



# Cisco RF Switch Firmware Configuration Guide

---

April 29, 2008

Cisco RF Switch Firmware Version 3.92

OL-15726-02

This document describes the cable-specific RF Switch Firmware and supporting command-line interface (CLI) through Version 3.92, to be used with Cisco IOS Release 12.3 BC and later releases, in the Cisco RF Switch.

This document supports commands and features (existing) in previous versions of Cisco RF Switch Firmware, subject to the restrictions and support for the N+1 Redundancy feature in Cisco IOS Release 12.3 BC.

For a list of the software enhancements or caveats that apply to Cisco RF Switch Firmware Version 3.92 or earlier, see the following document located on Cisco.com:

- *Release Notes for Cisco RF Firmware, Version 3.92*  
<http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/release/notes/rfswrn36.html>

For a list of general software configuration and operation procedures that are used for Cisco RF Switch Firmware Version 3.92 or earlier, see the following document located on Cisco.com:

- *Cisco RF Switch Firmware Command Reference Guide, Version 3.92*  
<http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html>

For detailed configuration and operation procedures that apply to HCCP N+1 Redundancy on the Cisco CMTS, see the following document located on Cisco.com:

- *N+1 Redundancy for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>

For a list of the software enhancements or caveats that apply to Cisco IOS Release 12.3 BC, see the following document located on Cisco.com:

- *Release Notes for Cisco IOS Software Release 12.3 BC*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html)



**Note**

---

You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after this document was initially published.

---



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected.

If you have an account on Cisco.com, you can find field notices at [http://www.cisco.com/en/US/customer/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html).

If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html)

## Contents

These release notes describe the following topics:

- [Prerequisites for Firmware Version 3.92](#)
- [Restrictions for Firmware Version 3.92](#)
- [Prerequisites for Firmware Version 3.90](#)
- [Restrictions for Firmware Version 3.90](#)
- [Prerequisites for Firmware Version 3.80](#)
- [Restrictions for Firmware Version 3.80](#)
- [Prerequisites for Firmware Version 3.60](#)
- [Restrictions for Firmware Version 3.60](#)
- [Information About Cisco RF Switch Firmware](#)
- [Information About the Cisco RF Switch](#)
- [How to Configure Cisco RF Switch Firmware](#)
- [Installing Cisco RF Switch Firmware Version 3.92](#)
- [Additional References](#)

## Prerequisites for Firmware Version 3.92

This section describes prerequisites that apply specifically to Firmware Version 3.92 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References”](#) section on page 22.

## Restrictions for Firmware Version 3.92

This section describes restrictions that apply specifically to Firmware Version 3.92 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.92, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.92:

*Release Notes for Cisco IOS Software Release 12.3 BC*

[http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod\\_release\\_notes\\_list.html](http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod_release_notes_list.html)

- Version 3.92 allocates new nvram location to support long passwords (32 characters) and SNMP community string (64 characters).
- In Version 3.92, on first reboot after migration from previous version, the new password and community string areas are installed and old settings (if any) are copied to new location.
- **If the user downgrades from 3.92 to a previous version, some of the configuration parameters in the newer versions are not recognized by the older software which causes the some of the config elements to be reset to default values.**
- **If user downgrades from Version 3.92 to Version 3.80, the new nvram location for password and community string is not recognized, and the password is removed and community string is set to private.**
- **If the user downgrades from Version 3.92 to Version 3.60 or earlier, the password is removed and community string is set to private, and the ip address, default gateway and tftp address are reset to default values.**

**Note**

Version 3.92 is case-sensitive and stores passwords and SNMP community strings as they are entered on the CLI. In previous versions the case-sensitivity was not preserved and passwords and community strings were converted internally — passwords were stored in all uppercase and community strings in all lowercase. The parser allowed the user to type in any case as long as the letters matched.

**When the user upgrades to Version 3.92, the mixed case passwords and SNMP community strings from previous versions are stored as lower case characters. After the upgrade, the user should verify the password and community string and set them as desired.**

## Prerequisites for Firmware Version 3.90

This section describes prerequisites that apply specifically to Firmware Version 3.90 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References” section on page 22](#).

## Restrictions for Firmware Version 3.90

This section describes restrictions that apply specifically to Firmware Version 3.90 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.90, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.90:

*Release Notes for Cisco IOS Software Release 12.3 BC*

[http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod\\_release\\_notes\\_list.html](http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod_release_notes_list.html)

## Prerequisites for Firmware Version 3.80

This section describes prerequisites that apply specifically to Firmware Version 3.80 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the “[Additional References](#)” section on page 22.
- The password on the RF Switch should be removed before upgrading the RF Switch to Version 3.80. The password can be set on the RF Switch when the upgrade to Version 3.80 is complete.

## Restrictions for Firmware Version 3.80

This section describes restrictions that apply specifically to Firmware Version 3.80 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.80, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.80:

*Release Notes for Cisco IOS Software Release 12.3 BC*

[http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod\\_release\\_notes\\_list.html](http://cisco.com/en/US/partner/products/hw/cable/ps2209/prod_release_notes_list.html)

## Prerequisites for Firmware Version 3.60

This section describes prerequisites that apply specifically to Firmware Version 3.60 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the “[Additional References](#)” section on page 22.
- Cisco recommends that the RF Switch Firmware be upgraded to Version 3.60 from previous Firmware versions, particularly for operation of the Cisco uBR10012 router with Cisco IOS Release 12.3(21)BC in N+1 Redundancy. Refer to general field notices, and the following documents for additional information:
  - *Field Notice: FN - 62695 - Cisco RF Switch Firmware Version 3.60 - Mandatory Upgrade*, Document ID: 82266  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_field_notices_list.html)
  - *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*  
[http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12\\_3bc/ubr10k\\_123bc\\_rn.html](http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html)

## Restrictions for Firmware Version 3.60

- The Cisco uBR7246VXR router only supports N+1 Redundancy using Cisco IOS Release 12.3(9a)BC or prior N+1-enabled Cisco IOS releases. Firmware Version 3.60 supports N+1 Redundancy in these earlier releases.
- Cisco recommends upgrading to Firmware Version 3.60, even with earlier Cisco IOS releases, subject to N+1 Prerequisites and Restrictions in the Cisco IOS release, such as feature interoperability, factory default configurations, and so forth.
- Refer to the following Firmware Upgrade Field Notice for additional information:
  - *Field Notice: FN - 62695 - Cisco RF Switch Firmware Version 3.60 - Mandatory Upgrade*, Document ID: 82266  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_field_notices_list.html)

## Information About Cisco RF Switch Firmware

The following topics in this section provide an overview of Firmware components and operation:

- [Cisco RF Switch Firmware and Cisco IOS Software, page 5](#)
- [Cisco RF Switch Firmware Components and Operation, page 5](#)
- [Cisco RF Switch Firmware Command-line Interface, page 9](#)

## Cisco RF Switch Firmware and Cisco IOS Software

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

- Cisco RF Switch Firmware—governs the configuration and operation of Cisco RF Switches, including the MAC addresses on RF Switch interfaces and multiple module-to-interface settings, and enables TFTP transfer of Firmware images.
- Cisco Internetwork Operating System (IOS)—governs the configuration and operation of Cisco universal broadband routers, and works closely with Cisco RF Switch Firmware.

Both command-line interfaces above are required for configuration and testing of N+1 Redundancy. Refer to [N+1 Redundancy for the Cisco Cable Modem Termination System](#) for complete N+1 configuration procedures covering both Cisco Firmware and Cisco IOS.

## Cisco RF Switch Firmware Components and Operation

The Cisco N+1 Redundancy Unit (NRU) Firmware is comprised of three components. The latest files and versions for each are shown below in [Table 1](#):

**Table 1** *Cisco RF Switch Firmware Components and Functions, Version 3.90*

Component	File	Version	Location	Functions
RomMon	1935033A.BIN	1.10	N/A	<ul style="list-style-type: none"> <li>• The first Firmware component to run during RF Switch startup, and loads the Bootflash image during a Watchdog (WDOG) timeout event or certain other events, but typically loads the Flash image for normal bootup or restart events with the <b>reboot</b> or <b>reload</b> command.</li> <li>• Determines the cause of system reset and controls the next phase of system startup.</li> </ul>

**Table 1 Cisco RF Switch Firmware Components and Functions, Version 3.90**

Component	File	Version	Location	Functions
SysLoader	1935022H.BIN	2.30	Bootflash:	<ul style="list-style-type: none"> <li>Commencing with Firmware Version 3.60, the SysLoader image in Bootflash is deprecated by the NruApp image, which is loaded into Bootflash instead.</li> <li>The legacy function of SysLoader was to increase system reliability, functions now performed by NruApp.</li> <li>SysLoader was normally invoked with system failure in Firmware versions prior to 3.60.</li> </ul>
NruApp	1935030J.BIN	3.60	Bootflash:	<ul style="list-style-type: none"> <li>Commencing with Firmware Version 3.60, the NruApp image is loaded in Bootflash and Flash, rather than Flash only.</li> <li>The NruApp image deprecates the SysLoader image in Firmware Version 3.60 and later.</li> <li>NruApp functions as the primary component of Cisco RF Switch Firmware, and provides users with the <code>rfswitch&gt;</code> command-line interface (CLI).</li> <li>NruApp provides full network functionality and line card control.</li> </ul>
NruApp	1935030K.BIN	3.80	Bootflash:	<ul style="list-style-type: none"> <li>Commencing with Firmware Version 3.60, the NruApp image is loaded in Bootflash and Flash, rather than Flash only.</li> <li>The NruApp image deprecates the SysLoader image in Firmware Version 3.60 and later.</li> <li>NruApp functions as the primary component of Cisco RF Switch Firmware, and provides users with the <code>rfswitch&gt;</code> command-line interface (CLI).</li> <li>NruApp provides full network functionality and line card control.</li> </ul>
NruApp	1935030L.BIN	3.90	Bootflash, Flash:	<ul style="list-style-type: none"> <li>Commencing with Firmware Version 3.60, the NruApp image is loaded in Bootflash and Flash, rather than Flash only.</li> <li>The NruApp image deprecates the SysLoader image in Firmware Version 3.60 and later.</li> <li>NruApp functions as the primary component of Cisco RF Switch Firmware, and provides users with the <code>rfswitch&gt;</code> command-line interface (CLI).</li> <li>NruApp provides full network functionality and line card control.</li> </ul>
NruApp	1935030N.BIN	3.92	Bootflash, Flash:	<ul style="list-style-type: none"> <li>Commencing with Firmware Version 3.60, the NruApp image is loaded in Bootflash and Flash, rather than Flash only.</li> <li>The NruApp image deprecates the SysLoader image in Firmware Version 3.60 and later.</li> <li>NruApp functions as the primary component of Cisco RF Switch Firmware, and provides users with the <code>rfswitch&gt;</code> command-line interface (CLI).</li> <li>NruApp provides full network functionality and line card control.</li> </ul>

## RomMon Overview

RomMon is the first component to run on the Cisco RF Switch. RomMon is invoked whenever a reset event occurs, such as with startup, WDOG timeout system failure, or a software-based restart (**reboot**, **reload** commands). RomMon is responsible for determining the cause of the reset event and controls the next phase of system startup.

RomMon is not contained in ROM, as the term implies, but in Flash. RomMon contains a menu-driven interface that updates Firmware images in the event of a catastrophic system failure. Image update for RomMon occurs through the RS-232 serial port and XYMODEM download feature.

There is only one copy of the RomMon image on the Cisco RF Switch. The RomMon image must be updated 'off-line.' As a safety measure, hardware DIP switches on the controller must be enabled for RomMon update. RomMon is not network-aware.

## NruApp and SysLoader Overview

The File System in Cisco RF Switch Firmware is comprised of two images, each of which has a Working and Backup copy:

- NruApp image contained in the Bootflash (`rfswitch>` prompt), and deprecates the SysLoader image in Firmware Version 3.60 Bootflash and later.
- In prior Firmware Versions, the SysLoader image was contained in the Bootflash (`Sys>` prompt).

**NruApp** is the primary component of Cisco RF Switch Firmware, and this is where the vast majority of Firmware configuration changes are made. NruApp provides full network functionality for RF Switch configuration and operation. The NruApp command-line interface (CLI) is the `rfswitch>` prompt.

**SysLoader** is a special build of the NruApp image. SysLoader is normally invoked as a result of a system failure and it helps increase system reliability and availability. SysLoader does not offer SNMP agent support or line card control, but SysLoader is capable of sending SNMPv1 traps as simple UDP packets. SysLoader fully supports Telnet and TFTP operations. The SysLoader command-line interface (CLI) is indicated by the `Sys>` prompt, but the SysLoader CLI applies to very few commands.

Both the SysLoader image (Bootflash prior to Version 3.60) and the NruApp image (Flash prior to Version 3.60, and Bootflash from Version 3.60 onward) contain built-in functions such as:

- image integrity verification
- automatic image backup
- image recovery functions

Firmware maintains two copies each of both NruApp and SysLoader images:

- Copy #1 (backup)
- Copy #2 (working)



### Note

File operations (open, read, write and close) automatically verify image integrity and create backups if required.

## Firmware Operation Overview and Read/Write Functions

In general, the Cisco RF Switch Firmware operates as follows, always working to maintain at least one valid copy of the SysLoader and NruApp files. [Table 2](#) summarizes automatic updates and standard read/write functions.

**Table 2** Read and Write Functions between Backup and Working Firmware Images

File Operation	Backup Copy (#1) Status	Working Copy (#2) Status	Result
Open (read)	Valid	N/A	Read #1.
	Invalid	Valid	Copy #2 to #1. Read #1
	Invalid	Invalid	File open error
Open (write)	Valid	N/A	Erase #2. Write data to #2.
	Invalid	Valid	Copy #2to #1. Write data to #2.
	Invalid	Invalid	Erase #2. Write data to #2
Close (read)	N/A	N/A	No operation required
Close (write)	Valid	Valid	If CRCs are different, then copy #2 to #1
	Valid	Invalid	Copy #1 to #2
	Invalid	Valid	Copy #2 to #1
	Invalid	Invalid	File write error

SysLoader and NruApp image files are opened for read mode during file loading and TFTP uploads. Files are opened in write mode for TFTP downloads.

File writing is performed directly to the Flash devices because the size of the file may exceed available RAM space. File writing is performed only on the working copy (#2).



### Note

When a file is closed in write mode (such as after a download) the system automatically backs up and restores the file as required.

Closing a file after a download may take some time. The reason is that any **erase** or **copy** operations involve erasing sectors of the Flash, which may require a few seconds per Flash sector.

## Firmware Startup Process

Continuing with the startup process (after file load), the RomMon verifies the integrity of the file system. If the reset event was caused by WDOG timeout (presumably due to a system failure, but WDOG timeouts can be manually induced), the RomMon attempts to load the image from Bootflash into RAM and run it. If the Bootflash image is invalid, RomMon then attempts to load the Flash image as a last resort.

If the cause of the reset event was a normal boot-up or software-based restart (**reboot** or **reload** commands), then an attempt is made to load and run the Flash i mage. If this load fails, then an attempt is made to load and run the Bootflash image.

## Firmware Prompts and LED Indicators

The Cisco RF Switch CLI displays the NruApp prompt (`rfswitch>`) under normal circumstances. In Cisco Firmware Version 3.60 and later, the system prompt always remains at `rfswitch>`.

In previous Cisco Firmware versions, the system prompt changed from `rfswitch>` to `Sys>` if the SysLoader image was running.

If the system has experienced a failure, the SysLoader (**SYS**) LED light flashes on the Cisco RF Switch Chassis.

If RomMon is unable to load either the SysLoader or NruApp image, then RomMon remains in control and the controller's **SYS** LED light turns off and the **ERR** LED light flashes.

## Cisco RF Switch Firmware Command-line Interface

This section provides guidelines and methods for using the command-line interface (CLI) of the Cisco RF Switch Firmware:

- [Usage Guidelines for Cisco RF Switch Firmware, page 9](#)
- [Keyboard Shortcuts for Cisco RF Switch Firmware, page 9](#)
- [Command and Keyword Abbreviations for Cisco RF Switch Firmware, page 9](#)

### Usage Guidelines for Cisco RF Switch Firmware

- For additional command information, type **config ?**, **generate ?**, or **erase ?** at the CLI.
- For a list of diagnostic and test commands, type **sys ?** at the CLI.'
- No command autocompletion is available through Version 3.50.

### Keyboard Shortcuts for Cisco RF Switch Firmware

To recall the previous commands issued at the Firmware command-line interface (CLI), use **Ctrl-P**.

### Command and Keyword Abbreviations for Cisco RF Switch Firmware

Most Firmware commands have alternate short forms. These are summarized below in [Table 3](#).



**Note**

To display a list of keyword abbreviations, type **cmd ?** at the RF Switch prompt.

**Table 3** *Firmware Command and Keyword Abbreviations*

Command or Keyword	Abbreviation(s)	Command or Keyword	Abbreviation(s)
address	ad, addr	protection	pr, prot, protect
community	comm	reload	re
config	cf, cfg, conf	run	ru
copy	c, co	serialno	sn, serno
count	cnt, cou	set	s, se
default-gateway	gate, gateway	set access system	se acc sys
device	dev	show	sh
disable	dis	slot	sl
enable	en, ena	status	st
echo	echo	switch	sw, swit

**Table 3**      **Firmware Command and Keyword Abbreviations**

Command or Keyword	Abbreviation(s)	Command or Keyword	Abbreviation(s)
<b>fault</b>	<b>fa</b>	<b>switchover-group</b>	<b>switchover-gr</b>
<b>file</b>	<b>f, fi</b>	<b>system</b>	<b>sys, syst</b>
<b>gateway</b>	<b>gate</b>	<b>telnet</b>	<b>telnet</b>
<b>generate</b>	<b>ge, gen</b>	<b>test</b>	<b>te</b>
<b>group</b>	<b>gr</b>	<b>tftp-host</b>	<b>tftp</b>
<b>help</b>	<b>?</b>	<b>timeout</b>	<b>tout</b>
<b>host</b>	<b>ho</b>	<b>trap/traps</b>	<b>tr</b>
<b>interval</b>	<b>int</b>	<b>version</b>	<b>v, ve, ver, vers</b>
<b>module</b>	<b>m, mod</b>	<b>wdog</b>	<b>wd</b>
<b>no</b>	<b>n</b>	<b>bootflash:</b>	<b>bf:</b>
<b>password</b>	<b>pa, pass</b>	<b>flash:</b>	<b>fl:</b>

## Information About the Cisco RF Switch

The topics in this section describe hardware components of the Cisco RF Switch that are configured with or influenced by the Cisco RF Switch Firmware after cabling and initial setup is complete:

- [Cisco RF Switch Overview, page 10](#)
- [Cisco RF Switch Modules and Slot Numeration, page 10](#)

### Cisco RF Switch Overview

Cisco offers the The Cisco uBR 3x10 RF Switch, which supports three downstream and 10 upstream RF Switch modules. The 3x10 RF Switch can be configured as two “virtual” switches when configuring N+1 Redundancy with the Cisco uBR7246VXR router.

The Cisco 3x10 RF Switch offers an Ethernet controller module, an AC or DC power supply, and optional color-coded cabling that is terminated in advance.

The Cisco RF Switch is a multiplexing system that can reroute any of the RF cables connected to active Cisco RF line cards to a spare or backup set of RF line cards.

### Cisco RF Switch Modules and Slot Numeration

Both Cisco RF Switches contain 14 modules, and each RF switch module supports the full frequency range specified by DOCSIS and EuroDOCSIS standards.

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.

#### **Online Insertion and Removal (OIR) for the Cisco RF Switch Chassis**

The online insertion and removal (OIR) feature allows you to remove an Ethernet controller or an upstream or downstream assembly and replace it with another that is configured in identical fashion. If the new controller or assembly matches the controller or assembly you removed, the system immediately brings it online. In order to enable 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.

**MAC Addresses and the Cisco RF Switch Chassis**

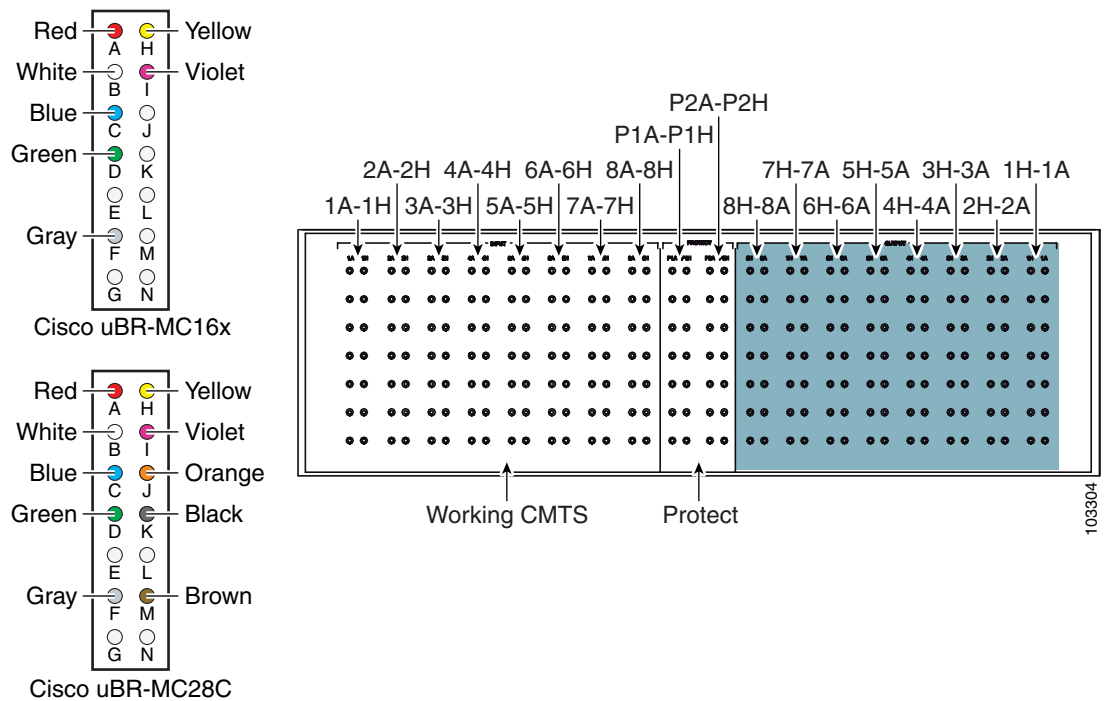
The MAC-layer or hardware address is a standardized data link layer address that is required for certain network interface types. The Cisco RF Switch uses a specific method to assign and control the MAC-layer addresses of its Ethernet controller.

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 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.

**Slot Numeration on the Cisco RF Switch Chassis**

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.

**Figure 1 Cisco RF Switch Modules, Rear View**



The Working and the Protect line cards are cabled from the Cisco router chassis to the Cisco RF Switch ports. 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.

**Module and Port Numeration on the Cisco RF Switch Chassis**

Table 4 lists the RF modules and the ports assigned to each module, as illustrated in Figure 1.



**Tip**

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

<sup>8</sup>  
**Table 4** *Switching Matrix for the Cisco uBR 3x10 RF Switch (Upstream and Downstream Modules)*

Module	Working Ports	PROTECT Ports	Type	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.

**Upstream Modules and Ports on the Cisco RF Switch Chassis**

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

**Downstream and Unassigned Modules and Ports on the Cisco RF Switch Chassis**

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.

# How to Configure Cisco RF Switch Firmware

This section describes the following procedures for basic Cisco Firmware configuration and operation:

- [Enabling and Operating DHCP on the Cisco RF Switch, page 13](#)
- [Reloading Default Settings on the Cisco RF Switch, page 14](#)
- [Loading Updated Firmware Images and Configurations on the Cisco RF Switch, page 15](#)
- [Using Passwords with Cisco RF Switch Firmware, page 17](#)
- [Setting System-Level Access in Firmware Versions 3.80 and later, page 17](#)
- [Recovering Passwords from Console Ports in Firmware Versions 3.80 and later, page 17](#)
- [Using Telnet Client Access with Cisco RF Switch Firmware, page 18](#)
- [Installing Cisco RF Switch Firmware Version 3.92, page 20](#)

## Enabling and Operating DHCP on the Cisco RF Switch

Beginning with Version 3.30, Cisco RF Switch Firmware includes full support for a DHCP client. DHCP operation is enabled by default, unless the you have defined a static IP address at the command-line interface (CLI).

When the Cisco RF Switch starts, it checks to see if DHCP has been enabled. You can enable DHCP at the Cisco RF Switch CLI in any one of these three ways:

- **set ip address dhcp**
- **set ip address 0.0.0.0**
- **no set ip address** (to set the default, which is DHCP enabled)

Beginning with Firmware Version 3.30, the Cisco RF Switch no longer assumes a static IP address of 10.0.0.1 as in Version 2.50. The default setting for Version 3.30 is DHCP enabled.

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** command. Because the actual lease time is granted from the server, this command is primarily used for debug/testing, and should not be required for normal operation.

If 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.

If a server is not located within 20-30 seconds, the DHCP client is suspended, and the CLI runs. The DHCP client remains running in the background attempting to contact a server approximately every 5 seconds until a server is located, a static IP address 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** command parameters are stored in non-volatile memory (nvram), and are maintained through reboots.

## Commands Supporting DHCP on the Cisco RF Switch

Because the current network settings may come from either DHCP or the CLI, a number of Firmware commands have been implemented to support DHCP. These commands are as follows:

- **show config**—This command displays the settings of all the non-volatile memory (nvram) parameters, which are not necessarily the ones in effect at the time of command execution.
- **show dhcp**—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.
- **show ip**—Displays the current network parameters in use. 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 once a valid IP exists).

Assignment of static values for any of the definable network parameters (using **set** commands) should go into effect immediately, and override the current setting without further action. This automatic update allows some of the parameters to remain dynamic while fixing others.

In the case of DHCP, 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 changing from using a static IP address to DHCP. Because the DHCP client is only installed at boot-up as required, transitioning from a static IP address to DHCP requires the system to be rebooted for DHCP to take effect.

## Reloading Default Settings on the Cisco RF Switch

The commands in this procedure save the default settings on the Cisco RF Switch and then restart the Switch so that the default settings take effect.

### SUMMARY STEPS

Use the **save config** command to save the current config into nvram. Normally used after ERASE CONFIG and RELOAD, which would save the default settings.

1. **enable**
2. **set access system**
3. **allow erase**
4. **erase config**
5. **reboot** or **reload**
6. **save config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> rfswitch> enable	This command enables the use of system-level commands.
Step 2	<b>set access system</b>  <b>Example:</b> rfswitch> set access system	This command sets the system access.
Step 3	<b>allow erase</b>  <b>Example:</b> rfswitch> allow erase	Enables the use of the separate <b>erase</b> commands for a single execution.
Step 4	<b>erase</b>  <b>Example:</b> rfswitch> erase config	Removes the contents of the Cisco RF Switch non-volatile memory (nvmem).
Step 5	<b>reboot</b> or <b>reload</b>  <b>Example:</b> rfswitch> reboot	This command restarts the Cisco RF Switch so that the original image runs. Use either the <b>reboot</b> or <b>reload</b> command.
Step 6	<b>save config</b>  <b>Example:</b> rfswitch> save config	Saves the newly loaded default settings to non-volatile memory (nvmem).

## Loading Updated Firmware Images and Configurations on the Cisco RF Switch

To save Firmware image configuration changes, perform the following steps at the Firmware prompt (rfswitch>).

## SUMMARY STEPS

1. **enable**
2. **copy tftp: *URL-filename* flash:**
3. **reboot** or **reload**
4. **copy tftp: *URL-filename* bootflash: noverify**
5. **reboot** or **reload**
6. **enable**
7. **set access system**
8. **save config**
9. **reboot** or **reload**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> rfswitch> enable	This command enables the use of system-level commands.
Step 2	<b>copy tftp:</b> <i>URL-filename</i> <b>flash:</b>  <b>Example:</b> rfswitch> copy tftp:1935030f.bin fl:	Install the new NruApp image update using the <b>copy tftp</b> command. <ul style="list-style-type: none"> <li>• <i>URL-filename</i>—IP address and image filename on the TFTP host.</li> <li>• <b>flash:</b>—The Flash image on the Cisco RF Switch. The keyword <b>flash:</b> may be abbreviated as <b>FL:</b>.</li> </ul>
Step 3	<b>reboot</b> or <b>reload</b>  <b>Example:</b> rfswitch> reboot	This command restarts the Cisco RF Switch so that the new images run. Use either the <b>reboot</b> or <b>reload</b> command.
Step 4	<b>copy tftp:</b> <i>URL-filename</i> <b>bootflash:</b> <b>noverify</b>  <b>Example:</b> rfswitch> copy tftp:1935022e.bin bf:	Install the new SysLoader image update using the <b>copy tftp</b> command. <ul style="list-style-type: none"> <li>• <i>URL-filename</i>—IP address and image filename on the TFTP host.</li> <li>• <b>bootflash:</b>—The Bootflash image on the Cisco RF Switch. The keyword <b>bootflash:</b> may be abbreviated as <b>BF:</b>.</li> <li>• <b>noverify</b>—Firmware Version 3.60 or later. Overrides the file type verification, and places a file in either the flash (FL:) or bootflash (BF:) device.</li> </ul>
Step 5	<b>reboot</b> or <b>reload</b>  <b>Example:</b> rfswitch> reboot	This command restarts the Cisco RF Switch so that the new images run. Use either the <b>reboot</b> or <b>reload</b> command.
Step 6	<b>enable</b>  <b>Example:</b> rfswitch> enable	This command enables the use of system-level commands.
Step 7	<b>set access system</b>  <b>Example:</b> rfswitch> set access system	This command sets the system access.
Step 8	<b>save config</b>  <b>Example:</b> rfswitch> save config	This command saves the latest configuration or image upgrade changes in both Flash and Bootflash, and synchronizes Backup and Working copies in each.
Step 9	<b>reboot</b> or <b>reload</b>  <b>Example:</b> rfswitch> reload	This command restarts the Cisco RF Switch so that all changes above take effect.

## Using Passwords with Cisco RF Switch Firmware

Passwords can be used to help prevent inadvertent changes to the Cisco RF Switch configuration. However, password protection as a security scheme is generally weak on the Cisco RF Switch alone.

With Firmware Version 2.50, a user can view the current password using the **show config** command in User mode.

Beginning with Firmware Version 3.30 and continuing with later versions, the password is encrypted, and is not decipherable from the **show config** command.

Prior to Version 3.80, there was a fixed password (**system**) that grants system-level access to many commands normally reserved for system testing and configuration. Refer to **Table 6**.

Version 3.92 allows passwords up to 32 characters in length and SNMP community strings up to 64 characters in length, which may contain any of the printable ASCII characters (0x20-0x7e), with the exception of the space (0x20), double quote (0x22), semicolon (0x3b), backslash (\), and forward slash (/) characters. In addition the character '?' and 'HELP' cannot be used in strings by themselves as they invoke the help function.

The passwords and SNMP community strings are stored the way they are entered on the command-line interface (CLI). The user can store mixed case strings for passwords and SNMP community strings. In previous versions the case-sensitivity was not preserved and passwords and community strings were converted internally — passwords were stored in all uppercase and community strings in all lowercase. The parser allowed the user to type in any case as long as the letters matched.

Refer also to the **set password** command (**enable password** replaces **set password** from Version 3.80 and later) for additional information.

Beginning with Firmware Version 3.80 and continuing with later versions, all commands previously utilizing a backdoor password will only be usable using **set access system**.

## Setting System-Level Access in Firmware Versions 3.80 and later

Cisco RF Switch Firmware Versions 3.80 and later enables access to system level commands, previously accessible using backdoor password, through **set access system**.

To exit and return to normal user mode, use the **disable** or **exit** command.



**Note**

The **set access system** command can only be used in the enable mode.

## Recovering Passwords from Console Ports in Firmware Versions 3.80 and later

Passwords can be recovered from the console ports without having to clear the entire nvram in Firmware Versions 3.80 and later.

The following procedure details the steps for recovering a password from a console port:

1. Send break to rf-switch from console port.
2. When rf-switch receives this break character through the console port only, it enables password recovery mode. Password recovery enables the following console port cmds:
  - **show password**: Displays current password
  - **recover password**: Erases current password, but leaves config intact

3. Password recovery mode automatically terminates on the third attempt or command.
4. The module switch states are now cached for both SETs and GETs.

Caching can be enabled/disabled via a new cli SET SNMP CACHE 0/1, whose setting is stored in nvram (by default, caching is enabled). Caching may also be controlled via an snmp object “nruCacheSnmpData”, which is a read-write integer at OID 1.3.6.1.4.1.6804.2.1.1.9:

```
nruCacheSnmpData OBJECT-TYPE
    SYNTAX      INTEGER (0..1)
    ACCESS      read-write
    STATUS      mandatory
    DESCRIPTION "The desired state of the module AdminState caching flag."
    ::= { nruObjs 9}
```

Setting the “nruCacheSnmpData” object via snmp alters the run-time setting of the cache flag, but does not effect the state of the nvram setting. This allows you to dynamically override the setting of the cache flag to verify the state of the settings if needed.

The state of the nvram setting has been added to the **show config** command. The current run-time state has been added to the **show module** command.

## Using Telnet Client Access with Cisco RF Switch Firmware

The Telnet and console command-line interfaces (CLIs) do not have simultaneous, shared access. Each has separate access rights. Telnet CLI access is characterized by the following guidelines for session startup and disconnect:

- 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.
- Access to the Telnet CLI can be restricted using the **set password** (Version 3.60 and earlier) or **enable password** (Version 3.80 and later) command in User mode.
- Telnet access to the RF Switch from the router console makes double entries when typing. One workaround is to disable local echo. For example, from the Cisco uBR10012 router CLI, use the **/noecho** option (as shown below):

```
Router# telnet 10.0.0.1 /noecho
```

where 10.0.0.1 is the IP address of the Ethernet interface on the RF Switch chassis.

- The default state for echoing in the rfsw telnet server can be set using the **set telnet echo** command (A setting of “0” will disable the server echoing).
- The echo mode can be changed using the **set telnet echo** command. The default state for this command is “ON”. However, if the client supports **echo** options negotiations, it can over-ride the RF Switch echo setting.



### Note

The **set telnet echo** command is only available in Firmware 3.80 and later.

- Proper disconnect is essential to ending your Telnet session, and enabling Telnet access for the next session. Common Telnet disconnect methods are as follows:
  - Press **Ctrl+Break**.
  - Press **Ctrl+]**.
  - Type **quit** or **send break**.

Another Telnet disconnect method is as follows:

- Press **Ctrl+Shift 6 6 x**.
- Type **disc 1** from the router CLI.

**Note**

---

With Firmware 3.90 or later, typing the **quit** or **exit** command in a telnet session will cause the rfs w telnet server to close the connection.

---

For additional Telnet break sequences, refer to the document [Standard Break Key Sequence Combinations During Password Recovery](#) on Cisco.com.

# Installing Cisco RF Switch Firmware Version 3.92

As with previous Firmware upgrades on the Cisco RF Switch, the new Version 3.92 image can be downloaded and installed via TFTP using the COPY TFTP: command. This command can be applied from either the serial console port or a via a Telnet session.

One recommended procedure for installing the upgrade is as follows:

1. Copy the image to CMTS:

```
COPY TFTP: //<tftpserver-ip>/<userid>/1935030N.BIN BOOTFLASH:
```

2. Setup the tftp server on CMTS:

```
CONF T  
TFTP-SERVER BOOTFLASH:1935030N.BIN ALIAS 1935030N.BIN  
END
```

3. Setup RF Switch with tftp host, if not already set:

```
SET TFTP HOST <tftpserver-ip-addr>
```

4. Remove the password that has been set on the RF Switch, only if you are loading Version 3.80:

The CLI to remove password in Version 3.80 or later is:

```
NO ENABLE PASSWORD
```

The CLI to remove password in versions prior to 3.80 is:

```
NO SET PASSWORD
```

5. Install the new code update with the following command:

```
COPY TFTP:1935030N.BIN FLASH:
```

6. Reboot the Cisco RF Switch to run the new version of firmware:

```
REBOOT
```

7. Go to the enable prompt:

```
ENABLE
```

8. Install the new firmware image into the bootflash: using the new COPY command:

```
COPY TFTP:1935030N.BIN BOOTFLASH: NOVERIFY
```

9. Reboot the Cisco RF Switch to run the new version of firmware:

```
REBOOT
```

10. Set the password back on the RF Switch if you had removed it before upgrade. In Version 3.80 and later, the CLI to set enable password is:

```
ENABLE PASSWORD <password>
```

After the upgrade, the console will display the following warning message to show that changes have been made.

```
Recalling nvmem... ** nvmem default(s) used (0x0c) **  
**WARNING** The following non-volatile configuration memory area(s)  
**WARNING** have been modified or updated:  
Ethernet/IP  
SNMP
```

This procedure is subject to the changes and additional restrictions applied by the Field Notice in the following document on Cisco.com:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*  
[http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12\\_3bc/ubr10k\\_123bc\\_rn.html](http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html)

# Additional 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/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html</a></li> </ul>
Cisco RF Switch Firmware	<ul style="list-style-type: none"> <li>• <i>Release Notes for Cisco RF Switch Firmware, Version 3.92</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2929/products_documentation_roadmap09186a00801c9b9c.html">http://www.cisco.com/en/US/products/hw/cable/ps2929/products_documentation_roadmap09186a00801c9b9c.html</a></li> <li>• <i>Cisco RF Switch Firmware Command Reference Guide, Version 3.92</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2929/prod_command_reference09186a00807d75cf.html">http://www.cisco.com/en/US/products/hw/cable/ps2929/prod_command_reference09186a00807d75cf.html</a></li> <li>• <i>N+1 Redundancy for the Cisco CMTS</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.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/warp/public/770/fn19290.shtml">http://www.cisco.com/warp/public/770/fn19290.shtml</a></li> </ul>
Cisco RF Switch Hardware	<ul style="list-style-type: none"> <li>• <i>Cisco RF Switch Documentation Guide</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2929/products_documentation_roadmap09186a00801c9b9c.html">http://www.cisco.com/en/US/products/hw/cable/ps2929/products_documentation_roadmap09186a00801c9b9c.html</a></li> <li>• <i>Cisco RF Switch Installation and Cabling Guide</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2929/products_installation_guide_book09186a008007ca42.html">http://www.cisco.com/en/US/products/hw/cable/ps2929/products_installation_guide_book09186a008007ca42.html</a></li> <li>• <i>Cisco RF Switch Product Data Sheet</i>  <a href="http://www.cisco.com/univercd/cc/td/doc/pcat/rfswitch.htm">http://www.cisco.com/univercd/cc/td/doc/pcat/rfswitch.htm</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/products_documentation_roadmap09186a00805e0d0c.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_documentation_roadmap09186a00805e0d0c.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/products_documentation_roadmap09186a0080733a04.html">http://www.cisco.com/en/US/products/hw/cable/ps2209/products_documentation_roadmap09186a0080733a04.html</a></li> </ul>
High Availability References for Cisco Broadband Cable	<ul style="list-style-type: none"> <li>• <i>N+1 Redundancy for the Cisco CMTS</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html</a></li> <li>• <i>N+1 Tips and Configuration for the uBR 10012 Router with MC28C Cards</i>  <a href="http://www.cisco.com/warp/public/109/n_1_ubr10k_19135_1.html">http://www.cisco.com/warp/public/109/n_1_ubr10k_19135_1.html</a></li> <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>PacketCable and PacketCable Multimedia for the Cisco CMTS</i>  <a href="http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html</a></li> </ul>

Related Topic	Document Title
DOCSIS and EuroDOCSIS	<ul style="list-style-type: none"> <li>• <i>DOCSIS 1.1 for Cisco uBR7200 Series Universal Broadband Routers</i> <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121cx/docsis11.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121cx/docsis11.htm</a></li> <li>• <i>Internal DOCSIS Configurator File Generator for the Cisco Cable Modem Termination System</i> <a href="http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57d.html">http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57d.html</a></li> </ul>
Additional Broadband Cable Technical Reference	<ul style="list-style-type: none"> <li>• <i>Cisco Cable Solutions Home Page</i> <a href="http://cisco.com/warp/public/779/servpro/solutions/cable/">http://cisco.com/warp/public/779/servpro/solutions/cable/</a></li> <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>• <i>Cable Radio Frequency (RF) FAQs</i> <a href="http://www.cisco.com/warp/public/109/cable_faq_rf.html">http://www.cisco.com/warp/public/109/cable_faq_rf.html</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 release notes for additional information about standards supported by your specific CMTS equipment.

## MIBs

### MIBs for Cisco RF Switch Firmware Version 3.30

Access to the chassis line card configuration via SNMP requires the addition of the following new objects to the MIB database, summarized in [Table 5](#). Each of these objects has these three attributes:

- SYNTAX: OCTET STRING (SIZE(2))
- ACCESS: read-only
- STATUS: mandatory



#### Note

Because these objects are 16-bit hex integer bitmasks, in keeping with the conventions currently used in other bitmask values, they are declared as OCTET STRING (SIZE(2)).

**Table 5** *MIBs Objects Required with Firmware Version 3.30 and Later.*

Object	Description
nruCacheSnmpData	Value of <b>set snmp cache</b> command. A value of <b>1</b> in a bit position indicates that the caching is enabled. It is enabled by default.
nruUpstreamSlotConfig	Value of the <i>upstreamslots</i> parameter of the <b>set slot config</b> command. A value of <b>1</b> in a bit position indicates that the corresponding slot should expect an upstream linecard.
nruUpstreamSlotDetected	Results of line card enumeration. A value of <b>1</b> in a bit position indicates that an upstream linecard was detected in the slot. Normally, this value should equal nruUpstreamSlotConfig.
nruUpstreamSlotErrors	A value of <b>1</b> in any bit position indicates that there is a discrepancy between the configured versus the detected settings for the slot.
nruDnstreamSlotConfig	Value of the <i>dnstreamslots</i> parameter of the <b>set slot config</b> command. A value of <b>1</b> in a bit position indicates that the corresponding slot should expect a downstream line card.
nruDnstreamSlotDetected	Results of line card enumeration. A value of <b>1</b> in a bit position indicates that a downstream linecard was detected in the slot. Normally, this value should equal nruDnstreamSlotConfig.
nruDnstreamSlotErrors	A value of <b>1</b> in any bit position indicates that there is a discrepancy between the configured versus the detected settings for the slot.

**Additional MIB Information**

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.

**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/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.