168.1.7
!
! This is the Protect for the first group. Remember to configure the Protect interface(s) last; after the Working interfaces are configured. This is the HCCP first group and it's protecting member 1 with member one's FE IP address.
!
hccp 1 channel-switch 1 rfswl1 rfs-switch-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it's protecting member 1, which has a bitmap of AA880800 in Switch slot 5.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) 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.
!
hccp 1 protect 2 192.168.1.8
!
! This is the HCCP first group and it's protecting member 2 with its IP address.
!
hccp 1 channel-switch 2 rfswl1 rfs-switch-group 192.168.1.5 44440400 2
hccp 1 channel-switch 2 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 9
hccp 1 protect 3 192.168.1.9
hccp 1 channel-switch 3 rfswl1 rfs-switch-group 192.168.1.5 44440400 3
hccp 1 channel-switch 3 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 1
hccp 1 protect 4 192.168.1.10
hccp 1 channel-switch 4 rfswl1 rfs-switch-group 192.168.1.5 44440400 4
hccp 1 channel-switch 4 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 9
hccp 1 timers 666 2000
hccp 1 timers <hellotime> <holdtime> This is for inter-chassis communication.
!
interface Cable3/1

hccp 2 protect 1 192.168.1.7
hccp 2 channel-switch 1 rfswl1 rfs-switch-group 192.168.1.5 11110100 1
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 protect 2 192.168.1.8
hccp 2 channel-switch 2 rfswl1 rfs-switch-group 192.168.1.5 11110100 2
hccp 2 channel-switch 2 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 10
hccp 2 protect 3 192.168.1.9
hccp 2 channel-switch 3 rfswl1 rfs-switch-group 192.168.1.5 11110100 3
hccp 2 channel-switch 3 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 2

```

```
hccp 2 protect 4 192.168.1.10
hccp 2 channel-switch 4 rfs1a rfs1a-group 192.168.1.5 11110100 4
hccp 2 channel-switch 4 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 10
hccp 2 timers 666 2000

interface Cable4/0

hccp 3 protect 1 192.168.1.7
hccp 3 channel-switch 1 rfs1b rfs1b-group 192.168.1.5 88880800 1
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 protect 2 192.168.1.8
hccp 3 channel-switch 2 rfs1b rfs1b-group 192.168.1.5 88880800 2
hccp 3 channel-switch 2 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 11
hccp 3 protect 3 192.168.1.9
hccp 3 channel-switch 3 rfs1b rfs1b-group 192.168.1.5 88880800 3
hccp 3 channel-switch 3 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 3
hccp 3 protect 4 192.168.1.10
hccp 3 channel-switch 4 rfs1b rfs1b-group 192.168.1.5 88880800 4
hccp 3 channel-switch 4 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 11
hccp 3 timers 666 2000

interface Cable4/1

hccp 4 protect 1 192.168.1.7
hccp 4 channel-switch 1 rfs1b rfs1b-group 192.168.1.5 22220200 1
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 protect 2 192.168.1.8
hccp 4 channel-switch 2 rfs1b rfs1b-group 192.168.1.5 22220200 2
hccp 4 channel-switch 2 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 12
hccp 4 protect 3 192.168.1.9
hccp 4 channel-switch 3 rfs1b rfs1b-group 192.168.1.5 22220200 3
hccp 4 channel-switch 3 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 4
hccp 4 protect 4 192.168.1.10
hccp 4 channel-switch 4 rfs1b rfs1b-group 192.168.1.5 22220200 4
hccp 4 channel-switch 4 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 12
hccp 4 timers 666 2000

interface Cable5/0

hccp 5 protect 1 192.168.1.7
hccp 5 channel-switch 1 rfs2a rfs2a-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 protect 2 192.168.1.8
hccp 5 channel-switch 2 rfs2a rfs2a-group 192.168.1.6 44440400 2
hccp 5 channel-switch 2 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 13
hccp 5 protect 3 192.168.1.9
hccp 5 channel-switch 3 rfs2a rfs2a-group 192.168.1.6 44440400 3
hccp 5 channel-switch 3 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 5
hccp 5 protect 4 192.168.1.10
hccp 5 channel-switch 4 rfs2a rfs2a-group 192.168.1.6 44440400 4
hccp 5 channel-switch 4 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 13
hccp 5 timers 666 2000

interface Cable5/1

hccp 6 protect 1 192.168.1.7
hccp 6 channel-switch 1 rfs2a rfs2a-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 protect 2 192.168.1.8
hccp 6 channel-switch 2 rfs2a rfs2a-group 192.168.1.6 11110100 2
hccp 6 channel-switch 2 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 14
hccp 6 protect 3 192.168.1.9
hccp 6 channel-switch 3 rfs2a rfs2a-group 192.168.1.6 11110100 3
hccp 6 channel-switch 3 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 6
hccp 6 protect 4 192.168.1.10
hccp 6 channel-switch 4 rfs2a rfs2a-group 192.168.1.6 11110100 4
hccp 6 channel-switch 4 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 14
hccp 6 timers 666 2000

interface Cable6/0

hccp 7 protect 1 192.168.1.7
hccp 7 channel-switch 1 rfs2b rfs2b-group 192.168.1.6 88880800 1
hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 protect 2 192.168.1.8
hccp 7 channel-switch 2 rfs2b rfs2b-group 192.168.1.6 88880800 2
hccp 7 channel-switch 2 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 15
hccp 7 protect 3 192.168.1.9
hccp 7 channel-switch 3 rfs2b rfs2b-group 192.168.1.6 88880800 3
```

```

hccp 7 channel-switch 3 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 7
hccp 7 protect 4 192.168.1.10
hccp 7 channel-switch 4 rfs2b rfs2b-group 192.168.1.6 88880800 4
hccp 7 channel-switch 4 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 15
hccp 7 timers 666 2000

interface Cable6/1

hccp 8 protect 1 192.168.1.7
hccp 8 channel-switch 1 rfs2b rfs2b-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 protect 2 192.168.1.8
hccp 8 channel-switch 2 rfs2b rfs2b-group 192.168.1.6 22220200 2
hccp 8 channel-switch 2 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 16
hccp 8 protect 3 192.168.1.9
hccp 8 channel-switch 3 rfs2b rfs2b-group 192.168.1.6 22220200 3
hccp 8 channel-switch 3 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 8
hccp 8 protect 4 192.168.1.10
hccp 8 channel-switch 4 rfs2b rfs2b-group 192.168.1.6 22220200 4
hccp 8 channel-switch 4 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 16
hccp 8 timers 666 2000

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 10.11.13.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
network 192.168.5.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps tty
snmp-server enable traps cable
snmp-server manager
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```

## Examples: Cisco 3x10 RF Switch with Cisco uBR10012 Chassis

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 5X20U or -S broadband processing engines (BPEs)

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



### Note

If you add one additional Cisco UBR10-MC 5X20U or -S 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 5X20U or -S 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](http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/quick/start/MC52_cbl.html)

### Summary Steps For This Configuration

1. Take the header that says RF Switch 2 (top Switch) and leave in slots 1, 2, 3, & 4.
2. Take the header that says RF Switch 1 and place in slots 5, 6, 7, & 8 of RF Switch 2.
3. Take the Protect from RF Switch 2 and put in Protect 2.
4. Take the Protect from RF Switch 1 and place in Protect 1 of RF Switch 2.
5. Once you get to five UBR10-MC 5X20U or -S BPEs, the bitmap configuration needs to be changed and the headers moved around from one Cisco RF Switch to the other. For example, the slot 5 header moves to the slot 1 header of Cisco RF Switch 1.

### Additional Configuration Notes

- The configuration is labeled “`rfswa`” as pertaining to slots 1-4 and their respective Protect slot, which is Protect 2.
- Protect 1 covers slots 5-8 on the Cisco RF Switch and is labeled as “`rfswb`.” In the 4+1 mode the RF Switch slots 5-8 are considered to be slots 1-4 for configuration purposes.
- These configurations are for MAC interface switchovers. Bear in mind that the entire JIB (ASIC) switches over when circumstances require. DS channels 0 and 1 share the same ASIC, DS channels 2 and 3 share the same ASIC, and DS channel 4 is on its own ASIC. If an interface does not have HCCP configured, it will not switch over even if it does share the same JIB with an HCCP interface.
- If using the **keepalive** command on HCCP interfaces that share a common ASIC, Cisco Systems recommends that you configure **no hccp g revertive** on the respective Protect interfaces. For additional information, refer to the topic [Disabling HCCP Revertive on Protect Cable Interfaces](#), page 12-8.

## HCCP Working 1 Example

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
```

## HCCP Working 2 Example

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
```

## HCCP Working 3 Example

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 rfsa rswitch-group 10.10.10.10 44440400 3

interface c7/0/1
 hccp 2 working 3
 hccp 2 channel-switch 3 rfsa rswitch-group 10.10.10.10 11110100 3

interface c7/0/2
 hccp 3 working 3
 hccp 3 channel-switch 3 rfsa rswitch-group 10.10.10.10 00005000 3
 hccp 3 channel-switch 3 rfsb rswitch-group 10.10.10.10 0000a080 3

interface c7/0/3
 hccp 4 working 3
 hccp 4 channel-switch 3 rfsb rswitch-group 10.10.10.10 88880800 3

interface c7/0/4
 hccp 5 working 3
 hccp 5 channel-switch 3 rfsb rswitch-group 10.10.10.10 22220200 3
```

## HCCP Working 4 Example

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 rfsa rswitch-group 10.10.10.10 44440400 4

interface c7/1/1
 hccp 2 working 4
 hccp 2 channel-switch 4 rfsa rswitch-group 10.10.10.10 11110100 4

interface c7/1/2
 hccp 3 working 4
 hccp 3 channel-switch 4 rfsa rswitch-group 10.10.10.10 00005000 4
 hccp 3 channel-switch 4 rfsb rswitch-group 10.10.10.10 0000a080 4

interface c7/1/3
 hccp 4 working 4
 hccp 4 channel-switch 4 rfsb rswitch-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 rfs witch-group 10.10.10.10 44440400 1
hccp 1 protect 2 10.10.10.1
hccp 1 channel-switch 2 rfswa rfs witch-group 10.10.10.10 44440400 2
hccp 1 protect 3 10.10.10.1
hccp 1 channel-switch 3 rfswa rfs witch-group 10.10.10.10 44440400 3
hccp 1 protect 4 10.10.10.1
hccp 1 channel-switch 4 rfswa rfs witch-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 rfs witch-group 10.10.10.10 11110100 1
hccp 2 protect 2 10.10.10.1
hccp 2 channel-switch 2 rfswa rfs witch-group 10.10.10.10 11110100 2
hccp 2 protect 3 10.10.10.1
hccp 2 channel-switch 3 rfswa rfs witch-group 10.10.10.10 11110100 3
hccp 2 protect 4 10.10.10.1
hccp 2 channel-switch 4 rfswa rfs witch-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 rfs witch-group 10.10.10.10 00005000 1
hccp 3 channel-switch 1 rfswb rfs witch-group 10.10.10.10 0000a080 1
hccp 3 protect 2 10.10.10.1
hccp 3 channel-switch 2 rfswa rfs witch-group 10.10.10.10 00005000 2
hccp 3 channel-switch 2 rfswb rfs witch-group 10.10.10.10 0000a080 2
hccp 3 protect 3 10.10.10.1
hccp 3 channel-switch 3 rfswa rfs witch-group 10.10.10.10 00005000 3
hccp 3 channel-switch 3 rfswb rfs witch-group 10.10.10.10 0000a080 3
hccp 3 protect 4 10.10.10.1
hccp 3 channel-switch 4 rfswa rfs witch-group 10.10.10.10 00005000 4
hccp 3 channel-switch 4 rfswb rfs witch-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 rfs witch-group 10.10.10.10 88880800 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfswb rfs witch-group 10.10.10.10 88880800 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfswb rfs witch-group 10.10.10.10 88880800 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfswb rfs witch-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 rfs witch-group 10.10.10.10 22220200 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfswb rfs witch-group 10.10.10.10 22220200 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfswb rfs witch-group 10.10.10.10 22220200 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfswb rfs witch-group 10.10.10.10 22220200 4

```

## Example: Channel Switch Information from the Cisco uBR10012 Router

The following output from the **show hccp channel-switch** command illustrates typical information about the current channel switch activity on a Cisco uBR10012 router configured with a Cisco 3x10 RF Switch.

```
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: Cisco 3x10 RF Switch and Cisco uBR10012 Chassis



### Note

This is the N+1 Redundancy configuration commonly cited in this document for Cisco 3x10 RF Switch examples (there are exceptions).

The following output from the **show run** command illustrates the configuration of N+1 Redundancy using the following CMTS:

- One Cisco 3x10 RF Switch in 8+1 mode
- One Cisco uBR10012 router
- Eight Cisco UBR10-LCP2-MC28C broadband processing engines (BPEs)

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 1gigetherne-1
  card 1/1 2cable-tccplus
  card 2/0 1gigetherne-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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 rfs witch rfs witch-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: Cisco 3x10 RF Switches and Cisco uBR10012 Chassis

The following output from the **show run** command illustrates the configuration of N+1 Redundancy using the following CMTS:

- Two Cisco RF Switches, each in 8+1 mode
- Cisco uBR10012 router
- Cisco UBR10-MC 5X20U or -S broadband processing engines (BPEs)

```
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 1gigetherenet-1
card 1/1 2cable-tccplus
card 2/0 1gigetherenet-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 rfs2 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 rfs2 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.
!

```

```

hcp 1 protect 2 10.10.10.1
!
! This is the first HCCP group and it is protecting member 2 with the loopback
! IP address.
!
hcp 1 channel-switch 2 rfs2 rswitch-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.
!
hcp 1 protect 3 10.10.10.1
hcp 1 channel-switch 3 rfs2 rswitch-group 10.97.1.20 AA200000 3
hcp 1 protect 4 10.10.10.1
hcp 1 channel-switch 4 rfs2 rswitch-group 10.97.1.20 AA200000 4
hcp 1 protect 5 10.10.10.1
hcp 1 channel-switch 5 rfs2 rswitch-group 10.97.1.20 AA200000 5
hcp 1 protect 6 10.10.10.1
hcp 1 channel-switch 6 rfs2 rswitch-group 10.97.1.20 AA200000 6
hcp 1 protect 7 10.10.10.1
hcp 1 channel-switch 7 rfs2 rswitch-group 10.97.1.20 AA200000 7
!
! These channel-switch configurations can be copied and pasted into their respective
! Working interfaces.
!
hcp 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
!
hcp 2 protect 1 10.10.10.1
hcp 2 channel-switch 1 rfs2 rswitch-group 10.97.1.20 55100000 1
!
! Because this MAC domain is on right side of header, the bitmap in
! hexadecimal code is 55100000.
!
hcp 2 protect 2 10.10.10.1
hcp 2 channel-switch 2 rfs2 rswitch-group 10.97.1.20 55100000 2
hcp 2 protect 3 10.10.10.1
hcp 2 channel-switch 3 rfs2 rswitch-group 10.97.1.20 55100000 3
hcp 2 protect 4 10.10.10.1
hcp 2 channel-switch 4 rfs2 rswitch-group 10.97.1.20 55100000 4
hcp 2 protect 5 10.10.10.1
hcp 2 channel-switch 5 rfs2 rswitch-group 10.97.1.20 55100000 5
hcp 2 protect 6 10.10.10.1
hcp 2 channel-switch 6 rfs2 rswitch-group 10.97.1.20 55100000 6
hcp 2 protect 7 10.10.10.1
hcp 2 channel-switch 7 rfs2 rswitch-group 10.97.1.20 55100000 7
hcp 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
hcp 3 protect 1 10.10.10.1
hcp 3 channel-switch 1 rfs1 rswitch-group 10.97.1.19 00C80000 1
hcp 3 channel-switch 1 rfs2 rswitch-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 rfswl rfswitch-group 10.97.1.19 AA200000 1
hccp 4 protect 2 10.10.10.1
hccp 4 channel-switch 2 rfswl rfswitch-group 10.97.1. 19 AA200000 2
hccp 4 protect 3 10.10.10.1
hccp 4 channel-switch 3 rfswl rfswitch-group 10.97.1. 19 AA200000 3
hccp 4 protect 4 10.10.10.1
hccp 4 channel-switch 4 rfswl rfswitch-group 10.97.1. 19 AA200000 4
hccp 4 protect 5 10.10.10.1
hccp 4 channel-switch 5 rfswl rfswitch-group 10.97.1. 19 AA200000 5
hccp 4 protect 6 10.10.10.1
hccp 4 channel-switch 6 rfswl rfswitch-group 10.97.1. 19 AA200000 6
hccp 4 protect 7 10.10.10.1
hccp 4 channel-switch 7 rfswl 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 rfswl rfswitch-group 10.97.1.19 55100000 1
hccp 5 protect 2 10.10.10.1
hccp 5 channel-switch 2 rfswl rfswitch-group 10.97.1. 19 55100000 2
hccp 5 protect 3 10.10.10.1
hccp 5 channel-switch 3 rfswl rfswitch-group 10.97.1. 19 55100000 3
hccp 5 protect 4 10.10.10.1
hccp 5 channel-switch 4 rfswl rfswitch-group 10.97.1. 19 55100000 4
hccp 5 protect 5 10.10.10.1
hccp 5 channel-switch 5 rfswl rfswitch-group 10.97.1. 19 55100000 5
hccp 5 protect 6 10.10.10.1
hccp 5 channel-switch 6 rfswl rfswitch-group 10.97.1. 19 55100000 6
hccp 5 protect 7 10.10.10.1
hccp 5 channel-switch 7 rfswl 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 rfs2 rfs2-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 rfs2 rfs2-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 minislots-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 rfs1 rfs1-switch-group 10.97.1.19 00c80000 1
hccp 3 channel-switch 1 rfs2 rfs2-switch-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 rfs1 rfs1-switch-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 rfs1 rfs1-switch-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: Cisco 3x10 RF Switches and uBR7246VXR Chassis

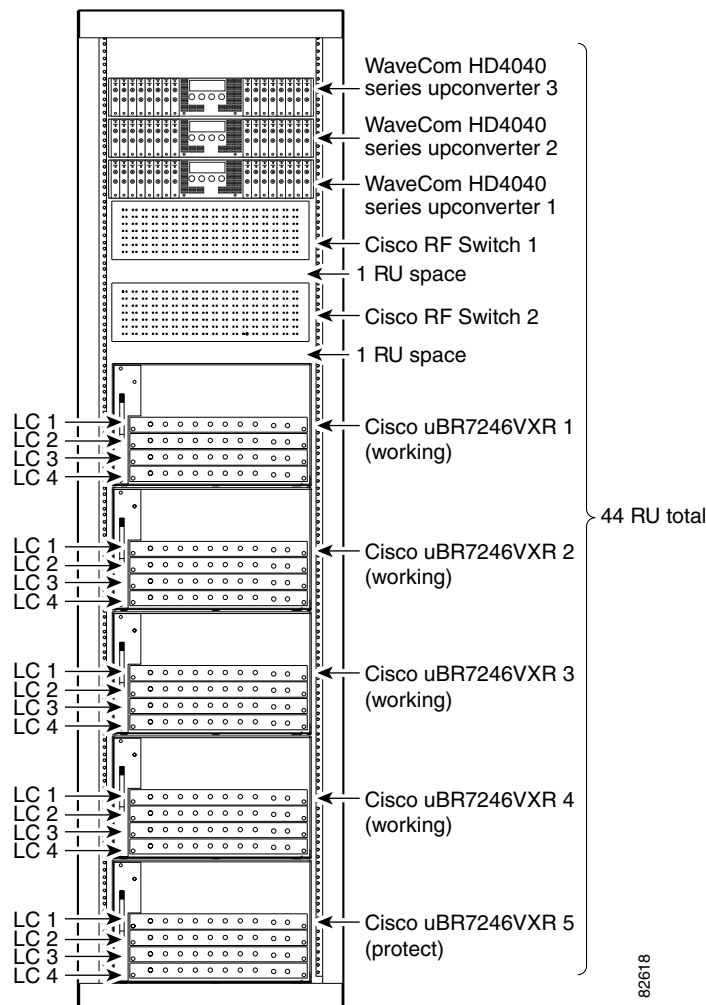
This is a sample N+1 configuration using the following Cisco CMTS:

- Two Cisco 3x10 RF Switches in 4+1 mode
- Five Cisco uBR7246VXR routers
- 20 uBR-MC28C line cards
- Three Vecima HD4040 chassis containing 40 modules

The physical rack layout is shown below in [Figure 6](#). A cabling document can be found on Cisco.com at:

<http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/installation/guide/310HIG.pdf>

**Figure 6** Physical Stack: 4+1 Redundancy Using Five uBR7246VXR Chassis with Two Cisco 3x10 RF Switches and Three Vecima Upconverters



The physical stack illustrated above assumes IP assignments starting with 192.168.1.2 from the top and continuing downward. Cisco RF Switch 1 is considered to be two switches because it will be in the 4+1 mode (a & b), where a contains slots 1-4 and b contains slots 5-8. The Cisco RF Switch 2 is also considered to be two switches (a & b).

## HCCP Working uBR7246VXR Chassis 1

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "WorkingVXR1"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxabcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
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
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.7 255.255.255.0
no keepalive
speed auto
full-duplex
!
! This interface is used for HCCP traffic.
!
interface FastEthernet0/1
ip address 192.168.2.7 255.255.255.0
keepalive 1
!
! Keepalive is set to 1 second so that if the cable is disconnected, this interface
! switches over within 3 seconds.
!
speed auto
full-duplex
!
interface Cable3/0

```

```

ip address 10.11.12.1 255.255.255.0 secondary
ip address 192.168.3.5 255.255.255.0
load-interval 30
keepalive 1
!
! The keepalive time is in seconds and the default is 10 seconds for HCCP code.
!
load-interval 30
cable downstream channel-id 0
cable bundle 1 master
!
! Interface bundling is supported as are subinterfaces.
! Note: Bundles switch over together.
!
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 UPx.
! This must be set when using the MC28U cards with internal UPxs or when doing N+1 with
! MC28C cards, so the Protect UPx knows what frequency to use.
!
cable upstream 0 frequency 24000000
!
! If doing dense mode combining, the upstream frequencies will need to be different.
! If no 2 US ports are shared, the same frequency can be used.
!
cable upstream 0 power-level 0
cable upstream 0 channel-width 3200000
cable upstream 0 minislot-size 2
cable upstream 0 data-backoff automatic
cable upstream 0 modulation-profile 3
no cable upstream 0 shutdown

cable dhcp-giaddr policy
!
! This tells CMs to get an IP address from the primary scope and CPEs to use the
! secondary scope.
!
hccp 1 working 1
!
! This is the working first group, member 1.
!
hccp 1 channel-switch 1 rfswl1 rswitch-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it's protecting member 1 in the left side
! of Switch slot 1.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) that is backing
! module 1 (A) of another 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 later Cisco
! IOS releases, IF Muting is assumed to be enabled and an external upconverter with
! SNMP capability is not needed.
!
hccp 1 track FastEthernet0/1
!
! Tracking was enabled for the egress port in case the WAN-backhaul was disrupted.
! This cable interface would switch over to the Protect.
!
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 there is a fault on the Protect card,
! it reverts back after the suspend time & does not wait for the full revert time.
!
interface Cable3/1
hccp 2 working 1
hccp 2 channel-switch 1 rfswl1 rswitch-group 192.168.1.5 11110100 1
!
! This is the IP address of the Switch and it is protecting member 1 in the right side
! of Switch slot 1.
!
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 reverttime 120

interface Cable4/0
hccp 3 working 1
hccp 3 channel-switch 1 rfswl1b rswitch-group 192.168.1.5 88880800 1

```

```

!
! This is the IP address of the Switch and it is protecting member 1 in the left side
! of Switch slot 5.
!
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 reverttime 120
!
interface Cable 4/1
hccp 4 working 1
hccp 4 channel-switch 1 rfswlb rswitch-group 192.168.1.5 22220200 1
!
! This is the IP address of the Switch and it is protecting member 1 in the right side
! of Switch slot 5.
!
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 reverttime 120

interface Cable5/0
hccp 5 working 1
hccp 5 channel-switch 1 rfs2a rswitch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 reverttime 120
!
interface Cable 5/1
hccp 6 working 1
hccp 6 channel-switch 1 rfs2a rswitch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 reverttime 120

interface Cable 6/0
hccp 7 working 1
hccp 7 channel-switch 1 rfs2b rswitch-group 192.168.1.6 88880800 1
hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 reverttime 120

interface Cable 6/1
hccp 8 working 1
hccp 8 channel-switch 1 rfs2b rswitch-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 reverttime 120

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
!
! This does not affect the HCCP communications between the Upconverter, Switch, and 7200.
!
snmp-server community public RO
snmp-server enable traps tty
snmp-server manager
tftp-server disk0:
tftp-server disk1:
tftp-server disk1:rfs250-fl-1935030e
tftp-server disk1:rfs250-bf-1935022d
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote
alias exec sm show cab modu
alias exec sch show cab hop
alias exec sc300 show cont c3/0 u0
alias exec sint300 show int c3/0 u0
alias exec scs show cable spec

```

## HCCP Protect uBR7246VXR Chassis

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname "ProtectVXR"
!
boot system disk0:ubr7200-ik8s-mz.BC.28July03
no logging console
enable secret 5 $1$5YHG$mquxabcqzFoUUKhp/c9WT4/
!
cab modem remote-query 10 public
cab modulation-prof 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw8
cab modulation-prof 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 2 short 4 76 6 8 qpsk scrambler 152 no-diff 72 short uw8
cab modulation-prof 2 long 8 220 0 8 qpsk scrambler 152 no-diff 80 short uw8
cab modulation-prof 3 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cab modulation-prof 3 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cab modulation-prof 3 short 7 76 7 8 16qam scrambler 152 no-diff 144 short uw16
cab modulation-prof 3 long 9 220 0 8 16qam scrambler 152 no-diff 160 short uw16
no cable qos permission create
no cable qos permission update
cable qos permission modems
no cable clock source-midplane
no cable clock force primary
no cable clock force secondary
!
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
!
ip subnet-zero
ip cef
!
ip host protect 192.168.1.7
ip host work2 192.168.1.6
ip name-server 171.68.226.120
!
ip dhcp pool MODEMS1
network 192.168.3.0 255.255.255.0
bootfile docsis.cm
next-server 192.168.3.5
default-router 192.168.3.5
option 7 ip 192.168.3.5
option 4 ip 192.168.3.5
option 2 hex 0000.0000
lease 2 3 4
!
ip dhcp pool PC
network 10.11.12.0 255.255.255.0
default-router 10.11.12.1
dns-server 171.68.226.120
lease 10 1 11
!
packetcable element_id 35417
!
interface FastEthernet0/0
ip address 192.168.1.11 255.255.255.0
no keepalive
speed auto
full-duplex
no cdp enable
!
interface FastEthernet0/1
ip address 192.168.2.11 255.255.255.0
keepalive 1
speed auto
full-duplex

```

```

no cdp enable
!
interface Cable3/0
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 to default of 10 seconds with the N+1 IOS code, but recommended
! to 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, Annex mode, and Interleave must be same on the Protect and
! Working of the same group.
!
no shut
!
! The interface must be activated to start HCCP functionality. Do this configuration last.
!
cable upstream 0 shutdown
!
! This automatically becomes "no shut" (enabled) when a switchover occurs.
!
hccp 1 protect 1 192.168.1.7
!
! This is the Protect for the first group. Remember to configure the Protect
! interface(s) last; after the Working interfaces are configured. This is the
! HCCP first group and it is protecting member 1 with member 1's FE IP address.
!
hccp 1 channel-switch 1 rfs1a rfs1a-group 192.168.1.5 44440400 1
!
! This is the IP address of the Switch and it is protecting member 1, which has a
! bitmap of 44440400 in Switch slot 1.
!
hccp 1 channel-switch 1 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 1
!
! This is the IP address of upconverter and its module 1 (A) that is backing
! module 1 (A) of another 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 later Cisco
! IOS releases, IF Muting is assumed to be enabled and an external upconverter with
! SNMP capability is not needed.
!
hccp 1 protect 2 192.168.1.8
!
! This is the HCCP first group and it is protecting member 2 with its IP address.
!
hccp 1 channel-switch 2 rfs1a rfs1a-group 192.168.1.5 44440400 2
hccp 1 channel-switch 2 uc31 wavecom-hd 192.168.1.2 1 192.168.1.4 9
hccp 1 protect 3 192.168.1.9
hccp 1 channel-switch 3 rfs1a rfs1a-group 192.168.1.5 44440400 3
hccp 1 channel-switch 3 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 1
hccp 1 protect 4 192.168.1.10
hccp 1 channel-switch 4 rfs1a rfs1a-group 192.168.1.5 44440400 4
hccp 1 channel-switch 4 uc32 wavecom-hd 192.168.1.2 1 192.168.1.3 9
hccp 1 timers 666 2000
hccp 1 timers
!
! Cisco IOS command = <hellotime> <holdtime>
! This is for inter-chassis communication.
!
interface Cable3/1

hccp 2 protect 1 192.168.1.7
hccp 2 channel-switch 1 rfs1a rfs1a-group 192.168.1.5 11110100 1
hccp 2 channel-switch 1 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 2
hccp 2 protect 2 192.168.1.8
hccp 2 channel-switch 2 rfs1a rfs1a-group 192.168.1.5 11110100 2
hccp 2 channel-switch 2 uc31 wavecom-hd 192.168.1.2 2 192.168.1.4 10
hccp 2 protect 3 192.168.1.9

```

```
hccp 2 channel-switch 3 rfswl1a rfs-switch-group 192.168.1.5 11110100 3
hccp 2 channel-switch 3 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 2
hccp 2 protect 4 192.168.1.10
hccp 2 channel-switch 4 rfswl1a rfs-switch-group 192.168.1.5 11110100 4
hccp 2 channel-switch 4 uc32 wavecom-hd 192.168.1.2 2 192.168.1.3 10
hccp 2 timers 666 2000
```

```
interface Cable4/0
```

```
hccp 3 protect 1 192.168.1.7
hccp 3 channel-switch 1 rfswl1b rfs-switch-group 192.168.1.5 88880800 1
hccp 3 channel-switch 1 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 3
hccp 3 protect 2 192.168.1.8
hccp 3 channel-switch 2 rfswl1b rfs-switch-group 192.168.1.5 88880800 2
hccp 3 channel-switch 2 uc31 wavecom-hd 192.168.1.2 3 192.168.1.4 11
hccp 3 protect 3 192.168.1.9
hccp 3 channel-switch 3 rfswl1b rfs-switch-group 192.168.1.5 88880800 3
hccp 3 channel-switch 3 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 3
hccp 3 protect 4 192.168.1.10
hccp 3 channel-switch 4 rfswl1b rfs-switch-group 192.168.1.5 88880800 4
hccp 3 channel-switch 4 uc32 wavecom-hd 192.168.1.2 3 192.168.1.3 11
hccp 3 timers 666 2000
```

```
interface Cable4/1
```

```
hccp 4 protect 1 192.168.1.7
hccp 4 channel-switch 1 rfswl1b rfs-switch-group 192.168.1.5 22220200 1
hccp 4 channel-switch 1 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 4
hccp 4 protect 2 192.168.1.8
hccp 4 channel-switch 2 rfswl1b rfs-switch-group 192.168.1.5 22220200 2
hccp 4 channel-switch 2 uc31 wavecom-hd 192.168.1.2 4 192.168.1.4 12
hccp 4 protect 3 192.168.1.9
hccp 4 channel-switch 3 rfswl1b rfs-switch-group 192.168.1.5 22220200 3
hccp 4 channel-switch 3 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 4
hccp 4 protect 4 192.168.1.10
hccp 4 channel-switch 4 rfswl1b rfs-switch-group 192.168.1.5 22220200 4
hccp 4 channel-switch 4 uc32 wavecom-hd 192.168.1.2 4 192.168.1.3 12
hccp 4 timers 666 2000
```

```
interface Cable5/0
```

```
hccp 5 protect 1 192.168.1.7
hccp 5 channel-switch 1 rfsw2a rfs-switch-group 192.168.1.6 44440400 1
hccp 5 channel-switch 1 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 5
hccp 5 protect 2 192.168.1.8
hccp 5 channel-switch 2 rfsw2a rfs-switch-group 192.168.1.6 44440400 2
hccp 5 channel-switch 2 uc31 wavecom-hd 192.168.1.2 5 192.168.1.4 13
hccp 5 protect 3 192.168.1.9
hccp 5 channel-switch 3 rfsw2a rfs-switch-group 192.168.1.6 44440400 3
hccp 5 channel-switch 3 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 5
hccp 5 protect 4 192.168.1.10
hccp 5 channel-switch 4 rfsw2a rfs-switch-group 192.168.1.6 44440400 4
hccp 5 channel-switch 4 uc32 wavecom-hd 192.168.1.2 5 192.168.1.3 13
hccp 5 timers 666 2000
```

```
interface Cable5/1
```

```
hccp 6 protect 1 192.168.1.7
hccp 6 channel-switch 1 rfsw2a rfs-switch-group 192.168.1.6 11110100 1
hccp 6 channel-switch 1 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 6
hccp 6 protect 2 192.168.1.8
hccp 6 channel-switch 2 rfsw2a rfs-switch-group 192.168.1.6 11110100 2
hccp 6 channel-switch 2 uc31 wavecom-hd 192.168.1.2 6 192.168.1.4 14
hccp 6 protect 3 192.168.1.9
hccp 6 channel-switch 3 rfsw2a rfs-switch-group 192.168.1.6 11110100 3
hccp 6 channel-switch 3 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 6
hccp 6 protect 4 192.168.1.10
hccp 6 channel-switch 4 rfsw2a rfs-switch-group 192.168.1.6 11110100 4
hccp 6 channel-switch 4 uc32 wavecom-hd 192.168.1.2 6 192.168.1.3 14
hccp 6 timers 666 2000
```

```
interface Cable6/0
```

```
hccp 7 protect 1 192.168.1.7
hccp 7 channel-switch 1 rfsw2b rfs-switch-group 192.168.1.6 88880800 1
```

```

hccp 7 channel-switch 1 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 7
hccp 7 protect 2 192.168.1.8
hccp 7 channel-switch 2 rfs2b rfs2b-group 192.168.1.6 88880800 2
hccp 7 channel-switch 2 uc31 wavecom-hd 192.168.1.2 7 192.168.1.4 15
hccp 7 protect 3 192.168.1.9
hccp 7 channel-switch 3 rfs2b rfs2b-group 192.168.1.6 88880800 3
hccp 7 channel-switch 3 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 7
hccp 7 protect 4 192.168.1.10
hccp 7 channel-switch 4 rfs2b rfs2b-group 192.168.1.6 88880800 4
hccp 7 channel-switch 4 uc32 wavecom-hd 192.168.1.2 7 192.168.1.3 15
hccp 7 timers 666 2000

interface Cable6/1

hccp 8 protect 1 192.168.1.7
hccp 8 channel-switch 1 rfs2b rfs2b-group 192.168.1.6 22220200 1
hccp 8 channel-switch 1 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 8
hccp 8 protect 2 192.168.1.8
hccp 8 channel-switch 2 rfs2b rfs2b-group 192.168.1.6 22220200 2
hccp 8 channel-switch 2 uc31 wavecom-hd 192.168.1.2 8 192.168.1.4 16
hccp 8 protect 3 192.168.1.9
hccp 8 channel-switch 3 rfs2b rfs2b-group 192.168.1.6 22220200 3
hccp 8 channel-switch 3 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 8
hccp 8 protect 4 192.168.1.10
hccp 8 channel-switch 4 rfs2b rfs2b-group 192.168.1.6 22220200 4
hccp 8 channel-switch 4 uc32 wavecom-hd 192.168.1.2 8 192.168.1.3 16
hccp 8 timers 666 2000

router eigrp 2500
network 10.11.12.0 0.0.0.255
network 10.11.13.0 0.0.0.255
network 192.168.1.0
network 192.168.3.0
network 192.168.5.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.0 255.255.255.0 FastEthernet0/0
ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
no ip http server
!
cdp run
!
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps tty
snmp-server enable traps cable
snmp-server manager
alias exec shb show hccp brief
alias exec shd show hccp detail
alias exec scm show cable modem
alias exec scr show cable modem remote

```

## Additional References

Cisco supports N+1 Redundancy using the Cisco 3x10 RF Switch on the following Cisco CMTS platforms:

- Cisco uBR10012 Universal Broadband Router
- Cisco uBR7246VXR Universal Broadband Router

For additional information related to N+1 Redundancy, the Cisco RF switch, and the Cisco uBR10012 and uBR7246VXR routers, refer to the following references.

## Related Documents

Related Topic	Document Title
Broadband Cable Command References	<ul style="list-style-type: none"> <li>• <i>Cisco Broadband Cable Command Reference Guide</i> <a href="http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html">http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html</a></li> <li>• <i>Cisco RF Switch Firmware Command Reference Guide</i> <a href="http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html">http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html</a></li> </ul>
Cisco RF Switches	<ul style="list-style-type: none"> <li>• <i>Cisco RF Switch Documentation</i> Web page (complete documentation set) <a href="http://www.cisco.com/en/US/products/hw/cable/ps2929/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/hw/cable/ps2929/tsd_products_support_series_home.html</a></li> <li>• Cisco RF Switch Installation and Configuration Guide <a href="http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/installation/guide/icg.html">http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/installation/guide/icg.html</a></li> <li>• Cisco RF Switch Product Data Sheet <a href="http://www.cisco.com/en/US/products/index.html">http://www.cisco.com/en/US/products/index.html</a></li> <li>• Field Notice—<i>uBR-RF-SW (N+1 Switch) Firmware Upgrade to Version 3.3 to Enable Setting of Default Gateway for Remote Software Upgrades</i> <a href="http://www.cisco.com/en/US/ts/fn/100/fn19290.html">http://www.cisco.com/en/US/ts/fn/100/fn19290.html</a></li> </ul>
Cisco uBR7246VXR Universal Broadband Router	<ul style="list-style-type: none"> <li>• <i>Cisco uBR7200 Series Universal Broadband Routers</i> Web page (complete documentation set) <a href="http://www.cisco.com/en/US/products/hw/cable/ps2217/index.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/index.html</a></li> </ul>
Cisco uBR10012 Universal Broadband Router	<ul style="list-style-type: none"> <li>• <i>Cisco uBR10012 Universal Broadband Router</i> Web page (complete documentation set) <a href="http://www.cisco.com/en/US/products/hw/cable/ps2209/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/hw/cable/ps2209/tsd_products_support_series_home.html</a></li> </ul>
High Availability References for Cisco Broadband Cable	<ul style="list-style-type: none"> <li>• <i>Bitmap Calculator for N+1 Configuration with the Cisco RF Switch</i> (Microsoft Excel format) <a href="http://www.cisco.com/warp/public/109/BitMap.xls">http://www.cisco.com/warp/public/109/BitMap.xls</a></li> <li>• <i>CMTS Feature Guide—Configuring PacketCable on the Cisco CMTS</i> (with emphasis on the Cisco uBR7246VXR router) <a href="http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html">http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html</a></li> </ul>

Related Topic	Document Title
DOCSIS and EuroDOCSIS	<ul style="list-style-type: none"> <li>Feature Module—<i>DOCSIS 1.1 for Cisco uBR7200 Series Universal Broadband Routers</i> <a href="http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html">http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html</a></li> <li>CMTS Feature Guide—<i>Internal DOCSIS Configurator File Generator for the Cisco Cable Modem Termination System</i> <a href="http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufgCFile.html">http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufgCFile.html</a></li> </ul>
Additional Broadband Cable Technical Reference	<ul style="list-style-type: none"> <li><i>Cisco Multiservice Broadband Cable Guide</i> <a href="http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_brochure09186a008014eeb0.pdf">http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_brochure09186a008014eeb0.pdf</a></li> <li>Cable Radio Frequency (RF) FAQs <a href="http://www.cisco.com/en/US/customer/tech/tk86/tk319/technologies_q_and_a_item09186a0080134faa.shtml">http://www.cisco.com/en/US/customer/tech/tk86/tk319/technologies_q_and_a_item09186a0080134faa.shtml</a></li> </ul>

## Standards

The Cisco uBR10012 router, Cisco uBR7246VXR router and the Cisco RF Switch each support N+1 redundancy in compliance with these industry standards:

- Data-Over-Cable Service Interface Specifications (DOCSIS):
  - DOCSIS 1.0 support for end-to-end cable telecommunications*
  - DOCSIS 1.1 support for end-to-end cable telecommunications*
- European DOCSIS (EuroDOCSIS)
- PacketCable

Refer to the your CMTS platform's release notes for additional information about standards supported by your specific CMTS equipment.

## MIBs

Certain versions of Cisco RF Switch Firmware may increase the MIBs that support N+1 Redundancy on the Cisco CMTS. To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the [Cisco Network Management Software](#) web page (MIBs sections) on Cisco.com. MIBs information for the Cisco RF Switch is also summarized in the *Cisco RF Switch Firmware Command Reference Guide* (document cited above).

## RFCs

No new or modified RFCs are supported 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>