Release Notes for Cisco uBR7100 Series for Cisco IOS Release 12.2 BC

November 2, 2005
Cisco IOS Release 12.2(15)BC2i
OL-2774-20

These release notes for the Cisco uBR7100 series universal broadband routers document the cable-specific, early deployment 12.2 BC train, describing the enhancements and caveats provided in Cisco IOS Release 12.2(15)BC2i. This release includes features in previous Cisco IOS 12.2BC Releases. Cisco IOS Release 12.2(15)BC2g is a child of Cisco IOS Release 12.2(15)T.

The 12.2 BC train is an interim release train that provides DOCSIS 1.1 two-way support, along with support for selected new features. Cisco IOS Release 12.2(15)BC2i provides a migration path from the earlier 12.2 XF releases, which included a selected subset of the features supported for the Cisco uBR7100 series routers in Cisco IOS Release 12.0 SC, Cisco IOS Release 12.1 EC, and Cisco IOS Release 12.1(7)CX1.

These release notes are updated with each release in the train. For a list of the software caveats that apply to Cisco IOS Release 12.2(15)BC2i, see the "Caveats" section on page 66 and *Caveats for Cisco IOS Release 12.2 T.* Use these release notes in conjunction with the cross-platform *Release Notes for Cisco IOS Release 12.2* T located on Cisco.com and the Documentation CD-ROM.

Note Cisco IOS Release 12.2(15)BC2i does not include support for telco-return images.

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/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.

Cisco Systems

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

Contents

These release notes describe the following topics:

Inheritance Information

Cisco IOS Release 12.2(15)BC2i is an early deployment release that is a child of Cisco IOS Release 12.2(15)T. All features in Cisco IOS Release 12.2(15)T and specifically all features and caveats in Cisco IOS Release 12.2(15)T6 are in Cisco IOS Release 12.2(15)BC2i.

Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.2 T

Topic	Location
• Determining the Software Version • Upgrading to a New Software Release	To view information about the topics in the left-hand column, click **Cross-Platform System Requirements** at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122treqs.htm
• New and Changed Information (Feature Descriptions) • MIBs • Important Notes	To view information about the topics in the left-hand column. For Cisco IOS Release 12.2 T, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tnewf.htm Scroll down and click **New Hardware and Software Features in Cisco IOS Release 12.2(15)T**, or **MIBs**, or **Important Notes**.
• Related Documentation • Obtaining Documentation • Obtaining Technical Assistance	To view information about the topics in the left-hand column, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tdocs.htm

Introduction

For information on new features and the Cisco IOS documentation set supported by Cisco IOS Release 12.2(15)BC2i, see the "New and Changed Information" section on page 19 and the "Related Documentation" section on page 169.

Overview of Cisco Universal Broadband Routers

The Cisco uBR7100 series universal broadband routers—the Cisco uBR7111, Cisco uBR7111E, Cisco uBR7114, and Cisco uBR7114E—are based on the Data-over-Cable Service Interface Specification (DOCSIS) standards and designed to be installed at small cable operators and multiple dwelling unit (MDU) operators to enable them to offer services such as e-mail, high-speed Internet access, voice, and digital video over a bidirectional cable television and IP backbone network. The universal broadband routers function as the cable modem termination system (CMTS) for subscriber-end devices such as Cisco uBR905, Cisco uBR924, and Cisco uBR925 cable access routers, and other DOCSIS-compliant cable modems (CMs) and set-top boxes (STBs).

Both the Cisco uBR7100 series and Cisco uBR7200 series universal broadband routers allow two-way transmission of digital data and Voice over IP (VoIP) traffic over a hybrid fiber-coaxial (HFC) network. The Cisco uBR7100 series routers support IP routing with a wide variety of protocols and WAN interfaces selections.

Cisco IOS Release 12.2(15)BC2i supports the Cisco uBR7111, Cisco uBR7111E, Cisco uBR7114, and Cisco uBR7114E universal broadband routers.

Cisco uBR7100 Series Universal Broadband Routers

The Cisco uBR7100 series routers provide a fixed set of WAN and LAN interfaces with a combination of fixed and modular interfaces, allowing both flexibility and simplicity in configuration. Each Cisco uBR7100 series router includes one modular single-width port adapter, one integrated cable interface with an internal upconverter, and two integrated Fast Ethernet ports. The cable interface is based on the Cisco uBR-MC14C cable interface line card and is not field-replaceable.

The Cisco uBR7100 series routers support IP routing through the following optional WAN and LAN port adapters: Ethernet, Fast Ethernet, serial, High-Speed Serial Interface (HSSI), Packet over SONET (POS) OC-3c, and Asynchronous Transfer Mode (ATM) media. For more information, see Table 6 on page 12.

Depending on the model, the Cisco uBR7100 series routers support the following two standards:

- Data Over Cable Service Interface Specifications (DOCSIS), which supports the 6 MHz North American channel plans using the ITU J.83 Annex B RF standard. The downstream uses a 6 MHz channel width in the 85 to 860 MHz frequency range, and the upstream supports the 5 to 42 MHz frequency range.
- European Data Over Cable Service Interface Specifications (EuroDOCSIS), which supports the 8 MHz Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) channel plans using the ITU J.112 Annex A RF standard. The downstream uses an 8 MHz channel width in the 85 to 860 MHz frequency range, and the upstream supports multiple channel widths in the 5 to 65 MHz frequency range.

The Cisco uBR7100 series offers the following models:

- The Cisco uBR7111 and Cisco uBR7111E universal broadband routers provide a cable interface with one downstream port and one upstream port. The downstream port can be output either as an RF signal through the integrated upconverter or as an IF signal for processing by an external upconverter. The Cisco uBR7111 router supports DOCSIS cable plants, and the Cisco uBR7111E supports EuroDOCSIS cable plants.
- The Cisco uBR7114 and Cisco uBR7114E universal broadband routers provide a cable interface with one downstream port and four upstream ports. The downstream port can be output either as an RF signal through the integrated upconverter or as an IF signal for processing by an external upconverter. The Cisco uBR7114 router supports DOCSIS cable plants, and the Cisco uBR7114E supports EuroDOCSIS cable plants.

Cisco uBR7111 and Cisco uBR7111E Universal Broadband Routers

The Cisco uBR7111 and Cisco uBR7111E provide the following major hardware features:

- Integrated network processing engine
- 1 upstream cable modem interface
- 1 downstream cable modem interface
- 2 Fast Ethernet ports
- 1 port adapter slot
- 1 service adapter slot
- 1 AC power supply
- 1 Personal Computer Memory Card International Association (PCMCIA) slot that allows for software upgrades through the use of Flash memory cards

Cisco uBR7114 and Cisco uBR7114E Universal Broadband Routers

The Cisco uBR7114 and Cisco uBR7114E provide the following major hardware features:

- Integrated network processing engine
- 1 downstream cable modem interface
- 4 upstream cable modem interfaces
- 2 Fast Ethernet ports
- 1 port adapter slot
- 1 service adapter slot
- 1 AC power supply
- 1 Personal Computer Memory Card International Association (PCMCIA) slot that allows for software upgrades through the use of Flash memory cards

Universal Broadband Router Overview

Table 2 provides a quick overview of the major hardware features of the two universal broadband routers.

Table 2 Universal Broadband Router Overview

Supported Hardware	Cisco uBR7111, Cisco uBR7111E	Cisco uBR7114, Cisco uBR7114E
Upstream Cable Modem Interfaces	1	4
Downstream Cable Modem Interfaces	1	1
Fast Ethernet Ports	2	2
Port Adapter Slots	1	1
Service Adapter Slots	1	1
Power Supplies	1	1
PCMCIA Slots	1	1

Early Deployment Releases

These release notes describe the Cisco uBR7100 series universal broadband routers for Cisco IOS Release 12.2(15)BC2i. Release 12.2 XF is an early deployment (ED) release based that contains fixes to software caveats as well as support for new Cisco hardware and software features. Feature support is cumulative from release to release, unless otherwise noted.

Cisco IOS Release 12.2(15)BC2i supports a selected subset of the hardware and software features that were released in Cisco IOS Release 12.1 EC for the Cisco uBR7100 series universal broadband routers. Table 3 lists the features supported by the Cisco uBR7100 series in Cisco IOS Release 12.2(15)BC2i.

Table 3 Early Deployment (ED) Releases for the Cisco uBR7100 Series

ED Release	Software Features[1] and MIBs[2]	Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)BC2i	None	None	—
Cisco IOS Release 12.2(15)BC2h	None	None	—
Cisco IOS Release 12.2(15)BC2g	None	None	—
Cisco IOS Release 12.2(15)BC2f	None	None	—
Cisco IOS Release 12.2(15)BC2e	None	None	—
Cisco IOS Release 12.2(15)BC2c	None	None	—
Cisco IOS Release 12.2(15)BC2b	• Cable Arp Filter Enhancement • Show Controllers Cable Extensions • Source Verify Lease-Query Throttling	None	—

Table 3 Early Deployment (ED) Releases for the Cisco uBR7100 Series (continued)

ED Release	Software Features[1] and MIBs[2]	Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)BC2a	None	None	—
Cisco IOS Release 12.2(15)BC2	• Cable ARP Filter • CISCO-NBAR-PROTOCOL-DISCOVERY-MIB • Command-Line Interface (CLI) Enhancements • DOCS-IF-MIB Update • DOCSIS Set-Top Gateway • Extended Upstream Frequency Ranges • IEEE 802.1Q Transparent Lan Service • N+1 Support for Load Balancing • PacketCable Enhancements • Vendor-Specific Information Field to Authorize Dynamic Service Requests	None	—
Cisco IOS Release 12.2(15)BC1g	• None	None	—
Cisco IOS Release 12.2(15)BC1f	• None	None	—
Cisco IOS Release 12.2(15)BC1d	• Source Verify Lease-Query Throttling	None	—
Cisco IOS Release 12.2(15)BC1c	• Cable ARP Filter	None	—
Cisco IOS Release 12.2(15)BC1b	None	None	—
Cisco IOS Release 12.2(15)BC1a	None	None	—
Cisco IOS Release 12.2(15)BC1	• Command-Line Interface Enhancements • Dynamic Shared Secret • Nonstop Forwarding (NSF) Awareness—BGP, OSPF, and Integrated IS-IS • Subscriber Traffic Management • Support for Cisco Broadband Troubleshooter Version 3.0	None	—
Cisco IOS Release 12.2(11)BC3d	None	None	—
Cisco IOS Release 12.2(11)BC3c	None	None	—

Table 3 Early Deployment (ED) Releases for the Cisco uBR7100 Series (continued)

ED Release	Software Features[1] and MIBs[2]	Hardware Features	Hardware Availability
Cisco IOS Release 12.2(11)BC3b	None	None	—
Cisco IOS Release 12.2(11)BC3	• Transparent LAN Service over Cable • **clear cable modem** Commands • **debug cable** Commands	None	—
Cisco IOS Release 12.2(11)BC2	None	None	—
Cisco IOS Release 12.2(11)BC1b	None	None	—
Cisco IOS Release 12.2(11)BC1a	None	None	—
Cisco IOS Release 12.2(11)BC1	• Support for the **cable source-verify leasetimer** Command	None	—
Cisco IOS Release 12.2(8)BC2a	None	None	—
Cisco IOS Release 12.2(8)BC2	• Adding Load Information and a Timestamp to Show Commands • Display Modem Capabilities with the **show cable modem mac** Command • Support for the **cable modem vendor** Command • Support for the **cable tftp-enforce** Command • Support for a Secondary Shared Secret • Enhancement to the **show hccp brief** Command • Enhancement to the **cable filter group** Command	None	—
Cisco IOS Release 12.2(8)BC1	• EXEC Commands in Configuration Mode • Secure Shell (SSH)	• Support for the PA-A3-E3 port adapter card	Now
Cisco IOS Release 12.2(4)BC1b	• Baseline Privacy Interface Plus (BPI+) • Cisco IOS Network-Based Application Recognition (NBAR) • Turbo ACL • SNMP Cable Modem Remote Query	None	—
Cisco IOS Release 12.2(4)BC1	• PPPoE[3] Termination	• Support for PA-T3+ and PA-2T3+ port adapters	Now

Table 3 Early Deployment (ED) Releases for the Cisco uBR7100 Series (continued)

ED Release	Software Features[1] and MIBs[2]	Hardware Features	Hardware Availability
Cisco IOS Release 12.2(4)XF1	• DOCSIS 1.0 Support • DOCSIS 1.0+ Support • DOCSIS 1.1 Support, including: – TLV[4] Parser Support – BE[5], UGS[6], UGS-AD[7], rtPS[8] Service Flows – DSC[9] Service Flow, Classifier, and PHS[10] – Fragmentation – Concatenation – PHS – DS[11] Classification and Queuing • Cable Intercept Command • Cable Interface Setup Facility • DHCP/TOD/TFTP[12] Server Support • Cable Subinterface Support • Access Lists • Spectrum Management and Dynamic Upstream Modulation • Cable Source Verification Feature • MPLS[13] VPN[14] Support for Subinterfaces • Dynamic Mobile Hosts Feature • IP NAT/PAT[15] Translation • Internal Modem Configuration File Editor • Cable Flap List • Cable ARP[16] and Proxy ARP Support • Cable Downstream Frequency Override CLI[17] • MAX-CPE CLI override	None	Now

1. Only major features are listed.
2. MIB = Management Information Base
3. PPPoE = Point-to-Point Protocol over Ethernet
4. TLV = Type/Length/Value
5. BE = Best Effort
6. UGS = Unsolicited Grant Service
7. UGS-AD = Unsolicited Grant Service with Activity Detection
8. rtPS = Real-Time Polling Service
9. DSC = Dynamic Service Change

10. PHS = Payload Header Suppression
11. DS = Downstream
12. DHCP = Dynamic Host Configuration Protocol, TOD = Time of Day, TFTP = Trivial File Transfer Protocol
13. MPLS = Multiprotocol Label Switching
14. VPN = Virtual Private Network
15. NAT/PAT = Network Address Translation/Port Address Translation
16. ARP = Address Resolution Protocol
17. CLI = command line interface

Unsupported Features

Table 4 lists the features that are not supported in Cisco IOS Release 12.2(15)BC2i, along with the most recent, recommended Cisco IOS Release that does support that particular feature for the Cisco uBR7100 series routers.

Table 4 Features Not Supported in Cisco IOS Release 12.2(15)BC2i

Software or Hardware Feature	Supported Cisco IOS Release
MxU Bridging over the Cable Interface	Release 12.1(10)EC
Cable Downstream Frequency Command	Release 12.1(10)EC
Telco-Return Support	Release 12.1(10)EC
Web Cache Communication Protocol	Not supported for the Cisco uBR7100 series

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(15)BC2i and includes the following sections:

Memory Recommendations

Table 5 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7100 series universal broadband routers for Cisco IOS Release 12.2(15)BC2i. Cisco uBR7100 series routers are available with a 16-MB or 20-MB Type II PCMCIA Flash memory card.

Table 5 Memory Recommendations for the Cisco uBR7100 Series Routers, Cisco IOS Release 12.2(15)BC2i Feature Sets

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Two-Way Data/VoIP Images				
DOCSIS Two-Way	ubr7100-p-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus	ubr7100-is-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way with BPI	ubr7100-k8p-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus with BPI	ubr7100-ik8s-mz	16 MB Flash	128 MB DRAM	RAM
Boot Image				
UBR7100 Boot Image	ubr7100-boot-mz	None	None	—

The image subset legend for Table 5 is as follows:

- i = IP routing, MPLS-VPN support, and noncable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy and MPLS-VPN support
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no NAT
- s = “Plus” features: NAT and Inter-Switch Link (ISL)

Note All images support all of the hardware listed in the “Supported Hardware” section on page 12, unless otherwise indicated.

System Interoperability

This section clarifies the operation of certain features in the Cisco uBR7100 series universal broadband routers.

- DOCSIS 1.0 Baseline Privacy

  DOCSIS baseline privacy interface (BPI) gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and CM. BPI ensures that a CM, uniquely identified by its Media Access Control (MAC) address, can obtain keying material for only those services to which it has authorized access.

  To enable BPI, choose software at both the CMTS and CM that support the mode of operation. For the Cisco uBR7100 series software, choose an image with "k8" in its file name or BPI in the feature set description.

  The CM must also support BPI. CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment. BPI must be enabled using the DOCSIS configuration file.

  

  Note RSA stands for Rivest, Shamir, and Adelman, inventors of a public-key cryptographic system.

- CM Interoperability

  The Cisco uBR7100 series interoperates with DOCSIS (Cisco uBR7111 and Cisco uBR7114) or Euro-DOCSIS (Cisco uBR7111E and Cisco uBR7114E) two-way CMs that support basic Internet access, VoIP, or Virtual Private Networks (VPNs). Cisco IOS Release 12.2(15)BC2i does not support telco-return CMs/STBs.

  Also, if you have configured a Cisco cable modem for routing mode and are also using the **cable-modem dhcp-proxy nat** command on the cable modem, you must configure the corresponding cable interface on the Cisco uBR7100 series router with the **cable dhcp-giaddr policy** command. Otherwise, the cable interface could flap and the CM could go offline unpredictably.

- DOCSIS 1.0 Extensions

  The Cisco uBR7100 series supports the following DOCSIS 1.0 quality of service (QoS) extensions:

  – Multi-Service ID (SID) support, allowing the definition of multiple SIDs on the upstream—Voice traffic can be designated on a higher QoS committed information rate (CIR) secondary SID, while data traffic can be forwarded on a best-effort basis on a primary SID. Secondary SIDs are higher QoS CIR-type classes that have a nonzero minimum reserved rate (CIR-type service). These SIDs receive preferential treatment at the CMTS for grants over any tiered best-effort type data SID of that upstream. Reliable operation with voice requires multiple SIDs—at least two per CM to separate voice from data. In DOCSIS 1.0, SIDs are set up statically. When supporting DOCSIS 1.0 extensions, SIDs can be set up statically or dynamically. Both the CMTS and CM must support this capability.

  – CM-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted at run-time on a per-VoIP call basis.

  – Unsolicited grant service (constant bit rate [CBR] scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.

– Ability to provide separate downstream rates for any given ITCM, based on the IP-precedence value in the packet—This helps separate voice signaling and data traffic that goes to the same ITCM to address rate-shaping purposes.

– Concatenation—To increase the per-CM upstream throughput in certain releases of software, Cisco uBR7100 series software supports a concatenated burst of multiple MAC frames from a CM that supports concatenation.

Note All DOCSIS 1.0 extensions are activated only when a CM or Cisco uBR924 that supports these extensions solicits services via dynamic MAC messages or the feature set. If the CMs in your network are pure DOCSIS 1.0-based, they will receive regular DOCSIS 1.0 treatment from the CMTS.

Supported Hardware

Cisco IOS Release 12.2(15)BC2i supports the following Cisco uBR7100 series routers:

- Cisco uBR7111
- Cisco uBR7114
- Cisco uBR7111E
- Cisco uBR7114E

Port Adapter Cards

Table 6 lists and describes the port adapters supported by Cisco uBR7100 series routers in Cisco IOS Release 12.2(15)BC2i.

Note Table 6 identifies some port adapters for the Cisco uBR7100 series routers that are in an end-of-life (EOL) stage.

Table 6 Cisco uBR7100 Series Port Adapter Releases

WAN Technology	Product Number and Description	Introduced in Release[1]	End-of-Life
Ethernet			
	PA-4E—4-port Ethernet 10BASE-T port adapter	12.2(4)XF1	No
	PA-8E—8-port Ethernet 10BASE-T port adapter	12.2(4)XF1	Yes
Fast Ethernet			
	PA-FE-TX—1-port 100BASE-TX Fast Ethernet port adapter	12.2(4)XF1	No
	PA-FE-FX—1-port 100BASE-FX Fast Ethernet port adapter	12.2(4)XF1	No
	PA-2FE-TX—2-port 100BASE-TX Fast Ethernet port adapter	12.2(4)XF1	No

Table 6 Cisco uBR7100 Series Port Adapter Releases (continued)

WAN Technology	Product Number and Description	Introduced in Release[1]	End-of-Life
	PA-2FE-FX—2-port 100BASE-FX Fast Ethernet port adapter	12.2(4)XF1	No
Serial			
	PA-E3—1-port high-speed serial E3 interface port adapter	12.2(4)XF1	No
	PA-T3—1-port T3 serial interface port adapter	12.2(4)XF1	No
	PA-T3+—1-port T3 serial interface port adapter enhanced	12.2(4)BC1	No
	PA-2E3—2-port high-speed serial E3 interface port adapter	12.2(4)XF1	No
	PA-2T3—2-port T3 serial interface port adapter	12.2(4)XF1	No
	PA-2T3+—2-port T3 serial interface port adapter enhanced	12.2(4)BC1	No
	PA-4T+—4-port synchronous serial port adapter	12.2(4)XF1	No
	PA-4E1G-75—4-port unbalanced (75-ohm) E1-G.703/G.704 synchronous serial port adapter	12.2(4)XF1	No
	PA-4E1G-120—4-port balanced (120-ohm) E1-G.703/G.704 synchronous serial port adapter	12.2(4)XF1	No
	PA-8T-232—8-port EIA/TIA-232 synchronous serial port adapter	12.2(4)XF1	Yes
	PA-8T-V35—8-port V.35 synchronous serial port adapter	12.2(4)XF1	No
	PA-8T-X21—8-port X.21 synchronous serial port adapter	12.2(4)XF1	Yes
	PA-MC-2T1—2-port multichannel DS1 Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) single-wide port adapter	12.2(4)XF1	Yes
	PA-MC-4T1—4-port multichannel DS1 ISDN PRI single-wide port adapter	12.2(4)XF1	No
HSSI			
	PA-H—1-port HSSI port adapter	12.2(4)XF1	Yes
	PA-2H—2-port HSSI port adapter	12.2(4)XF1	No
ATM			

Table 6 Cisco uBR7100 Series Port Adapter Releases (continued)

WAN Technology	Product Number and Description	Introduced in Release[1]	End-of-Life
	PA-A3-E3—1-port E3 ATM, PCI-based, single-width port adapter, that uses an E3 interface with a coaxial cable BNC connector	12.2(8)BC1	No
	PA-A3-OC3MM—1-port OC-3c ATM, PCI-based multimode port adapter	12.2(4)XF1	No
	PA-A3-OC3SMI—1-port OC-3c ATM, PCI-based single-mode intermediate reach port adapter	12.2(4)XF1	Yes
	PA-A3-OC3SML—1-port OC-3c ATM, PCI-based single-mode long reach port adapter	12.2(4)XF1	No
	PA-A3-8T1/IMA—ATM inverse multiplexer over ATM port adapter with 8 T1 ports	12.2(4)XF1	No
Packet over SONET	PA-POS-OC3SMI—1-port OC3 single-mode, intermediate reach port adapter	12.2(4)XF1	No

1. The number in this column indicates the Cisco IOS release in which the interface was introduced in this train.

Determining Your Software Release

To determine the version of Cisco IOS software running on the Cisco uBR7100 series universal broadband router, log in to the router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 BC Software (ubr7100-k8p-mz), Version 12.2(15)BC2i, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* located at http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Table 7 lists the features and feature sets supported by the Cisco uBR7100 series in Cisco IOS Release 12.2(15)BC2i and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced (excluding deferred images). Cisco IOS Release 12.2(4)XF1 is the base release; all features, unless otherwise noted, were introduced in this release.

Note Table 7 might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.2(15)BC2i by using the Feature Navigator tool at http://www.cisco.com/go/fn.

Table 7 Feature List by Feature Sets for Cisco uBR7100 Series Universal Broadband Routers

	Feature Set		
Feature	**In[1]**	**DOCSIS Two-way with BPI**	**DOCSIS Two-way IP Plus with BPI**
IP Routing			
DHCP[2] Server		Yes	Yes
DRP[3] Server Agent		Yes	Yes
Easy IP (Phase 1)		Yes	Yes
Hot-Standby 1+1 Redundancy		No	No
HSRP[4] over ISL[5] in Virtual LAN Configurations		No	No
IP Type of Service and Precedence for GRE[6] Tunnels		Yes	Yes
IP Enhanced IGRP[7] Route Authentication		Yes	Yes
MxU Bridging		No	No
Nonstop Forwarding (NSF) Awareness—BGP, OSPF, and Integrated IS-IS	12.2(15)BC1	Yes	Yes
Per-Modem Filters		Yes	Yes
PPPoE Termination		Yes	Yes
Transparent LAN Service over Cable	12.2(11)BC3	Yes	Yes
Management			
Cable Interface Setup Facility		Yes	Yes

Table 7 Feature List by Feature Sets for Cisco uBR7100 Series Universal Broadband Routers

Feature	Feature Set		
	In[1]	DOCSIS Two-way with BPI	DOCSIS Two-way IP Plus with BPI
Cisco Broadband Troubleshooter Version 3.0 Support	12.2(15)BC 1	Yes	Yes
Cisco Call History MIB Command Line Interface		Yes	Yes
DOCSIS Ethernet MIB Objects Support (RFC 2665)		Yes	Yes
DOCSIS OSSI[8] Objects Support (RFC 2233)		Yes	Yes
Dynamic Ranging Support		Yes	Yes
Enhanced Modem Status Display		Yes	Yes
Enhanced Per-Modem Error Counter		Yes	Yes
Internal Modem Configuration File Editor		Yes	Yes
LinkUp/Down Traps Support (RFC 2233)		Yes	Yes
RF Interface MIB		Yes	Yes
SNMPv2C[9] and SNMPv3[10]		Yes	Yes
Multimedia			
Bidirectional PIM[11]		No	No
IP Multicast Load Splitting Across Equal-Cost Paths		No	No
IP Multicast over ATM[12] Point-to-Multipoint Virtual Circuits		No	No
IP Multicast over Token Ring LANs		No	No
Stub IP Multicast Routing		No	No
Quality of Service			
252 Operator Configurable QoS Service Profiles for DOCSIS 1.0		Yes	Yes
Admission Control for Load Balancing		Yes	Yes
Admission Control (Including Weighting Functions per QoS Profile)		Yes	Yes
DOCSIS 1.0 Configuration File Editor (IOS CLI-based)		Yes	Yes
Dynamic Upstream Modulation		Yes	Yes
DOCSIS 1.0+[13] QoS Enhancements		Yes	Yes
Downstream QoS Handling		Yes	Yes
Downstream Traffic Shaping		Yes	Yes
Dynamic SID Support		Yes	Yes
Dynamic Map-Advance		Yes	Yes
Guaranteed Upstream Minimum Throughput per Modem for DOCSIS 1.0		Yes	Yes

Table 7 Feature List by Feature Sets for Cisco uBR7100 Series Universal Broadband Routers

Feature	Feature Set		
	In[1]	DOCSIS Two-way with BPI	DOCSIS Two-way IP Plus with BPI
Improved Upstream QoS		Yes	Yes
Multiple SID Support for DOCSIS 1.0+		Yes	Yes
Multiple SID Support for DOCSIS 1.1		Yes	Yes
Multiple SID Support (static only)		Yes	Yes
QoS Configuration		Yes	Yes
QoS Profile Enforcement		Yes	Yes
QoS Profile Management via SNMP, CLI, or Dynamic		Yes	Yes
RTP[14] Header Compression		Yes	Yes
Subscriber Traffic Management	12.2(15)BC 1	Yes	Yes
Telco Return		No	No
Time of Day (ToD) Server		Yes	Yes
TOS Bit Restamping and TOS-based QoS for DOCSIS 1.0		Yes	Yes
Upstream Address Verification		Yes	Yes
Upstream Traffic Shaping		Yes	Yes
Security			
Automated Double Authentication		Yes	Yes
BPI and BPI+ Encryption		Yes	Yes
Cable Modem and Multicast Authentication using RADIUS[15]		No	No
Cable source-verify		Yes	Yes
Cable source-verify DHCP (Including lease-query)		Yes	Yes
Cisco IOS Firewall Enhancements		Yes	Yes
Dynamic Mobile Hosts		Yes	Yes
Dynamic Shared Secret	12.2(15)BC 1	Yes	Yes
HTTP[16] Security		Yes	Yes
Named Method Lists for AAA[17] Authorization & Accounting		Yes	Yes
Per-Modem and Per-Host Access List Support		Yes	Yes
Per-User Configuration		Yes	Yes
Reflexive Access Lists		Yes	Yes
Secure Shell (SSH)		Yes	Yes

Table 7 Feature List by Feature Sets for Cisco uBR7100 Series Universal Broadband Routers

Feature	Feature Set		
	In[1]	DOCSIS Two-way with BPI	DOCSIS Two-way IP Plus with BPI
SNMP Access Lists (Including Logging Feature)		Yes	Yes
TACACS+		Yes	Yes
TFTP-enforce		Yes	Yes
Vendor-Proprietary RADIUS Attributes		No	No
Switching			
Fast-Switched Policy Routing		Yes	Yes
VPN			
MPLS VPN Support for Subinterfaces		Yes	Yes
WAN Optimization			
PAD[18] Subaddressing		Yes	Yes
WAN Services			
Bandwidth Allocation Control Protocol (BACP)		Yes	Yes
Enhanced Local Management Interface (ELMI)		Yes	Yes
Frame Relay Enhancements		Yes	Yes
Frame Relay MIB Extensions		Yes	Yes
Frame Relay Router ForeSight		Yes	Yes
ISDN[19] Advice of Charge		Yes	Yes
ISDN Caller ID Callback		Yes	Yes
ISDN Multiple Switch Type		Yes	Yes
ISDN NFAS[20]		Yes	Yes
Microsoft Point-to-Point Compression (MPPC)		Yes	Yes
National ISDN Switch Types for BRI[21] and PRI[22]		Yes	Yes
VPDN[23] MIB and Syslog Facility		Yes	Yes
X.25 Enhancements		Yes	Yes
X.25 Switching Between PVCs[24] and SVCs[25]		Yes	Yes

1. The number in the “In” column indicates the Cisco IOS release in which the feature was introduced in this release train. If a cell in this column is empty, the feature was included in the initial base release.
2. DHCP = Dynamic Host Configuration Protocol
3. DRP = Director Response Protocol
4. HSRP = Hot-Standby Routing Protocol
5. ISL = Inter-Switch Link
6. GRE = generic routing encapsulation
7. IGRP = Interior Gateway Routing Protocol
8. OSSI = Operations Support System Interface
9. SNMPv2 = Simple Network Management Protocol version 2
10. SNMPv3 = Simple Network Management Protocol version 3

11. PIM = Protocol Independent Multicast
12. ATM = Asynchronous Transfer Mode
13. The DOCSIS 1.0+ QoS Enhancements is a set of Cisco's Quality of Service extensions to DOCSIS 1.0 to enable basic VoIP service over the DOCSIS link before DOCSIS 1.1 becomes available. The main enhancements include support for dynamic creation and teardown of flows during voice calls, support for one new unsolicited grant service (UGS) slot scheduling mechanism for voice slots, and per IP-precedence rate shaping on the downstream.
14. RTP = Real-Time Transport Protocol
15. RADIUS = Remote Access Dial-In User Service
16. HTTP = Hypertext Transfer Protocol
17. AAA =authentication, authorization, and accounting
18. PAD = packet assembler/disassembler
19. ISDN = Integrated Services Digital Network
20. NFAS = non-facility-associated signaling
21. BRI = Basic Rate Interface
22. PRI = Primary Rate Interface
23. VPDN = virtual private dial-up network
24. PVC = permanent virtual circuit
25. SVC = switched virtual circuit

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco uBR7100 series routers for Cisco IOS Release 12.2(15)BC2i. These sections also show the features inherited from Release 12.2(4)XF1 and other earlier releases.

No New Hardware Features in Release 12.2(15)BC2i

There are no new hardware features in Cisco IOS Release 12.2(15)BC2i.

New Software Features in Release 12.2(15)BC2i

There are no new software features in Cisco IOS Release 12.2(15)BC2i.

No New Hardware Features in Release 12.2(15)BC2h

There are no new hardware features in Cisco IOS Release 12.2(15)BC2h.

New Software Features in Release 12.2(15)BC2h

There are no new software features in Cisco IOS Release 12.2(15)BC2h.

No New Hardware Features in Release 12.2(15)BC2g

There are no new hardware features in Cisco IOS Release 12.2(15)BC2g.

New Software Features in Release 12.2(15)BC2g

There are no new software features in Cisco IOS Release 12.2(15)BC2g.

No New Hardware Features in Release 12.2(15)BC2f

There are no new hardware features in Cisco IOS Release 12.2(15)BC2f.

New Software Features in Release 12.2(15)BC2f

There are no new software features in Cisco IOS Release 12.2(15)BC2f.

No New Hardware Features in Release 12.2(15)BC2e

There are no new hardware features in Cisco IOS Release 12.2(15)BC2e.

New Software Features in Release 12.2(15)BC2e

There are no new software features in Cisco IOS Release 12.2(15)BC2e.

No New Hardware Features in Release 12.2(15)BC2c

There are no new hardware features in Cisco IOS Release 12.2(15)BC2c.

New Software Features in Release 12.2(15)BC2c

There are no new software features in Cisco IOS Release 12.2(15)BC2c.

No New Hardware Features in Release 12.2(15)BC2b

There are no new hardware features in Cisco IOS Release 12.2(15)BC2b.

New Software Features in Release 12.2(15)BC2b

The following software features are new in Cisco IOS Release 12.2(15)BC2b.

Cable Arp Filter Enhancement

The ip-requests-filtered option was added to the show cable arp-filter command to display the specific Service IDs (SIDs) that are generating or forwarding a minimum number of ARP packets.

Show Controllers Cable Extensions

The Show Controllers Cables Extensions feature has been supported for Cisco IOS Release 12.2(15)BC2b.

In this feature, the mem-stats, memory, proc-cpu, and tech-support keywords execute the related command on the processor that runs on are added to obtain the relevant information from the onboard processor on Broadband Processing Engine (BPE) cable interface line cards, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards. This allows the user to obtain information that is specific for that particular cable interface card, as opposed to having to run these commands on the entire router.

Source Verify Lease-Query Throttling

When the cable source-verify dhcp and no cable arp commands are configured on a cable interface, problems can occur when viruses, denial of service (DoS) attacks, and theft-of-service attacks begin scanning a range of IP addresses, in an attempt to find unused addresses. When the Cisco CMTS router is verifying unknown IP addresses, this type of scanning generates a large volume of DHCP lease queries, which can result in a number of problems, such as dropped packets and high CPU utilization of both the Cisco CMTS router and DHCP server.

To prevent these problems, you can enable filtering of these requests on upstream interfaces, downstream interfaces, or both. When this feature is enabled, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests for each service ID (SID) on an interface within the configured interval time period. If a SID generates more lease queries than the maximum, the router drops the excess number of requests until the next interval period begins.

For more information on this feature, see the document “Filtering Cable DHCP Lease Queries”, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cblsrcvy.htm

Note The Source Verify Lease-Query Throttling feature is only available in Cisco IOS Release 12.2(15)BC1d and Cisco IOS Release 12.2(15)BC2b.

No New Hardware Features in Release 12.2(15)BC2a

There are no new hardware features in Cisco IOS Release 12.2(15)BC2a.

No New Software Features in Release 12.2(15)BC2a

There are no new software features in Cisco IOS Release 12.2(15)BC2a

No New Hardware Features in Release 12.2(15)BC2

There are no new hardware features in Cisco IOS Release 12.2(15)BC2.

New Software Features in Release 12.2(15)BC2

The following software features are new in Cisco IOS Release 12.2(15)BC2.

Cable ARP Filter

Cisco IOS Release 12.2(15)BC2 adds support for the **cable arp filter** command, which enables service providers to filter ARP request and reply packets, to prevent a large volume of such packets from interfering with the other traffic on the cable network. For more information, see the *Cable ARP Filtering* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cblarpfl.htm

CISCO-NBAR-PROTOCOL-DISCOVERY-MIB

Cisco IOS Release 12.2(15)BC2 adds support for the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB to the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers. This allows service providers to use SNMP requests to configure and monitor the Network-Based Application Recognition (NBAR) feature.

For more information about NBAR, see the *Network-Based Application Recognition and Distributed Network-Based Application Recognition* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

For more information about the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB, see the *Network-Based Application Recognition Protocol Discovery Management Information Base* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftpdmib.htm

Command-Line Interface (CLI) Enhancements

Cisco IOS Release 12.2(15)BC2 has enhanced or updated the following commands:

- **cable dhcp-giaddr**—Supports a new option, **strict**, that uses the GIADDR IP address as the source IP address in the forwarded DHCP OFFER packet, when using the **policy** option. By default, the Cisco CMTS changes the source IP address in the DHCPOFFER packet to match that of the primary address on the cable interface. Use the **strict** option to prevent this behavior, which could interfere with any access lists applied to the CM when the CM is using a different subnet from the cable interface's primary address space.

Caution You cannot use the **strict** option with the internal DHCP server that is onboard the Cisco CMTS router, because the **strict** option requires the use of DHCP relay operation, which is not performed by DHCP termination points such as the internal DHCP server.

- **cable downstream frequency**—Changed to allow the center frequency to be set only in 250 KHz increments. Previously, this command allowed the center frequency to be specified in 125 KHz increments, but this had to be changed to support all of the operational modes of the Broadband Processing Engine (BPE) cards that include integrated onboard upconverters, such as the Cisco uBR-MC16U, Cisco uBR-MC28U, and Cisco uBR-MC5X20S/U.
- **cable modem qos profile**—Supports a new option, **no-persistence**, which specifies that the quality-of-service (QoS) profile for a cable modem should not remain in force when the modem reboots. Instead, when a cable modem reboots, it uses the QoS profile specified in its DOCSIS configuration file. The default is without this option, so that the QoS profile remains in force for cable modems across reboots.
- **cable primary-sflow-qos11 keep**—Specifies whether the Cisco CMTS should preserve the DOCSIS 1.1 service flow traffic counters after a DOCSIS 1.1-provisioned CM goes offline and then comes back online. This allows service providers to track the total usage of CMs over a period of time, regardless of the number of times the CMs go offline and reboot.
- **cable service flow qi-rate-limit** {**all** | **none** | **standard** | **threshold** *n*}—Configures the Cisco CMTS for how it should grant bandwidth requests for extra bandwidth (packets that have the Queue Indicator (QI) bit set) for Unsolicited Grant Service (UGS) service flows.
- **cable spectrum-group**, **cable upstream spectrum-group**, **show cable spectrum-group**—The maximum number of spectrum groups has been increased from 32 to 40.
- **cable upstream fragment-force**—Specifies the size of DOCSIS 1.1 frames that should be fragmented, as well as the number of fragments that should be created when fragmenting. By default, the Cisco CMTS fragments DOCSIS frames that are 2,000 bytes or larger in size, and it fragments these frames into three equally-sized fragments.

Note On the Cisco uBR-MC5X20S/U cable interface line cards, do not use a fragment size greater than 2,000 bytes. On all other cable interface line cards, do not use a fragment size greater than 3,500 bytes, unless otherwise instructed by a Cisco TAC engineer.

- **clear cable hop**—Clears the forward error corrections (FEC) hop counters on one or all cable interfaces.
- **debug hccp sync cable cpe-management**—Displays debugging for SYNC messages that concern CPE-related parameters, such as MAX CPE, MAX CPE IP, and max learnable addresses.

- **dir** *filesystem:* and **show** *filesystem:*—These commands display a new field that shows the timezone for the file's date and time. The timezone field shows the number of hours the timezone is offset from the Coordinated Universal Time (UTC) timezone. For example:

```
Router# dir disk0:

Directory of disk0:/

    1  -rw-     5666024  Jan 24 1981 07:20:02 -05:00  ubr7200-kboot-mz.122BC
    2  -rw-    19445128  Jan 30 2004 10:24:40 -05:00  ubr7200-ik9s-mz.12215BC1
    3  -rw-    19680432   Feb 4 2004 09:17:44 -05:00  ubr7200-ik9s-mz.12215BC2
    4  -rw-        1289   Sep 4 2003 18:53:30 -04:00  startup.cfg
    5  -rw-      241940  Jan 27 2004 18:07:06 -05:00  system-log

47906816 bytes total (2883584 bytes free)

Router#
```

- **show cable modem verbose**—This command now also shows the total time that a particular cable modem has been online.
- **show hccp detail**—This command now shows separate lists of the critical and non-critical CLI commands that are being synchronized for each Working and Protect interface and subinterface.

For more information on these command changes, see the *Cisco Broadband Cable Command Reference Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

DOCS-IF-MIB Update

The DOCS-IF-MIB (released as RFC 2670) has been updated to conform to the version 5 of the DOCSIS 2.0 RF MIB Specification (draft-ietf-ipcdn-docs-rfmibv2-05.txt).

DOCSIS Set-Top Gateway

Cisco IOS Release 12.2(15)BC2 supports the initial version of the DOCSIS Set-Top Gateway (DSG) feature, which is an CableLabs specification that allows the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging to set-top boxes (STBs) over existing DOCSIS cable networks. This allows cable Multi-System Operators (MSOs) and other service providers to combine both DOCSIS and STB operations over one, open, vendor-independent network, without requiring any changes to the existing DOCSIS network infrastructure.

For more information about the DSG feature, see the *DOCSIS Set-Top Gateway (DSG) for the Cisco CMTS* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/ubrdsg.htm

Extended Upstream Frequency Ranges

Cisco IOS Release 12.2(15)BC2 adds support for the extended upstream frequency range that is used in cable networks in Japan and other areas. This feature also clarifies the configuration of DOCSIS and EuroDOCSIS networks, so that the router shows only those upstream and downstream frequencies that are valid for each mode of operation.

A new CLI command, **cable freq-range**, was also added to support this feature on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards. For more information, see the *Support for Extended Upstream Frequency Ranges*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/mclcjfm.htm

IEEE 802.1Q Transparent Lan Service

Cisco IOS Release 12.2(15)BC2 enhanced the existing support for Transparent Lan Services (TLS), which allows the Cisco CMTS to create Layer 2 tunnels for traffic to and from cable modems. This allows customers to create their own virtual local area network (VLAN) using any number of cable modems in multiple sites.

In addition to the ATM PVC Mapping, which was previously supported, Cisco IOS Release 12.2(15)BC2 added the ability to map a cable modem's MAC address to an IEEE 802.1Q VLAN on a specific Ethernet interface, so that all traffic from the cable modem is tagged with the specified VLAN ID. Service providers can now map cable modem traffic onto an ATM PVC or onto an Ethernet IEEE 802.1Q VLAN, depending on their customer's specific needs.

For more information on this service, see the *Transparent LAN service over Cable* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_11/sidatmpv.htm

N+1 Support for Load Balancing

Cisco IOS Release 12.2(15)BC2 supports configuring a cable interface for both load balancing and N+1 HCCP redundancy.

PacketCable Enhancements

Cisco IOS Release 12.2(15)BC2 supports PacketCable operations on the Cisco uBR-MC5X20S/U cable interface line cards on the Cisco uBR10012 router, and on the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards on the Cisco uBR7246VXR router.

In addition, cable interfaces can be configured for both PacketCable operations and for N+1 HCCP redundancy. The **debug packetcable hccp** and **show packetcable event** commands have been added as part of this support.

Vendor-Specific Information Field to Authorize Dynamic Service Requests

DOCSIS 1.1 cable modems can request additional bandwidth via the DOCSIS 1.1 dynamic services mechanism, by sending dynamic service add (DSA) and dynamic service change (DSC) messages (known collectively as DSX messages). By default, the CMTS grants these requests because a DOCSIS-compliant cable modem does not request services that would violate their provisioned service flows.

However, a cable modem that is using software that is not DOCSIS-compliant, or that is using software that has been hacked to include unauthorized changes that violate the DOCSIS specifications, could use dynamic services requests to obtain bandwidth that the user is not authorized to use. Users could also use dynamic services requests as part of a denial-of-service attack on the cable network.

To prevent this, Cisco IOS Release 12.2(15)BC2 supports including an optional vendor-specific information field (VSIF) in the DOCSIS configuration file to enable or disable DSX requests by the cable modem:

TLV = 43 (VSIF)

SubTLV 12, Length = 1

Value = 0, denies all DSX requests

Value = 1, allows all DSX requests

For example, the following string of decimal digits in the DOCSIS configuration file would enable DSX requests for a cable modem:

```
43-08-08-03-00-00-12-12-01-01
```

This string translates to the following TLV values:

```
TLV = 43
    Length = 08
    SubTLV = 08
        Length = 03
        Value = 00-00-12
    SubTLV = 12
        Length = 1
        Value = 1 (change to 0 to disable DSX requests)
```

By default, all DSX requests are allowed. The **show cable modem verbose** command has also been enhanced to show whether DSX messages are supported for a particular cable modem. For example, the following excerpt from the command shows the display when a cable modem is allowed to make DSX requests:

```
Router# show cable modem 0010.7bb3.fcd1 verbose

MAC Address                     : 00C0.7bb3.fcd1
IP Address                      : 10.20.113.2
Prim Sid                        : 1
QoS Profile Index               : 6
Interface                       : C5/0/U5
sysDescr                        : Vendor ABC DOCSIS 2.0 Cable Modem

...

Active Classifiers              : 0 (Max = NO LIMIT)
DSA/DSX messages                : permit all
Dynamic Secret                  : A3D1028F36EBD54FDCC2F74719664D3F

Router#
```

If DSX requests are not allowed, the **DSA/DSX messages** line would show “reject all.”

Tip We recommend also using the **cable dynamic-secret** and **cable tftp-enforce** commands to ensure that users cannot substitute their own DOCSIS configuration file in place of the original file provided by the service provider.

No New Hardware Features in Release 12.2(15)BC1g

There are no new hardware features in Cisco IOS Release 12.2(15)BC1g.

New Software Features in Release 12.2(15)BC1g

There are no new software features in Cisco IOS Release 12.2(15)BC1g.

No New Hardware Features in Release 12.2(15)BC1f

There are no new hardware features in Cisco IOS Release 12.2(15)BC1f.

New Software Features in Release 12.2(15)BC1f

There are no new software features in Cisco IOS Release 12.2(15)BC1f.

No New Hardware Features in Release 12.2(15)BC1d

There are no new hardware features in Cisco IOS Release 12.2(15)BC1d.

New Software Features in Release 12.2(15)BC1d

The following software features are new in Cisco IOS Release 12.2(15)BC1d.

Source Verify Lease-Query Throttling

When the cable source-verify dhcp and no cable arp commands are configured on a cable interface, problems can occur when viruses, denial of service (DoS) attacks, and theft-of-service attacks begin scanning a range of IP addresses, in an attempt to find unused addresses. When the Cisco CMTS router is verifying unknown IP addresses, this type of scanning generates a large volume of DHCP lease queries, which can result in a number of problems, such as dropped packets and high CPU utilization of both the Cisco CMTS router and DHCP server.

To prevent these problems, you can enable filtering of these requests on upstream interfaces, downstream interfaces, or both. When this feature is enabled, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests for each service ID (SID) on an interface within the configured interval time period. If a SID generates more lease queries than the maximum, the router drops the excess number of requests until the next interval period begins.

For more information on this feature, see the document “Filtering Cable DHCP Lease Queries”, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cblsrcvy.htm

Note The Source Verify Lease-Query Throttling feature is only available in Cisco IOS Release 12.2(15)BC1d and Cisco IOS Release 12.2(15)BC2b.

No New Hardware Features in Release 12.2(15)BC1c

There are no new hardware features in Cisco IOS Release 12.2(15)BC1c.

No New Software Features in Release 12.2(15)BC1c

The following software feature is new in Cisco IOS Release 12.2(15)BC1c:

Cable ARP Filter

Cisco IOS Release 12.2(15)BC2 adds support for the **cable arp filter** command, which enables service providers to filter ARP request and reply packets, to prevent a large volume of such packets from interfering with the other traffic on the cable network. For more information, see the *Cable ARP Filtering* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cblarpfl.htm

No New Hardware Features in Release 12.2(15)BC1b

There are no new hardware features in Cisco IOS Release 12.2(15)BC1b.

No New Software Features in Release 12.2(15)BC1b

There are no new software features in Cisco IOS Release 12.2(15)BC1b

No New Hardware Features in Release 12.2(15)BC1a

There are no new hardware features in Cisco IOS Release 12.2(15)BC1a.

No New Software Features in Release 12.2(15)BC1a

There are no new software features in Cisco IOS Release 12.2(15)BC1a

No New Hardware Features in Release 12.2(15)BC1

There are no new hardware features in Cisco IOS Release 12.2(15)BC1.

New Software Features in Release 12.2(15)BC1

The following software features are new in Cisco IOS Release 12.2(15)BC1.

Command-Line Interface Enhancements

Cisco IOS Release 12.2(15)BC1 supports the following additions and enhancements to the Cisco IOS command-line interface (CLI):

- The **cable slfog** global configuration command has been added to support a log of deleted service flow entries that is maintained in the DOCSIS-QOS SNMP MIB, which is required by the DOCSIS 2.0 specifications. This command enables service flow logging and configures the number and duration of entries in the log.
- The **clear cable modem flap-list** command was added to reset a particular cable modem's flap list counters to zero.
- The output for the **show cable modem verbose** command includes the value of the sysDescr SNMP attribute, as reported by the cable modem. This field shows a value only when the **cable modem remote-query** command has been enabled.

For a complete description of these commands and the changes, see the Cisco Broadband Cable Command Reference Guide, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

Dynamic Shared Secret

The Dynamic Shared Secret feature provides service providers a way of providing higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks, by using randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem. The Dynamic Shared Secret feature is enabled using the **cable dynamic-secret** interface configuration command.

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

For information on the Dynamic Shared Secret feature, see the *Configuring a Dynamic Shared Secret for the Cisco CMTS* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/ubrdmic.htm

Note The Dynamic Shared Secret feature does not affect the use of the original shared secret or secondary shared secrets that are configured using the **cable shared-secondary-secret** and **cable shared-secret** commands. If these shared secrets are configured, the Cisco CMTS continues to use them to validate the original DOCSIS configuration file that is downloaded from the TFTP server. If the DOCSIS configuration file fails to pass the original or secondary shared secret verification checks, the cable modem is not allowed to register, and the Dynamic Shared Secret feature is not invoked for that particular cable modem.

Tips Verify that a cable modem is able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.

Nonstop Forwarding (NSF) Awareness

The Nonstop Forwarding (NSF) Awareness feature, introduced in Cisco IOS release 12.2(15)T and inherited by Cisco IOS release 12.2(15)BC1, allows customer premises equipment (CPE) routers that are NSF-aware to assist NSF-capable routers perform nonstop forwarding of packets.

The NSF Awareness feature is supported on three IP routing protocols—Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Integrated Intermediate System-to-Intermediate System (IS-IS).

BGP NSF Awareness

BGP NSF Awareness assists NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation. The BGP NFS Awareness feature allows an NSF-aware router that is running BGP to forward packets along routes that are already known for a router that is performing an SSO operation.

If you use BGP, you need to enable NSF Awareness using the **bgp graceful-restart** command in global configuration mode. This procedure enables smooth switchover operations on the Cisco uBR10012 CMTS.

For information on the BGP NSF Awareness feature for Cisco IOS Release 12.2(15)T, refer to the *BGP Nonstop Forwarding (NSF) Awareness* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbgpnsf.htm

For configuration information, refer to the “Configuring BGP” section in the *Cisco IOS IP Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfbgp.htm

OSPF NSF Awareness

The local router's awareness of NSF allows the integrity and accuracy of the RIB and link state database occurring on the neighboring NSF-capable router to be maintained during the switchover process.

For information on the OSPF NSF Awareness feature for Cisco IOS Release 12.2(15)T, refer to the *OSPF Nonstop Forwarding (NSF) Awareness* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftosnsfa.htm

For configuration information, refer to the "Configuring OSPF" section in the *Cisco IOS IP Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfospf.htm

Integrated IS-IS NSF Awareness

The local router's awareness of NSF allows the integrity and accuracy of the RIB and link state database occurring on the neighboring NSF-capable router to be maintained during the switchover process.

For information on the Integrated IS-IS NSF Awareness feature for Cisco IOS Release 12.2(15)T, refer to the *Integrated IS-IS Nonstop Forwarding (NSF) Awareness* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/isnsfawa.htm

For configuration information, refer to the "Configuring Integrated IS-IS" section in the *Cisco IOS IP Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfisis.htm

Subscriber Traffic Management

The Subscriber Traffic Management feature allows service providers to identify and control subscribers who exceed the maximum bandwidth allowed under their registered quality of service (QoS) profiles. This feature supplements current techniques such as Network-Based Application Recognition (NBAR) and access control lists (ACLs) to ensure a minority of users do not consume a majority of the cable network's bandwidth.

Current subscriber controls, such as NBAR and ACLs, examine all packets coming into the CMTS. These techniques can curb a large volume of problem traffic, but they are not as effective in dealing with the latest generation of peer-to-peer file-sharing applications that can swamp a network's available bandwidth. The Subscriber Traffic Management feature allows service providers to focus on a minority of potential problem users, without impacting network performance or other users who are abiding by their service agreements.

In addition, when a cable modem goes offline and remains offline for 24 hours, the Cisco CMTS deletes its service flow IDs from its internal databases, and also deletes the modem's traffic counters. This can allow some users to exceed their bandwidth limits, go offline, and come back online with new counters.

The Subscriber Traffic Management feature helps to thwart these types of theft-of-service attacks by implementing a penalty period for cable modems that violate their service level agreements (SLA). Even if the cable modem goes offline, its counters are still reset, but the CMTS continues to enforce the penalty period.

For more information about the Subscriber Traffic Management feature, see the *Subscriber Traffic Management for the Cisco CMTS* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/ubsubmon.htm

Support for Cisco Broadband Troubleshooter Version 3.0

Cisco IOS Release 12.2(15)BC1 supports version 3.0 of the Cisco Broadband Troubleshooter, which includes graphic-based spectrum analysis for supported platforms and cable interface line cards. For more information, see the Cisco Broadband Troubleshooter documentation, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/trblshtr/cbt30/index.htm

No New Hardware Features in Release 12.2(11)BC3d

There are no new hardware features in Cisco IOS Release 12.2(11)BC3d.

No New Software Features in Release 12.2(11)BC3d

There are no new software features in Cisco IOS Release 12.2(11)BC3d.

No New Hardware Features in Release 12.2(11)BC3c

There are no new hardware features in Cisco IOS Release 12.2(11)BC3c.

No New Software Features in Release 12.2(11)BC3c

There are no new software features in Cisco IOS Release 12.2(11)BC3c.

No New Hardware Features in Release 12.2(11)BC3b

There are no new hardware features in Cisco IOS Release 12.2(11)BC3b.

No New Software Features in Release 12.2(11)BC3b

There are no new software features in Cisco IOS Release 12.2(11)BC3b.

No New Hardware Features in Release 12.2(11)BC3

There are no new hardware features in Cisco IOS Release 12.2(11)BC3.

New Software Features in Release 12.2(11)BC3

The following software features are introduced in Cisco IOS Release 12.2(11)BC3.

Transparent LAN Service over Cable

Cisco IOS Release 12.2(11)BC3 introduces support for the Transparent LAN Service over Cable feature for the Cisco uBR7100 series routers.

The Transparent LAN Service over Cable feature enhances the existing Asynchronous Transfer Mode (ATM) support to provide more flexible Managed Access for multiple Internet Service Provider (ISP) support over a hybrid fiber-coaxial (HFC) cable network. This feature allows service providers to map an upstream service identifier (SID) to an ATM permanent virtual connection (PVC).

The Transparent LAN Service over Cable feature enables service providers to provide Layer-2 tunnels over an ATM network, allowing customers to create their own virtual network using any number of cable modems in different sites.

On the Cisco CMTS, you map each cable modem (on the basis of its MAC address) to a separate PVC on an ATM interface. The CMTS then creates an internal database of this one-to-one mapping of cable modems to PVCs, and uses it to determine which packets should be forwarded to the ATM network.

The CMTS encapsulates the CPE traffic from mapped cable modems using AAL5 SNAP encapsulation, as defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5. It then forwards those packets to the appropriate ATM interface and PVC.

Traffic to and from this group of cable modems is routed to a group of PVCs that are bridged into a single ATM network by the ATM bridge aggregator, creating a secure virtual private network (VPN) for that particular group of cable modems. This allows service providers to provide Layer-2 VPN support that does not have the limitations of Layer-3 VPN solutions, such as MPLS-VPN:

- Unlike Layer-3 VPN solutions that support only IP packets, the Transparent LAN Service over Cable feature can support multiple Layer-3 protocols.
- Layer-2 VPN solutions provide Ethernet connectivity for the participating devices, so that the service provider does not need to know the addressing and routing details of the customer's private network.

Service providers can provide a Layer-2 VPN with only minimal configuration changes on the providers' routers. The end customer does not need to make any changes to their private network or cable modems, nor does the service provider have to provide any special DOCSIS configuration files to enable this feature.

The Transparent LAN Service over Cable feature has the following prerequisites:

- The Cisco uBR7100 series routers must be running Cisco IOS Release 12.2(11)BC3 or later Cisco IOS Release 12.2 BC release.
- You must know the hardware (MAC) addresses of the cable modems that are to be mapped to ATM PVCs.

You must create a bridge group for each separate customer on the ATM bridge aggregator, so that traffic from all of the CPE devices for the customer are grouped together into the same ATM tunnel.

Note See Limitations and Restrictions, page 62 for a summary of the restrictions for the Transparent LAN Service over Cable feature.

For more information on the feature, refer to the *Transparent LAN Service over Cable* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_11/sidatmpv.htm

clear cable modem Commands

Cisco IOS Release 12.2(11)BC3 adds support for two new **clear cable modem** commands:

- **clear cable modem delete**

  This command removes one or more CMs from the internal address and routing tables.

- **clear cable modem offline**

  This command removes offline CMs from the internal address and routing tables for a cable interface.

For syntax and usage information on the commands, refer to the "Cisco CMTS Commands" chapter of the *Cisco Broadband Cable Command Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmts.htm

debug cable Commands

Cisco IOS Release 12.2(11)BC3 adds support for the following new debug commands:

- **debug cable arp**

  This command enables debugging of the Address Resolution Protocol when it is used on the cable interface.

- **debug cable dhcp**

  This command enables debugging of the Dynamic Host Configuration Protocol (DHCP) when it is used on the cable interface.

- **debug cable encap**

  This command enables debugging of encapsulated Point-to-Point Protocol over Ethernet (PPPoE) packets on the cable interface.

For syntax and usage information on the debug commands, refer to the "Cisco CMTS Debugging Commands" chapter of the *Cisco Broadband Cable Command Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmtsde.htm

No New Hardware Features in Release 12.2(11)BC2

There are no new hardware features in Cisco IOS Release 12.2(11)BC2.

No New Software Features in Release 12.2(11)BC2

There are no new software features in Cisco IOS Release 12.2(11)BC2.

No New Hardware Features in Release 12.2(11)BC1b

There are no new hardware features in Cisco IOS Release 12.2(11)BC1b.

No New Software Features in Release 12.2(11)BC1b

There are no new software features in Cisco IOS Release 12.2(11)BC1b.

No New Hardware Features in Release 12.2(11)BC1a

There are no new hardware features in Cisco IOS Release 12.2(11)BC1a.

No New Software Features in Release 12.2(11)BC1a

There are no new software features in Cisco IOS Release 12.2(11)BC1a.

No New Hardware Features in Release 12.2(11)BC1

There are no new hardware features in Cisco IOS Release 12.2(11)BC1.

New Software Features in Release 12.2(11)BC1

The following new software feature was introduced in Cisco IOS Release 12.2(11)BC1.

cable source-verify leasetimer Command

Cisco IOS Release 12.2(11)BC1 introduces the **cable source-verify leasetimer** <n> command.

The **leasetimer** option allows you to configure how often the timer checks the lease times, so as to specify the maximum amount of time a customer premises equipment (CPE) device can use an IP address that was previously assigned by the Dynamic Host Configuration Protocol (DHCP) server but whose lease time has since expired. The time period can range from 1 minute to 240 minutes (4 hours), with a grace period of 2 minutes to allow a PC enough time to make a DHCP request to renew the IP address.

To turn off the timer, so that the CMTS no longer checks the lease times, issue the **cable source-verify** command without the **dhcp** option, or turn off the feature entirely with the **no cable source-verify** command. The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface or subinterface.

The **leasetimer** option adds another level of verification by activating a timer that periodically examines the lease times for the IP addresses for known CPE devices. If the CMTS discovers that the DHCP lease for a CPE device has expired, it removes that IP address from its database, preventing the CPE device from communicating until it makes another DHCP request. This prevents users from treating DHCP-assigned addresses as static addresses, as well as from using IP addresses that were previously assigned to other devices.

Note The leasetimer option for the cable source-verify command cannot be configured on subinterfaces. Instead, configure the command on the master interface, and the leasetimer will apply to all subinterfaces as well.

The following example shows how to enable the **leasetimer** feature so that every two hours, the CMTS checks the IP addresses in the CPE database for that particular interface for expired lease times:

```
router# configure terminal
router#(config) interface c1/0
router(config-if)# cable source-verify dhcp
router(config-if)# cable source-verify leasetimer 120
```

For more information on the command, refer to the “Cisco Cable Modem Termination System Commands” chapter in the *Cisco Broadband Cable Command Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmts.htm

No New Hardware Features in Release 12.2(8)BC2a

There are no new hardware features in Cisco IOS Release 12.2(8)BC2a.

No New Software Features in Release 12.2(8)BC2a

There are no new software features in Cisco IOS Release 12.2(8)BC2a.

No New Hardware Features in Release 12.2(8)BC2

There are no new hardware features in Cisco IOS Release 12.2(8)BC2.

New Software Features in Release 12.2(8)BC2

Cisco IOS Release 12.2(8)BC2 supports the following new software feature for the Cisco uBR7100 series routers.

Adding Load Information and a Timestamp to Show Commands

Cisco IOS Release 12.2(8)BC2 adds a new command, **exec prompt timestamp**, that adds load information and a timestamp to all show commands. This can be useful for troubleshooting and system analysis.

The new command has the following syntax in line configuration mode:

```
Router(config-line)# [no] exec prompt timestamp
```

The command has the following syntax in User EXEC mode, so that users who do not know the enable password can also timestamp their show commands:

```
Router> terminal [no] exec prompt timestamp
```

The following example shows how to enable and disable the timestamp for the console connection:

```
Router# config t
Router(config)# line console 0
Router(config-line)# exec prompt timestamp
Router(config-line)# no exec prompt timestamp
```

The following example shows how to enable and disable the timestamp for the first five telnet connections:

```
Router(config)# line vty 0 4
Router(config-line)# exec prompt timestamp
Router(config-line)# no exec prompt timestamp
```

The following example shows how to enable and disable the timestamp when logged into User EXEC mode:

```
Router> terminal exec prompt timestamp
Router> terminal no exec prompt timestamp
```

Display Modem Capabilities with the show cable modem mac Command

In Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases, the **mac** option displays both the maximum DOCSIS Version of the CM as well as the currently provisioned DOCSIS version. This allows you to see both the capabilities of the CM as well as its current provisioning.

```
Router# show cable modem mac

MAC Address    MAC          Prim  Ver     Prov    Frag  Concat PHS   Priv  DS    US
               State        Sid                                           Saids Sids
0010.64ff.e4ad online       1     DOC1.1  DOC1.0 yes   yes    yes   BPI+  0     4
0010.f025.1bd9 init(rc)     2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.9659.4447 online(pt)   3     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.9659.4461 online(pt)   4     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0010.64ff.e459 online       5     DOC1.0  DOC1.0 no    yes    no    BPI   0     0
0020.4089.7ed6 online       6     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3831 online(pt)   7     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0090.9607.3830 online(pt)   1     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0050.7366.12fb init(i)      2     DOC1.0  DOC1.0 no    no     no    BPI   0     0
0010.fdfa.0a35 online(pt)   3     DOC1.1  DOC1.1 yes   yes    yes   BPI+  0     4
```

Support for the cable modem vendor command

Cisco IOS Release 12.2(8)BC2 adds support for associating the name of a vendor with its Organizational Unique Identifier (OUI), so that the vendor name can appear in the displays of the **show cable modem vendor** command. The software comes with a default database that contains approximately 300 OUIs associated with approximately 60 vendor names, and you can use the **cable modem vendor** command in global configuration mode to create new associations or overwrite existing associations.

The syntax of the **cable modem vendor** command is:

[**no**] **cable modem vendor** *OUI* [*vendor-name*]

where *OUI* is the first 3 octets (3 bytes, 6 hexadecimal digits) of the CM MAC address and typically indicates the vendor for the CM. Each octet should be separated by a period or colon (for example: **00:01:02** or **00.01.02**). The *vendor-name* is the arbitrary string identifying the vendor for this OUI.

If you specify an OUI with the **cable modem vendor** command that already exists in the OUI database, the previous value is overwritten with the new value. You can use the **default** prefix to restore the original value for an OUI in the default database.

Use the **no cable modem vendor** command to remove the association between an OUI and a vendor name. The **show cable modem vendor** command then displays only the OUI as the vendor name.

Tip The Institute of Electrical and Electronics Engineers (IEEE) is the official issuer of OUI values. The IEEE OUI web site is at http://standards.ieee.org/regauth/oui/index.shtml.

The following shows several examples of the **cable modem vendor** command using Cisco OUIs:

```
Router(config)# cable modem vendor 00:01:42 Cisco
Router(config)# cable modem vendor 00:01:43 Cisco
Router(config)# cable modem vendor 00:01:63 Cisco
Router(config)# cable modem vendor 00:01:64 Cisco
Router(config)# cable modem vendor 00:0A:41 Cisco
Router(config)# cable modem vendor 00:0A:42 Cisco
```

The following example shows sample output for the **vendor** option on the Cisco uBR10012 router:

```
Router# show cable modem vendor

Vendor     MAC Address    I/F       MAC         Prim  RxPwr  Timing  Num BPI
                                    State       Sid   (db)   Offset  CPE Enb
Thomson    0010.9507.01db C5/1/0/U5 online      1     0.00    938   1    N
Ericsson   0080.37b8.e99b C5/1/0/U5 online      2     -0.25   1268  0    N
Cisco      0002.fdfa.12ef C6/1/0/U0 online      13    0.00    1920  1    N
Cisco      0002.fdfa.137d C6/1/0/U0 online      16    -0.50   1920  1    N
Cisco      0003.e38f.e9ab C6/1/0/U0 online      3     -0.25   1926  1    N
Cisco      0001.9659.519f C6/1/1/U2 online      26    0.25    1930  1    N
Motorola   0020.4005.3f06 C7/0/0/U0 online      2     0.00    1901  1    N
Motorola   0020.4006.b010 C7/0/0/U5 online      3     0.25    1901  1    N
Cisco      0050.7302.3d83 C7/0/0/U0 online      18    -0.25   1543  1    N
Cisco      00b0.6478.ae8d C7/0/0/U5 online      44    0.50    1920  21   N
Cisco      00d0.bad3.c0cd C7/0/0/U5 online      19    0.00    1543  1    N
Cisco      00d0.bad3.c0cf C7/0/0/U0 online      13    0.00    1546  1    N
Cisco      00d0.bad3.c0d5 C7/0/0/U0 online      12    -0.50   1546  1    N
Router#
```

Support for the cable tftp-enforce Command

Cisco IOS Release 12.2(8)BC2 adds support for the new **cable tftp-enforce** cable interface configuration command, which requires all cable modems on a cable interface to attempt a TFTP request for the DOCSIS configuration file through the cable interface with the Cisco CMTS router before being allowed to register and come online. This can help prevent the following situations from occurring:

- Users who attempt theft-of-service by reconfiguring their local networks to allow the downloading of an unauthorized DOCSIS configuration file from a local TFTP server. Typically, some users do this to obtain services that they have not paid for, such as higher guaranteed bandwidths or a higher priority Quality of Service (QoS) profile.
- Some brands or models of cable modems might be running older software releases that cache the DOCSIS configuration file and use the cached version instead of downloading the actual file from a TFTP server during the registration process. Although this can marginally speed up the registration process, it also violates the DOCSIS requirements and could create a situation in which the cable modem is not using the proper DOCSIS configuration file. A user might then be mistakenly accused of theft-of-service, when in reality the problem is the non-DOCSIS-compliant cable modem.

The **cable tftp-enforce** command identifies these situations and can block these cable modems from registering and coming online. This command also has an option that allows these cable modems to come online, but it also identifies the cable modems so that the network administrators can investigate the situation further before taking any action.

Command Syntax

The new command has the following syntax:

```
cable tftp-enforce [mark-only]
no cable tftp-enforce [mark-only]
```

When the command is used without the **mark-only** option, cable modems that do not download a TFTP file are blocked from registering and coming online. The **mark-only** option allows the cable modems to come online, but it also prints a warning message and marks the cable modems in the **show cable modem** command.

Tips Cisco recommends that you initially configure cable interfaces with the **mark-only** option, so that potential problems are identified without initially interfering with users' ability to come online. After you identify and resolve these initial problems, reconfigure the cable interfaces without the **mark-only** option to block problem cable modems that attempt to come online without downloading a valid DOCSIS configuration file.

The default behavior is not to require the TFTP download through the cable interface with the Cisco CMTS router. Each cable interface must be configured with this command to require the TFTP download.

Enforcing TFTP Downloads and Blocking Non-Compliant Cable Modems

The following example shows how to enforce TFTP downloads for all of the cable modems on cable interface 1/0. These cable modems must attempt a TFTP download of the DOCSIS configuration file through their cable interface with the Cisco CMTS router. If they do not, they are not allowed to register or come online.

```
Router# configure terminal
Router(config)# interface cable 1/0
Router(config-if)# cable tftp-enforce
Router(config-if)# exit
Router(config)#
```

When the **cable tftp-enforce** command is configured, the following message is displayed on the console when a cable modem attempts to register without first attempting a TFTP download through the cable interface with the Cisco CMTS router:

```
06:53:57: %UBR7100-4-REGISTRATION_BEFORE_TFTP: Registration request unexpected:
Cable Modem did not attempt TFTP.  Registration Rejected. CM Mac Addr <00ff.ff66.12fb>
```

When a cable modem is rejected for not attempting a TFTP download, it is marked as having a Message Integrity Check (MIC) failure—reject(m)—in the **show cable modems** command.

```
Router# configure terminal
Router(config)# interface cable 1/0
Router(config-if)# cable tftp-enforce
Router(config-if)# exit
Router(config)#

Router# show cable modems
Interface   Prim  Online     Timing Rec    QoS CPE IP address      MAC address
            Sid   State      Offset Power
Cable1/0/U1 1     online(pt)  2734    0.50  5   0   10.1.1.38       00ff.fffa.0a35
Cable1/0/U0 2     online(pt)  2729    0.25  5   0   10.1.1.50       00ff.ff07.382f
Cable1/0/U0 3     init(i)     2732    0.25  2   0   10.1.1.48       00ff.ff03.307d
Cable1/0/U1 4     online(pt)  2737    0.75  5   0   10.1.1.34       00ff.ff59.4477
Cable1/0/U1 5     reject(m)   2215    0.25  2   0   10.1.1.47       00ff.ff66.12fb

Router#
```

Note DOCSIS-compliant cable modems that are rejected with a MIC failure go into the offline state for a short period of time and then retry the registration process.

The **debug cable registration** command can be used to display additional information:

```
Router# debug cable interface c1/0 verbose
Router# debug cable registration
CMTS registration debugging is on
```

```
Jun  6 23:27:15.859: Registration request from 00ff.ff66.12fb, SID 7 on Cable1/0/U1
Jun  6 23:27:15.859: Found a network access control parameter: Ok
Jun  6 23:27:15.859: Found a class of service block: Ok
Jun  6 23:27:15.859: Found Baseline Privacy config: Ok
Jun  6 23:27:15.859: Found Max CPE: Ok
Jun  6 23:27:15.859: Found CM MIC: Ok
Jun  6 23:27:15.859: Found CMTS MIC: Ok
Jun  6 23:27:15.859: Found modem ip: Ok
Jun  6 23:27:15.859: Found modem capabilities: Ok
Jun  6 23:27:15.859: Finished parsing REG Request
Jun  6 23:27:15.859: Cable Modem sent Registration Request without attempting required
TFTP
22:33:21 %UBR7100-4-REGISTRATION_BEFORE_TFTP: Registration request unexpected:
Cable Modem did not attempt TFTP. Registration Rejected. CM Mac Addr <00ff.ff66.12fb>
Registration failed for Cable Modem 00ff.ff66.12fb on interface Cable1/0/U0:
              CoS/Sflow/Cfr/PHS failed in REG-REQ
Jun  6 23:27:15.859: REG-RSP Status : failure (2)
Jun  6 23:27:15.859: Registration Response:
Jun  6 23:27:15.859: 0x0000: C2 00 00 1B 00 00 00 50 73 4E B4 19 00 05 00 E0
Jun  6 23:27:15.859: 0x0010: 56 AC 00 09 00 00 03 01 07 00 00 02 02
Jun  6 23:27:15.859: Registration Response Transmitted
```

Identifying Non-Compliant Cable Modems But Allowing Them to Come Online

The **mark-only** option of the **cable tftp-enforce** command allows CMs that do not attempt a TFTP download through the cable interface to come online, but the Cisco CMTS router displays a warning message on the console and marks the cable modem in the **show cable modem** command with a pound sign (#). This option allows network providers to identify potential problems and to investigate them before taking any corrective action.

When the **mark-only** option is configured, the following message is displayed on the console when a cable modem attempts to register without first attempting a TFTP download through the cable interface with the Cisco CMTS router:

```
06:53:57: %UBR7100-4-REGISTRATION_BEFORE_TFTP: Registration request unexpected:
Cable Modem did not attempt TFTP. Modem marked with #. CM Mac Addr <00ff.ff66.12fb>
```

In addition, the cable modem is marked with a pound sign (#) in the **show cable modems** command:

```
Router# configure terminal
Router(config)# interface cable 1/0
Router(config-if)# cable tftp-enforce mark-only
Router(config-if)# exit
Router(config)#

Router# show cable modems
Interface   Prim  Online     Timing Rec    QoS CPE IP address      MAC address
            Sid   State      Offset Power
Cable1/0/U1 1     online(pt)  2734    0.50  5   0   10.1.1.38       00ff.fffa.0a35
Cable1/0/U0 2     online(pt)  2729    0.25  5   0   10.1.1.50       00ff.ff07.382f
Cable1/0/U0 3     init(i)     2732    0.25  2   0   10.1.1.48       00ff.ff03.307d
Cable1/0/U1 4     online(pt)  2737    0.75  5   0   10.1.1.34       00ff.ff59.4477
Cable1/0/U1 5    #online      2213    0.25  6   0   10.1.1.47       00ff.ff66.12fb

Router#
```

The **debug cable registration** command can be used to display additional information:

```
Jun  6 23:27:15.859: Registration request from 00ff.ff66.12fb, SID 7 on Cable1/0/U1
Jun  6 23:27:15.859: Found a network access control parameter: Ok
Jun  6 23:27:15.859: Found a class of service block: Ok
Jun  6 23:27:15.859: Found Baseline Privacy config: Ok
Jun  6 23:27:15.859: Found Max CPE: Ok
Jun  6 23:27:15.859: Found CM MIC: Ok
Jun  6 23:27:15.859: Found CMTS MIC: Ok
Jun  6 23:27:15.859: Found modem ip: Ok
Jun  6 23:27:15.859: Found modem capabilities: Ok
Jun  6 23:27:15.859: Finished parsing REG Request
Jun  6 23:27:15.859: Cable Modem sent Registration Request without attempting required
TFTP
23:27:15: %UBR7100-4-REGISTRATION_BEFORE_TFTP: Registration request unexpected:
Cable Modem did not attempt TFTP. Modem marked with #. CM Mac Addr <00ff.ff66.12fb>
Jun  6 23:27:15.859: Sec sids obtained for all requested classes of service
Jun  6 23:27:15.859: Performing connection admission control (CAC) for each Sid
Jun  6 23:27:15.859: CAC Status for ClassID:1 is CAC_SUCCESS
Jun  6 23:27:15.859: Registration Status: ok (0)
Jun  6 23:27:15.859: Registration Response Transmitted
```

Support for a Secondary Shared Secret

Cisco IOS Release 12.2(8)BC2 adds support for one or more secondary shared-secret keys that cable modems can use to successfully process the DOCSIS configuration file and register with the Cisco CMTS. Secondary shared secrets can be defined with the **cable shared-secondary secret** command, which has the following syntax:

cable shared-secondary secret index *index-num* [**0** | **7**] *authentication-key*

no cable shared-secondary secret index *index-num*

where *index-num* specifies the order in which the Cisco CMTS will use the secondary shared-secrets to verify the cable modem during the registration process. The valid range is 1 to 16. The *authentication-key* is the secondary shared secret string, where **0** indicates it is unencrypted and **7** indicates it is encrypted.

Note To store the *authentication-key* in encrypted form in the configuration file, also use the **service password-encryption** command.

The cable modem must use the proper shared secret encryption string to successfully decrypt and process the configuration file, and then register with the Cisco CMTS. If the cable modem does not have the proper encryption string, it will be unable to calculate the proper MIC value, and the **show cable modem** command will show **reject(m)** for the modem to indicate a MIC authentication failure.

The **cable shared-secondary-secret** command allows a cable operator to specify up to 16 alternate DOCSIS shared secrets. If a cable modem has a MIC authentication failure during registration, the CMTS then checks the MIC values using the alternate shared secrets. If a match is found, the cable modem is allowed online. If none of the alternate MIC values match the value returned by the CM, the CMTS refuses to allow the cable modem to come online and instead logs a MIC authentication failure.

The use of secondary shared secrets allow the MSO to gradually phase in changes to the shared secret key. If a shared secret has been compromised, or if the MSO decides to regularly change the shared secret, the MSO can use the **cable shared-secret** command to immediately change the primary shared secret. The previous key can then be made a secondary shared secret, using the **cable shared-secondary-secret** command, so that CMs can continue to register until the MSO can change all of the DOCSIS configuration files to use the new shared secret.

To use the secondary shared-secret feature, you must do the following:

- You must specify a shared secret with the **cable shared-secret** command. The **cable shared-secondary-secret** command has no effect if you have not specified a primary shared secret.

Note At any particular time, the majority of cable modems should use the primary shared secret to avoid excessive registration times.

- Create DOCSIS configuration files that use the shared-secret encryption string to create the MD5 MIC value. This can be done using the Cisco DOCSIS Configurator tool by entering the shared-secret string in the **CMTS Authentication** field in the **Miscellaneous** parameters.

Note The shared-secret string itself is not saved in the DOCSIS configuration file, so you must re-enter the string in the **CMTS Authentication** field whenever you create or edit a DOCSIS configuration file using the Cisco DOCSIS Configurator tool.

- Use the **cable shared-secondary-secret** command to configure the cable interfaces with one or more matching shared-secret strings. The string configured on an interface must match the string used to create the DOCSIS configuration files downloaded to the CMs on that interface, or the CMs will not be able to register. You can use different shared secrets for each interface, if you are also using a different set of configuration files for each interface.
- To encrypt the shared-secret strings in the CMTS configuration, you must include the **service password-encryption** global configuration command in the router's configuration.

Note You cannot use the secondary shared secret feature with the files created by the internal DOCSIS configuration file editor (**cable config-file** command) because the internal DOCSIS configuration file editor automatically obtains the correct shared secret from the interface when the modems register.

The following example shows how to specify multiple secondary shared-secret string using encrypted keys:

```
Router# config t
Router(config)# service password-encryption
Router(config)# int c6/0
Router(config-if)# cable shared-secret n01jk_1a
Router(config-if)# cable shared-secondary-secret index 1 cabl3-x21b
Router(config-if)# cable shared-secondary-secret index 2 dasc9_ruld55ist5q3z
Router(config-if)# cable shared-secondary-secret index 3 j35u556_x_0
Router(config-if)# exit
Router(config)# exit
Router# show running-config | include shared
cable shared-secret 7 1407513181A0F13253920
cable shared-secondary-secret 7 14031A021F0D39263D3832263104080407
cable shared-secondary-secret 7 071B29455D000A0B18060615142B38373F3C2726111202431259545D6
cable shared-secondary-secret 7 0501555A34191B5F261D28420A555D
Router#
```

Note In this example, the shared-secret strings are initially entered as clear text, but because the **service password-encryption** command has been used, the strings are encrypted in the configuration file.

See the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* for more information about the **cable shared-secondary secret** command at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmts.htm

Enhancement to the show hccp brief Command

In Cisco IOS Release 12.2(8)BC2 and later 12.2 BC releases, the brief option now shows the amount of time left before the next resynchronization 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
```

Enhancement to the cable filter group Command

The **status** option was added to the **cable filter group** command to allow filter groups to be activated and deactivated without removing the filter group's configuration.

For example, the following command would deactivate a filter without changing its configuration:

```
Router(config)# cable filter group 1 index 1 status inactive
```

The following command would reactivate this filter:

```
Router(config)# cable filter group 1 index 1 status active
```

Note Filter groups are active by default when created.

New Hardware Features in Release 12.2(8)BC1

The following new hardware feature is supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(8)BC1.

PA-A3-E3 Port Adapter

The PA-A3-E3 is a single-width, single-port E3 ATM, PCI-based port adapter that uses an E3 interface with a coaxial cable BNC connector.

Note For configuration information on the PA-A3-E3 port adapter, see the *PA-A3 Enhanced ATM Port Adapter Installation and Configuration Guide*, which is available on the Customer Documentation CD-ROM, and on Cisco.com at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/portadpt/atm_port/pa_a3/index.htm

New Software Features in Release 12.2(8)BC1

The following new software features are supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(8)BC1.

EXEC Commands in Configuration Mode

In Cisco IOS Release 12.2(8)BC1, you can now issue EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) from within global configuration mode or other configuration modes by issuing the **do** command followed by the EXEC command. For example, you can display the run-time configuration file from within global configuration mode by issuing the following command:

```
Router(config)# do show running-config
```

Note You cannot use the **do** command to execute the **configure terminal** EXEC command because issuing the **configure terminal** command changes the mode to configuration mode.

Secure Shell Support

Secure Shell (SSH) allows network administrators to securely log in to the Cisco uBR7100 series routers, using authentication and encryption at the application layer and providing a secure connection even when logging in over insecure networks such as the Internet. Secure Shell allows an administrator to securely monitor and configure a router without having to be logged into the router's local console port or directly connected to the Ethernet port on the router's I/O controller.

To configure SSH on a Cisco uBR7100 router, use the following command in global configuration mode:

```
uBR7100(config)# crypto key generate rsa general-keys
```

When you are asked the size of the key seed, enter a value of at least 1024.

To verify whether SSH is configured on the Cisco uBR7100 router, use the following command in Privileged EXEC mode:

```
uBR7100# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

To verify whether the Cisco uBR7100 router has an SSH connection, use the following command in Privileged EXEC mode:

```
uBR7100# show ssh

Connection Version Encryption State           Username
1          1.5     DES        Session started admin
```

No New Hardware Features in Release 12.2(4)BC1b

There are no new hardware features in Cisco IOS Release 12.2(4)BC1b.

New Software Features in Release 12.2(4)BC1b

The following new software features are supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(4)BC1b.

Cisco IOS Network-Based Application Recognition (NBAR)

Cisco IOS Release 12.2(4)BC1b adds support for Cisco IOS Network-Based Application Recognition (NBAR). The NBAR feature is a new classification engine that can recognize a wide variety of network applications, including Web-based applications, client/server applications, and other difficult-to-classify protocols that dynamically assign TCP or UDP port numbers.

NBAR enhances existing methods of application-recognition by adding several new classification features:

- Classification of applications that use statically assigned TCP/UDP port numbers, that use dynamically assigned TCP/UDP port numbers, or that use protocols other than TCP and UDP
- Classification of HTTP traffic by URL, host, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although access control lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide other options and classification statistics that are not available when using ACLs.

Tips The Cisco IOS NBAR feature requires CPU resources to inspect, recognize, and process the packets coming through the router. In laboratory conditions, the use of NBAR can impact CPU performance by approximately 30 percent—the actual performance impact depends on the current CPU load, the number of packets processed, and the type of traffic being inspected. To limit the performance impact when using NBAR, activate the Turbo ACL feature to increase the performance of access list handling.

After NBAR recognizes an application, the Cisco uBR7100 series router can invoke specific services appropriate for that application. These services can provide QoS features such as:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping
- Packet coloring

The Cisco IOS NBAR feature can also be used to detect and respond to denial-of-service and other types of network attacks. Cisco IOS NBAR uses a protocol description language module (PDLM) to define the rules by which the NBAR processes recognize an application. New PDLM definitions can usually be loaded without the need for a Cisco IOS software upgrade or a router reboot, allowing for a rapid response to discovered attacks.

Note For basic information on configuring and using the Cisco IOS NBAR feature, see the *Network-Based Application Recognition* documentation. For information on configuring NBAR for Quality of Service (QoS) control, see the *Configuring Network-Based Application Recognition* chapter in the *Cisco IOS Release 12.2 Quality of Service Solutions Configuration Guide*. These documents are available on Cisco.com and the Customer Documentation CD-ROM.

Tips Cisco.com also contains a technical note, *Using Network-Based Application Recognition and Access Control Lists for Blocking the Code Red Worm*, that provides information on using NBAR to block denial-of-service attacks. This technical note is available at http://www.cisco.com/warp/customer/63/nbar_acl_codered.shtml.

SNMP Cable Modem Remote Query

The remote query feature allows the Cisco Cable Modem Termination System (CMTS) to use Simple Network Management Protocol (SNMP) requests to periodically poll online CMs to gather the signal-to-noise ratio (SNR), upstream power value, transmit timing offset, micro reflection value, and modem state. To enable the remote query feature, use the **cable modem remote-query** command. To display the collected statistics, use the **show cable modem remote-query** command, or display the attributes in the CISCO-DOCS-REMOTE-QUERY-MIB MIB. You can also generate SNMP traps to inform the SNMP manager when remote query polling has completed by using the **snmp-server enable cable cm-remote-query** command.

Turbo Access Control Lists

Cisco IOS Release 12.2(4)BC1b adds support for Turbo Access Control Lists (Turbo ACL), which increases the performance of access lists by compiling them into a form that is more quickly accessed during packet processing. The **access-list compiled** command enables the Turbo ACL feature, and the **show access-lists** and **show access-lists compiled** commands provide status information about these access lists.

Complete information about the Turbo ACL feature is available on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dttacl.htm. The related commands are also described in the *Addressing and Services* volume of the *Cisco IOS Release 12.1 IP and IP Routing Command Reference*. For complete information about access lists, see the *Traffic Filtering and Firewall* volume in the *Cisco IOS Release 12.1 Security Configuration Guide*.

Note The Turbo ACL feature was introduced in Cisco IOS Release 12.1(9)EC but was unusable because of caveats CSCdv04414 and CSCdv69271. These caveats have been resolved in Cisco IOS Release 12.1(10)EC.

No New Hardware Features in Release 12.2(4)BC1a

There are no new hardware features in Release 12.2(4)BC1a.

No New Software Features in Release 12.2(4)BC1a

There are no new software features in Release 12.2(4)BC1a.

New Hardware Features in Release 12.2(4)BC1

The following new hardware features are supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(4)BC1.

PA-T3+ and PA-2T3+ Port Adapter Cards

The PA-T3+ and PA-2T3+ port adapters provide full-duplex operation at the T3 (45 Mbps) speed. They support both 16- and 32-bit cyclic redundancy checks (CRCs), with the default being 16-bit CRCs. The PA-T3+ port adapter provides one port, and the PA-2T3+ port adapter provides two ports.

Cisco IOS Release 12.2(4)BC1 supports the PA-T3+ and PA-2T3+ port adapters on the Cisco uBR7223 and Cisco uBR7246VXR universal broadband routers. These port adapters are replacements for the PA-T3 and PA-2T3 port adapters, which have reached their end-of-life.

Note For configuration information on the PA-T3+ and PA-2T3+ port adapters, see the *PA-T3 Serial Port Adapter Installation and Configuration Guide*, which is available on Cisco.com and the Documentation CD-ROM.

New Software Features in Release 12.2(4)BC1

The following new software feature is supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(4)BC1.

PPPoE Termination Support on Cable interfaces

The Point-to-Point Protocol over Ethernet (PPPoE) on Cable Interfaces feature adds support for PPPoE by allowing a direct connection to cable interfaces. PPPoE provides service-provider digital-subscriber line (DSL) support. The support of PPPoE on cable interfaces of the Cisco uBR7100 series routers allows customer premises equipment (CPE) behind the cable modem to use PPP as a mechanism to get their IP addresses and use it for all subsequent data traffic, just like a dial-up PPP client. In a PPP dial-up session, the PPPoE session is authenticated and the IP address is negotiated between the PPPoE client and the server, which could be either a Cisco uBR7100 series router or a Home Gateway.

Information about configuring PPPoE is available in the *Configuring Broadband Access: PPP and Routed Bridge Encapsulation* chapter of the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*. Also see the *PPPoE on Ethernet* feature module and RFC 2516 (http://www.ietf.org/rfc/rfc2516.txt).

Note PPPoE is supported only in routing mode. Bridged mode is not supported in the Cisco IOS Release 12.2 BC train for the Cisco uBR7100 series routers.

No New Hardware Features in Release 12.2(4)XF1

There are no new hardware features supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(4)XF1.

New Software Features in Release 12.2(4)XF1

The following new software features are supported by the Cisco uBR7100 series routers in Cisco IOS Release 12.2(4)XF1.

DOCSIS 1.0 and 1.0+ Support

Cisco IOS Release 12.2(4)XF1 provides support for the original DOCSIS 1.0 standard that provides for basic best-effort data traffic and Internet access over the coaxial cable network. The DOCSIS 1.0+ extensions provided Quality of Service (QoS) enhancements for real-time traffic, such as voice calls, in anticipation of full DOCSIS 1.1 support.

Cisco IOS Release 12.2(4)XF1 interoperates seamlessly with both DOCSIS 1.0 and 1.0+ cable modems and set-top boxes.

DOCSIS 1.1 Support

Cisco IOS Release 12.2(4)XF1 provides support for the new DOCSIS 1.1 standard for the Cisco Release 12.2(4)XF1 series routers. DOCSIS 1.1 modifies the DOCSIS 1.0 specification to provide better performance, in particular for real-time traffic such as voice calls.

The DOCSIS 1.1 specification provides the following functional enhancements over DOCSIS 1.0 coaxial cable networks:

- Enhanced Quality of Service (QoS) to give priority for real-time traffic such as voice and video
  - The DOCSIS 1.0 QoS model (a Service IDs (SID) associated with a QoS profile) has been replaced with a service flow model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions
  - Multiple service flows per CM in either direction due to packet classifiers
  - Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic
  - Greater granularity in QoS per cable modem in either direction, using unidirectional service flows
  - Dynamic MAC messages that can create, modify, and tear-down QoS service flows dynamically when requested by a DOCSIS 1.1 cable modem

- Supported QoS models for the upstream are:
  - Best effort-Data traffic sent on a non-guaranteed best-effort basis
  - Committed Information Rate (CIR)—Guaranteed minimum bandwidth for data traffic
  - Unsolicited Grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals
  - Real Time Polling (rtPS)—Real Time service flows, such as video, that produce unicast, variable size packets at fixed intervals
  - Unsolicited Grants with Activity Detection (USG-AD)—Combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Enhanced time-slot scheduling mechanisms to support guaranteed delay/jitter sensitive traffic on the shared multiple access upstream link
- Payload Header Suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows
- Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the timeslots that are available between the timeslots used for the real-time traffic.
- Concatenation allows a cable modem to send multiple MAC frames in the same timeslot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.
- DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—the Cisco Release 12.2(4)XF1 series provides the levels of service that are appropriate for each cable modem

DOCSIS 1.1 Quality of Service

The DOCSIS 1.1 QoS framework is based on the following objects:

- Service class: A collection of settings maintained by the CMTS that provide a specific QoS service tier to a cable modem that has been assigned a service flow within a particular service class
- Service flow: a unidirectional sequence of packets receiving a service class on the DOCSIS link
- Packet classifier: A set of packet header fields used to classify packets onto a service flow to which the classifier belongs
- PHS rule: A set of packet header fields that are suppressed by the sending entity before transmitting on the link, and are restored by receiving entity after receiving a header-suppressed frame transmission. Payload Header Suppression increases the bandwidth efficiency by removing repeated packet headers before transmission

In DOCSIS 1.1, the basic unit of QoS is the service flow, which is a unidirectional sequence of packets transported across the RF interface between the cable modem and CMTS. A service flow is characterized by a set of QoS parameters such as latency, jitter, and throughput assurances.

Every cable modem establishes a primary service flow in both the upstream and downstream directions. The primary flows maintain connectivity between the cable modem and CMTS at all times.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows can either be permanently created (they persist until the cable modem is reset or powered off) or they can be created dynamically to meet the needs of the on demand traffic being transmitted.

Each service flow has a set of QoS attributes associated with it. These QoS attributes define a particular class of service and determine characteristics such as the maximum bandwidth for the service flow and the priority of its traffic. The class of service attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified at the time of the creation of the service flow.

Each service flow has multiple packet classifiers associated with it, which determine the type of application traffic allowed to be sent on that service flow. Each service flow can also have a Payload Header Suppression (PHS) rule associated with it to determine which portion of the packet header will be suppressed when packets are transmitted on the flow.

In Cisco IOS Release 12.2(4)XF1, the following new or enhanced software features are implemented for DOCSIS 1.1 functionality. (For more information, see the feature module *DOCSIS 1.1 for Cisco Release 12.2(4)XF1 Series Universal Broadband Routers*).

Cable ARP and Proxy ARP

The **cable arp** and **cable proxy-arp** commands control whether the Cisco Release 12.2(4)XF1 series router allows ARP requests on the cable interfaces and whether the router serves as a proxy ARP server for cable modems, so that cable modems on the same subnet can communicate with each other, without having to send the traffic through the Cisco Release 12.2(4)XF1 series router.

Cable Flap List

The cable flap list is a patented tool that is incorporated in the Cisco IOS software for the Cisco Release 12.2(4)XF1 series universal broadband routers for troubleshooting cable modem connectivity problems. The flap list tracks cable modems that have intermittent connectivity problems (known as “flapping”) that could indicate a problem with the cable modem or with the upstream or downstream portion of the cable plant.

The flap-list feature does not require any special polling or data transmissions but instead monitors the registration and station maintenance activity that is already performed over any network that conforms to Data-over-Cable Service Interface Specifications (DOCSIS). The router, therefore, collects its flap-list data without creating additional packet overhead and without impacting network throughput and performance.

The flap-list feature tracks reinsertions (a cable modem re-registers more frequently than a user-specified insertion time, hits and misses (a cable modem responds or does not respond to the DOCSIS MAC-layer “keepalive” messages that the router sends out), and the cable modem’s upstream transmission power level adjustments.

Cable Intercept Command

The **cable intercept** command forwards all traffic to and from a particular CM to a data collector located at particular User Datagram Protocol (UDP) port. This command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other law enforcement wiretap requirements for voice communications.

Note The **cable monitor** command, which performs a similar function, is not supported in Cisco IOS 12.2(15)BC2i, Release 12.2(11)BC3c, or Release 12.2(4)XF1.

Cable Interface Setup Facility

The Cable Interface Setup Facility is an alternative mechanism to enable or configure Cisco Release 12.2(4)XF1 series parameters. The setup facility supports automated configuration of upstream parameters.

In earlier releases, upstream ports were put in a default shut-down state after the setup facility was run. You had to use the CLI to configure a fixed frequency or create a spectrum group, assign an interface to it, and enable each upstream port on a cable interface line card. The setup facility now supports configuring and enabling upstream parameters.

In the following example, the upstream parameters for a cable interface line card in slot 5 are configured and enabled. Press **Return** to accept the default.

```
Do you want to configure Cable 5/0 interface? [no]: yes
Downstream setting frequency: 531000000
For cable upstream [0]
Shut down this upstream? [yes/no]: no
Frequency: 33808000
Would you like to configure the DHCP server? [yes/no]: yes
IP address for the DHCP server [X.X.X.X]: 10.0.0.2
Configure IP on this interface? [yes]:
IP address for this interface [10.20.133.65]:
Subnet mask for this interface [255.0.0.0]: 255.255.255.248
Class A network is 10.0.0.0, 29 subnet bits; mask is /29
```

In this example, the input above generates the following command interface script:

```
interface Cable 5/0
no shutdown
cable downstream frequency 531000000
no shutdown
cable downstream modulation 64qam
cable downstream annex B
cable downstream interleave-depth 32
no cable upstream 0 shutdown
cable upstream 0 frequency 33808000
cable helper-address 10.0.0.2
ip address 10.20.133.65 255.255.255.248
```

Note Cable modems or set-top boxes with integrated cable modems are brought online when the utility is run.

Note For Dynamic Host Configuration Protocol (DHCP)/time of day (TOD)/Trivial File Transfer Protocol (TFTP), a static route must exist to the host.

Cable Source Verification Feature

The **cable source-verify** command helps to prevent the spoofing of IP addresses by CMs or their CPE devices by verifying that the upstream packets coming from each CM are known to be associated with the IP address in that packet. Packets with IP addresses that do not match those associated with the CM are dropped.

Note The **cable source-verify** [**dhcp**] cable interface command specifies that DHCP lease-query requests are sent to verify any unknown source IP address found in upstream data packets. This feature requires a DHCP server that supports the new LEASEQUERY message type.

DHCP/TOD/TFTP Server Support

The Cisco uBR7100 series routers support onboard Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP servers that are compliant with the DOCSIS requirements. This allows the Cisco uBR7100 series routers to provide cable modems with IP address information, to supply an RFC 868-compliant time-of-day timestamp, and to download a DOCSIS configuration file, without requiring separate, external servers.

Dynamic Map-Advance

The Dynamic Map-Advance feature improves the upstream throughput for a cable modem. This feature enables the map-advance to be dynamic and self-adjusting to propagation delay, even for the furthest cable modem in the plant.

Dynamic Mobile Hosts

This feature addresses a security hole that occurs when the Cisco uBR7100 router supports mobile hosts. (Mobile host are hosts that can move from one modem to another modem.) Anyone who knows the MAC address of a mobile host can “fake” the mobile host, thereby causing denial of access for the real mobile host.

To avoid this security hole, the Dynamic Mobile Hosts feature pings the mobile host on the old SID to verify that the host has indeed been moved.

Dynamic Ranging Support

The **clear cable modem** <mac-address> **reset** command sends a “Ranging Abort” message instead of just removing the SID. To indicate this, the modem state—Reset (display: resetting)— has been introduced into the modem state list. A modem is deprovisioned when moving into this state as if going offline. Move the modem to the Continue Ranging list. If a ranging request is received from the modem, send a “Ranging Abort” message. Continue until an “Initial Ranging” message is received or until normal timeout (16 attempts). If the modem does not go back to initial ranging, set it to offline.

The Reset modem state may show as follows in the output of **show cable modem**:

```
Cable4/0/U1 80 resetting 3575 0.25 3 0 10.30.160.26 0050.7318.e965
```

This is an intermediate state. A modem will not be in this state for more than a few seconds; if the modem does not respond, it may be in this state for up to 30 seconds. The subsequent modem state is offline.

Dynamic Upstream Modulation

The Dynamic Upstream Modulation feature reduces the risks associated with transitioning to QAM16 modulation in the return path, and provides assurance that subscribers remain online and connected during periods of return-path impairments.

This new feature actively monitors the signal-to-noise-ratio (SNR) and forward error correction (FEC) counters in the active return path of each upstream port. The software tracks whether the current upstream channel signal quality can adequately support the higher modulation scheme configured, and proactively adjusts to the more robust Quadrature Phase-Shift Keying (QPSK) modulation scheme when necessary. When return-path spectrum conditions improve, the software proactively returns the upstream channel to the higher-modulation quadrature amplitude modulation (QAM) scheme. This is done through modulation profiles supported in Cisco IOS, which can be configured in a variety of ways to support the unique environment at each user's facility.

The Dynamic Upstream Modulation feature can be configured on interfaces with fixed upstream frequencies or on interfaces with spectrum groups assigned. Cisco IOS provides one preconfigured modulation profile resident in memory, which defines a typical profile for QPSK modulation. In order to use the Dynamic Upstream Modulation feature, a second profile must be created that is unique from the first profile and typically provides a higher modulation scheme.

The **cable upstream** <n> **modulation-profile** cable interface command configures the cable interface for the desired modulation profiles.

For more information on the Dynamic Upstream Module feature, including information on creating modulation profiles using the **cable modulation-profile** command, see the *Cisco Release 12.2(4)XF1 Dynamic Upstream Modulation* feature module. For more information on the above commands, see the documents listed in the "Related Documentation" section on page 169.

Internal Modem Configuration File Editor

This feature adds support for internal DOCSIS cable modem configuration file storage and generation. The cable modem configuration file is generated and stored as part of the Cisco IOS configuration file. The DOCSIS configuration files are not stored in Flash memory but are automatically generated when requested for TFTP downloads to cable modems.

Link Up/Down Traps Support (RFC 2233)

The objects in the varbind list, based on Internet Engineering Task Force (IETF) standard, are defined in IF-MIB. Since IF-MIB supports subinterfaces, all objects in this varbind list are also supported for subinterfaces. The feature allows the user to base the Link Up/Down trap varbind list on a Cisco-specific or IETF standard with a new CLI configuration command:

snmp-server link-trap [cisco | ietf]

The default is a Cisco-specific link trap (**snmp-server link-trap cisco**). The user can switch between Cisco and IETF standard.

"MAX-CPE" CLI Override

The following cable-specific configuration command provides a way to override the MAX-CPE parameter in the cable modem's DOCSIS configuration file:

[**no**] **cable modem max-cpe** [<*n*> | unlimited]

When set to unlimited or if *n* is larger than the "MAX-CPE" value in the configuration file of a cable modem, it overrides the config file value.

Note The **cable max-hosts** and **cable modem max-hosts** commands can also be used to set this value for all cable modems on a particular cable interface or for a particular cable modem.

MPLS VPN Support for Subinterfaces

Cisco IOS Release 12.2(4)XF1 includes MPLS support as part of its VPN offerings for cable subinterfaces. The software offers enhancements made to tags placed on the fronts of packets that contain forwarding information used to make switching decisions for cable interfaces and bundles. This tag switching infrastructure combines advanced routing protocol capabilities to define IP VPNs by selectively advertising IP reachability information to just those subscribers within the same VPN or extranet on a cable interface.

The MPLS-VPN approach of creating VPNs for individual Internet service providers (ISPs) requires subinterfaces to be configured on cable interfaces. One subinterface is required for each ISP. The subinterfaces are tied to VPN Routing Forwarding (VRF) tables for respective ISPs.

For more feature information, see the *Cisco Release 12.2(4)XF1 Series MPLS VPN Cable Enhancements* feature module. For information on feature modules, see the "Feature Modules" section on page 170.

Overlapping Subinterface IP Addresses

Multiprotocol Label Switching (MPLS)-based Virtual Private Networks (VPNs), which are created in layer 3, provide privacy and security by constraining the distribution of a VPN's routes to those routers that are members of the VPN only, and by using MPLS forwarding. Each ISP's VPN is insulated from all others sharing the HFC and IP-over-cable infrastructure. MPLS VPN enforces traffic separation by assigning a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what is in the forwarding table.

Earlier Cisco IOS releases assumed that IP addresses were unique, but it is possible with an MPLS VPN to configure overlapped IP addresses within a VRF. A configuration of overlapped IP addresses could have caused errors. Cisco IOS Release 12.1(4)CX and subsequent releases support a configuration of overlapping IP addresses for subinterfaces. The same IP subnet can be configured for CPEs on different VRFs using a Cisco Release 12.2(4)XF1 to configure an MPLS VPN. See also the "MPLS VPN Support for Subinterfaces" section on page 55.

The following CLI commands have been updated to support overlapping IP addresses on subinterfaces:

- Old CLI commands:

  cable host <ipaddr> [**no**] **access-group** <acl>
  cable device <ipaddr> [**no**] **access-group** <acl>
  show cable host <ipaddr> **access-group**
  show cable device <ipaddr> **access-group**
  clear cable host <ipaddr>

- New CLI commands:

  cable host [vrf <vrfname>] <ipaddr> [**no**] **access-group** <ac >
  cable device [vrf <vrfname> <ipaddr> [**no**] **access-group** <acl>
  show cable host [vrf <vrfname>] <ipaddr> **access-group**
  show cable device [vrf <vrfname>] <ipaddr> **access-group**
  clear cable host [vrf <vrfname>] <ipaddr>

Spectrum Management and Dynamic Upstream Modulation

Spectrum management allows the Cisco Release 12.2(4)XF1 series router to sense downstream and upstream plant impairments, report them to a management entity, and automatically mitigate them by changing to a different frequency using a blind hopping algorithm.

The Dynamic Upstream Modulation feature creates two modulation profiles for and upstream. The feature monitors the upstream channel signal quality and determines if the channel can support the primary modulation scheme. If noise or other impairments occur, the feature automatically adjusts to the most robust modulation scheme when necessary. When return path conditions improve, this feature returns the upstream channel to the higher modulation scheme that includes the modulation profile.

SNMP Cable Modem Remote Query

This feature provides a new MIB, CISCO-DOCS-REMOTE-QUERY-MIB, which, once implemented on a CMTS, facilitates SNMP polling of remote CMs. This MIB includes the configuration of the CMTS CM Poller, as well as status objects of remote CMs that are polled by the CMTS CM poller.

The following CLI command has been implemented for turning on the trap:

snmp-server enable cable cm-remote-query

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(15)BC2i that apply to Cisco uBR7100 series universal broadband routers.

Limitions on Upstream Modulation Parameters for PacketCable VoIP Calls

When PacketCable support is enabled on the Cisco CMTS to provide Voice over IP (VoIP) support, the following combinations of upstream modulation parameters should not be used, because the channel width is too small to allow the upstream MAC scheduler to provide sufficient grants for reliable VoIP communications.

The following Table lists unsupported Upstream Parameter Combinations for VoIP Calls:

Table 8 Unsupported Upstream Parameter Combinations for VoIP Calls

Modulation	Channel Width	Minislot Size
QPSK	200 KHz	32, 64, 128
QPSK	400 KHz	16, 32, 64
16-QAM	200 KHz	32, 64, 128
16-QAM	400 KHz	16, 32, 64

We recommend configuring upstreams that are being used for PacketCable operations and VoIP calls for a channel width that is larger than 400 KHz. (These channel widths and upstream parameter combinations can still be used, however, for best-effort data communications.)

Cable Modems Becoming Stuck in the TFTP Transfer State

Cable modems can become stuck in the TFTP transfer state under the following conditions. This state is indicated as “init(o)” by the **show cable modem** command.

- The Dynamic Shared Secret feature is enabled on the cable interface, using the **cable dynamic-secret** command.
- The cable modems on that cable interface are downloading a DOCSIS configuration file that is greater than 4 Kbytes in size.
- A large number of cable modems are registering at the same time. Some or all of those cable modems could also be downloading the DOCSIS configuration file using multiple TFTP transfers that use multiple TFTP ports on the Cisco CMTS router.

This situation can cause the TFTP server to run out of available ports, resulting in the cable modems failing the TFTP download stage. To prevent this situation from happening, temporarily disable the Dynamic Shared Secret feature on the cable interface or reduce the size of the DOCSIS configuration file.

CPE IP Addressing

If the IP address of a DHCP CPE is changed to a currently unused static IP address, the new IP address is not allowed into the CMTS router's host table and the CMTS router's Address Resolution Protocol (ARP) table. Consequently, traffic destined to the static IP address is dropped by the Cisco CMTS router.

Deprecated and Removed Cable MIB Objects

In Cisco IOS Release 12.2(15)BC1 and later releases, the DOCS-IF-EXT-MIB has been deprecated and removed. The objects in this MIB have been replaced by new objects in the DOCS-IF-MIB and the proposed DOCS-RFI-MIB, so as to conform to the requirements given in the *DOCSIS 2.0 Operations Support System Interface Specification* (SP-OSSIv2.0-I04-030730). In particular, the following objects are replaced as indicated:

- docsIfDocsisCapability (replaced by docsIfDocsisBaseCapability)
- docsIfDocsisOperMode (replaced by docsIfDocsisBaseCapability)
- docsIfCmtsCmStatusDocsisMode (replaced by docsIfCmtsCmStatusDocsisRegMode)

Also, the following objects have been removed from traps and notifications in DOCS-CABLE-DEVICE-TRAP-MIB because they duplicate existing objects:

- docsIfDocsisCapability
- docsIfDocsisOperMode

Using cable helper-address and ip helper-address Commands

On the Cisco CMTS, the Cisco IOS software provides two commands to forward User Datagram Protocol (UDP) broadcasts, such as DHCP/BOOTP packets, that are received on an interface—the **ip helper-address** and **cable helper-address** commands.

Use the **ip helper-address** command on all non-cable interfaces, and use the **cable helper-address** command for cable interfaces.

The **cable helper-address** command is optimized for cable interfaces and DOCSIS networks and should be used on cable interfaces instead of the **ip helper-address** command.

For more information on the **ip helper-address** command, refer to the *Cisco IOS Command Reference, Release 12.2 T* index page at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/crftindx.htm

For more information on the **cable helper-address** command, refer to the "Cable Modem Termination System Commands" chapter of the *Cisco Broadband Cable Command Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmts.htm

Synchronization of the System Clocks

Ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with Baseline Privacy Interface Plus (BPI+) operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

Upgrading When Using Shared Secret Passwords

Cisco IOS Release 12.2 BC changed the encryption algorithm used for the **shared-secret** command. If you are upgrading from Cisco IOS Release 12.1 EC or Cisco IOS Release 12.0 SC, you cannot cut and paste the "shared-secret" configuration lines that include an encrypted password. Instead, you must re-enter the original shared secret passwords at the CLI prompt.

For example, if the actual shared secret password is "cm-sharedsecret-password," you would enter the **cable shared-secret cm-sharedsecret-password** command at the CLI prompt. If you have enabled password encryption, the configuration file will then show only the newly encrypted password.

The following example shows a typical configuration session:

```
Router# config t
Router(config)# service password-encryption
Router(config)# int c6/0
Router(config-if)# cable shared-secret cm-sharedsecret-password
Router(config-if)# exit
Router(config)# exit
Router# show running-config | include shared
cable shared-secret 7 0458064B1C294D5C0C1D161211190910673B253B20222D0103
Router#
```

Note This change only affects the encryption of the passwords that are stored in the configuration file. It does not affect the actual encryption that is used between the CMTS and CMs, so you do not need to change the shared secret in the DOCSIS configuration files for the CMs.

SNR Algorithm Updated

Since Cisco IOS Release 12.2(4)BC1, the algorithm for calculating the SNR estimate in the show controllers cable upstream command was refined for a more accurate value. The new SNR estimate uses the algorithm as recommended by the chip manufacturer, and depending on plant characteristics, the new SNR value could be up to 6 dB lower than the values shown in earlier software releases.

Note This value is only an estimate—for the most accurate value, use specialized test equipment like a spectrum analyzer.

Avoiding the Dropping of SNMP Traps

When the **snmp-server enable traps** command is given without any options, it enables all traps, which can generate a significant number of traps at key events, such as system power-up. If the SNMP queue is not large enough to handle all of the traps, new traps will be dropped without notification until the existing traps are sent and slots become available in the queue.

You can do two things to avoid dropping traps in this situation:

- Increase the SNMP trap queue size. The default queue size is 10, which is insufficient to handle all traps. Use the **snmp-server queue-length** *length* global configuration command to increase the queue size. The *length* parameter can range from 10 to 1000. Increase the queue size until traps are no longer dropped.
- Disable unneeded SNMP traps. For example, if you do not need SYSLOG traps (which are sent for every message displayed on the console), disable those traps as follows:

```
router(config)# snmp-server enable traps
router(config)# no snmp-server enable traps syslog
```

DOCSIS 1.0 BPI Support

To conform with a recent change in the DOCSIS 1.0 Baseline Privacy Interface (BPI) Specification, Cisco IOS Release 12.2(8)BC1 and later releases require that the Baseline Privacy Configuration Settings Option (Type 17) must be included in the DOCSIS configuration file for all DOCSIS 1.0 cable modems attempting to register for BPI encryption. If the type 17 option is not included, an "Unauthorized SAID" warning will appear in the CMTS console, and the cable modem will not be allowed to come online.

Previous Cisco IOS Releases allowed DOCSIS 1.0 cable modems to register for BPI encryption and to come online, even if the DOCSIS configuration file did not include the type 17 option. The change to the DOCSIS BPI specification, however, made the type 17 option mandatory for BPI operation.

For more information about this requirement, see the TAC technical note on Cisco.com at http://www.cisco.com/warp/public/109/bpi_changes_23895.html.

Limitation on Vendor-Specific Information in the DOCSIS Configuration File

DOCSIS requires that when the cable modem sends its Registration Request (REG-REQ) message to the CMTS, it must include the configuration information found in the DOCSIS configuration file. This configuration information must include all vendor-specific information fields (VSIF). Because MAC-layer management messages, such as REG-REQ, have a maximum data size of 1522 bytes, this limits the amount of VSIF information that can be included in the DOCSIS configuration file.

In particular, the maximum packet size imposes a limit on the number of Cisco IOS CLI commands you can include as VSIF fields in the DOCSIS configuration file. The exact number of commands that will fit depends on the other information included in the file, as well as the length of each command.

If the REG-REQ message is larger than 1522 bytes, the cable modem will likely report errors similar to the following errors that appear on Cisco uBR900 series cable access routers:

```
%LINK-4-TOOBIG: Interface cable-modem0, Output packet size of 1545 bytes too big
%LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to down
```

In addition, the CMTS will also report that the cable modem timed out during the registration process. If this occurs, you can try the following steps:

- Reduce the length of the commands by using the abbreviated form of the command. For example, you can specify the **int c0** instead of the full command **interface cable-modem0**.
- SNMP MIB objects are not included in the Registration Request message, so wherever possible, replace the CLI commands with the corresponding SNMP MIB object statements in the DOCSIS configuration file.
- If a large number of CLI commands must be given, use VSIF option 128 to download a Cisco IOS configuration file to the cable modem.

For complete details on what is included in the REG-REQ message, see Chapter 6 of the current DOCSIS 1.1 specification (SP-RFIv1.1-I07-010829 or later).

Note This limitation is being tracked by caveat CSCdv83892 but is not expected to be resolved unless the DOCSIS specification is changed to remove the maximum size limit for MAC-layer management messages.

Hot-Standby 1+1 Redundancy Not Supported

The hot-standby 1+1 redundancy feature is not supported on any model of the Cisco uBR7100 series universal broadband router. The HCCP protocol therefore should not be configured on the cable interface using the **hccp** interface configuration commands.

Cable Source-Verify and Routing Configurations

In current Cisco IOS Release 12.2 BC software images, the Cisco CMTS can crash with a “bus error exception” when the **cable source-verify** command is configured on a cable interface, and the routing configuration of that interface is being changed while traffic is passing through the interface.

To avoid this problem, temporarily disable this feature (using **no cable source-verify**) on the interface before you configure the routing parameters. Then after you have finished the routing configuration, reenable the feature using the **cable source-verify** command. Alternatively, you can also change the routing parameters when the interface is not passing traffic (such as when the interface is shut down).

EIGRP, IS-IS, and OSPF Not Supported on Cable Interfaces

The Cisco uBR7100 series router supports advanced routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF) only on the WAN interfaces, not on the cable interfaces. On cable interfaces, use a routing protocol that is supported by the cable modems, such as RIPv2.

Configuring the Routing Protocol Causes a Reset of the Cable Modems

Be aware that when configuring a routing protocol on a Cisco uBR7100 series router, the Cisco IOS software must reset the interfaces to enable the change. This normally does not significantly affect operations on the interface, except that when this is done on a cable interface, it causes all cable modems on that particular downstream to reinitialize, potentially interfering with data transmission on that downstream. Therefore, you should use the routing protocol global configuration commands, such as **router rip**, only when a minimum of subscribers would be affected.

Field Notices and Bulletins

- Field Notices—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/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.
- Product Bulletins—If you have an account on Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.
- *What's New for IOS — What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

Limitations and Restrictions

The following limitations and restrictions apply to Cisco IOS Release 12.2(11)BC3c.

Transparent LAN Service over Cable

The Transparent LAN Service over Cable feature in Cisco IOS Release 12.2(11)BC3 has the following restrictions and limitations:

- The virtual connections (VC) on the ATM interface must be configured to use ATM Adaptation Layer 5 (AAL5) IEEE 802.1a SubNetwork Attachment Point (SNAP) encapsulation. On Cisco routers, this means that each PVC endpoint must be configured for the proper encapsulation using the encapsulation aal5snap command.
- If a cable modem is being mapped to an ATM PVC, all of its CPE traffic is sent through the ATM tunnel through the ATM cloud, even if the ultimate destination is another cable modem on the same CMTS.
- Cable modems must have a one-to-one mapping with ATM PVCs, with each cable modem being mapped to its own ATM PVC. Cable modems cannot share a single PVC. Multiple PVCs from the same customer are aggregated at the ATM bridge aggregator into the same bridge group.

The spanning tree protocol cannot be used with devices (cable modems, their CPE devices, and the endpoint CPE devices) that are using this feature. In particular, the spanning tree protocol cannot be used between the ATM bridge aggregator and the endpoint customer devices.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Supported MIBs

The Cisco uBR7100 series universal broadband routers support the following categories of MIBs:

- SNMP standard MIBs—These MIBs are required by any agent supporting SNMPv1 or SNMPv2 network management.
- Cisco's platform and network-layer enterprise MIBs—Common across most of Cisco's router platforms. If your network management applications are already configured to support other Cisco routers, such as the Cisco 2600 series or Cisco 7200 series, no further configuration is needed unless the version of Cisco IOS software being used has updated these MIBs.
- Cable-specific MIBs—Provide information about the cable interfaces and related information on the Cisco uBR7100 series routers. They include both DOCSIS-specific MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the Cisco uBR7100 series routers, these MIBs must be loaded.
- Deprecated MIBs—Supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network Management applications and scripts should convert to the replacement MIBs as soon as possible.

The cable-specific MIBs are described in the following section. For information on the SNMP standard MIBs and Cisco's platform and network-layer enterprise MIBs, see Cisco's MIB web site at
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cable-Specific MIBs

Table 9 shows the cable-specific MIBs that are supported on the Cisco uBR7100 series universal broadband routers. The table also provides a brief description of each MIB's contents and the Cisco IOS software release in which the MIB was initially functional—earlier releases might have had unsupported prototype versions of the MIB; later releases might have added new attributes and functionality. Because of interdependencies, the MIBs must be loaded in the order given in the table.

Note The names given in Table 9 are the filenames for the MIBs as they exist on Cisco's FTP site (ftp://ftp.cisco.com/pub/mibs/ or http://www.cisco.com/public/mibs). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames.

Table 9 Cable-Specific MIBs Supported on Cisco uBR7100 Series Routers

MIB Filename	Description	Introduced in Release
SNMPv2-SMI.my SNMPv2-SMI-V1SMI.my	This module specifies the Structure of Management Information (SMI) for SNMPv2, as defined in RFC 1902.	12.1(5)EC1
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in RFC 1903.	12.1(5)EC1
SNMPv2-MIB.my SNMPv2-MIB-V1SMI.my	The management protocol, SNMPv2, provides for the exchange of messages that convey management information between the agents and the management stations, as defined in RFC 1907.	12.1(5)EC1
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the SMI for Cisco's enterprise MIBs.	12.1(5)EC1
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco's enterprise MIBs.	12.1(5)EC1
IF-MIB.my IF-MIB-V1SMI.my	This module describes generic objects for the Layer 3 network interface sublayers. This MIB is an updated version of MIB-II's *if* table and incorporates the extensions defined in RFC 2233.	12.1(5)EC1
DOCS-IF-MIB.my DOCS-IF-MIB-V1SMI.my	This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems and cable modem termination systems, as defined in RFC 2670.	12.1(5)EC1

Table 9 Cable-Specific MIBs Supported on Cisco uBR7100 Series Routers (continued)

MIB Filename	Description	Introduced in Release
DOCS-BPI-MIB.my	This module—available in an SNMPv2 version only—describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS.	12.1(5)EC1
CISCO-DOCS-EXT-MIB.my CISCO-DOCS-EXT-MIB-V1SMI.my	This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as QoS attributes and connection status and other information regarding the cable modems and CPE devices supported by the CMTS.	12.1(5)EC1
CISCO-DOCS-REMOTE-QUERY-MIB.my	This module facilitates SNMP polling of remote CMs on a CMTS.	12.1(5)EC1
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.1(5)EC1

Deprecated MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 10.

Table 10 Replacements for Deprecated MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB

Table 10 Replacements for Deprecated MIBs (continued)

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Note Some of the MIBs listed in Table 10 represent feature sets that are not supported on Cisco uBR7100 series universal broadband routers.

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. If you have an account with Cisco.com, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to Cisco.com, press **Login**, and then go to **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

All caveats in Cisco IOS Release 12.2 T and specifically in Cisco IOS Release 12.2(15)T6 are also in Cisco IOS Release 12.2(15)BC2i.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.2 T and is located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Cisco IOS Release 12.2(15)BC2i and earlier releases are listed in this section.

Note If you have an account on Cisco.com, you can use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Technical Support**: **Tools & Utilities: Software BUG TOOLKIT (under Configuration Tools)**. Another option is to enter the following URL in your web browser or go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats for Release 12.2(15)BC2i

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2i and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC2i.

Closed and Resolved Caveats for Release 12.2(15)BC2i

The caveats listed in Table 12 are resolved in Cisco IOS Release 12.2(15)BC2i. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 11 Closed and Resolved Caveats for Release 12.2(15)BC2i

Caveat ID Number	Description
CSCei61732	Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution. Cisco has made free software available that includes the additional integrity checks for affected customers. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.
CSCei76358	Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

Open Caveats for Release 12.2(15)BC2h

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2h and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC2h.

Closed and Resolved Caveats for Release 12.2(15)BC2h

The caveats listed in Table 12 are resolved in Cisco IOS Release 12.2(15)BC2h. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 12 Closed and Resolved Caveats for Release 12.2(15)BC2h

Caveat ID Number	Description
CSCef68324	Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation. Cisco has made free software available to address this vulnerability for all affected customers. More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml..

Open Caveats for Release 12.2(15)BC2g

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2g and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC2g.

Closed and Resolved Caveats for Release 12.2(15)BC2g

The caveats listed in Table 35 are resolved in Cisco IOS Release 12.2(15)BC2g. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 13 Closed and Resolved Caveats for Release 12.2(15)BC2g

Caveat ID Number	Description
CSCef93215	A router configured for OSPF may reload unexpectedly and reference the “ospf_build_one_paced_update” process. This issue is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The issue may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA. There are no known workarounds.
CSCeh20178	Stablize periodic station maintenance scheduling. This fix is necessary for cable domains with more then 2000 modems on a single downstream. There are no known workarounds.

Open Caveats for Release 12.2(15)BC2f

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2f and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC2f.

Closed and Resolved Caveats for Release 12.2(15)BC2f

The caveats listed in Table 14 are resolved in Cisco IOS Release 12.2(15)BC2f. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2f

Caveat ID Number	Description
CSCed78149	TCP connections may be vulnerable to spoofed ICMP packets. A spoofed ICMP packet may cause the TCP connection to use a very low segment size for 10 minutes at a time. This issue is observed when TCP connections are configured for PMTU discovery. Note that PMTU discovery is disabled by default on a router. Workaround: Disable PMTU discovery.
CSCee67450	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. Cisco has made free software available to address this problem. This issue is tracked by CERT/CC VU#689326. This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml
CSCee76342	When running PacketCable call, without setting secondary RKS ip address in Event-Generation-Info object in Gate-Set message, the CMTS may unexpectedly reloads. Workaround: Set secondary RKS ip address in Event-Generation-Info object. It can even be a fake one.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2f (continued)

Caveat ID Number	Description
CSCef07105	Cable modems will come online fine to online(pt) state, but the following messages will fill up the logs : `%UBR10000-4-NOCFGFILE: Cannot read modem config file whatever.bin from <TFTP_IP_addr>: Unknown error` This only occurs when “cable dynamic-secret” enabled. Sniffer packet capture for “TFTP port 69” shows the malformed TFTP packets from UBR10K. Workaround: Disable “cable dynamic-secret”.
CSCef80943	IOS on MC28U or MC520 cable line card may unexpectedly reload. The stack in the crashinfo file will contiguously list 17 or more ip addresses in a secondary address range configured for the chassis. The IP addresses are addresses of CPEs behind a single modem. The unexpected reload will only occur if SNMP queries that list or count CPE ip addresses are executed. There must be more than 16 CPEs behind a cable modem to cause a stack overwrite. If there are 23 or more CPEs, the stack overwrite is severe enough to unexpectedly reload. Workarounds: Change the cable modem config file to allow a maximum of 16 CPEs behind a modem. Alternative Workaround: Stop all snmp queries for CPE ip addresses. Stop queries for the docsIfCmtsCmStatusEntry snmp table.
CSCef86926	On MC28U linecard with advanced spectrum management, modulation change does not occur when CNR is below the configured thresolds. There are no known workarounds.
CSCeg01817	A ubr7246vxr running 12.2(15)BC2a may unexpectedly reload due to memory corruption issues. The trigger is unknown. There are no known workarounds.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2f (continued)

Caveat ID Number	Description

CSCeg11416	A cable-modem on a distributed line card is seen as "not registered" by the NPE but seen as "online" by the LC. A sample router log is shown below. Both commands are run on the NPE; the first command gets data from an NPE table, the second command gets data from the distributed LC. When a CM enters this out-of-sync situation, packets from the CM will be silently dropped by the CMTS.
	`----`
	`uBR-13#show cable modem 0007.0e01.7d9d`
	`MAC Address  IP Address  I/F  MAC  Prim`
	`RxPwr  Timing  Num BPI`
	`State  Sid  (dB)`
	`Offset  CPE Enb`
	`Cable modem with MAC address 0007.0e01.7d9d not registered.`
	
	`uBR-13#show cable modem | incl 0007.0e01.7d9d`
	`MAC Address  IP Address  I/F  MAC  Prim`
	`RxPwr  Timing  Num BPI`
	`State  Sid  (dB)`
	`Offset  CPE Enb`
	`0007.0e01.7d9d 192.168.0.1  C4/0/U0  online  3  0.00`
	`5701  0  N`
	
	`uBR-13#`
	`----`
	
	This issue is observed on a ubr7200 running code version 12.3(9a)BC and 12.2(15)BC2c.
	
	The CMTS usually appears to running normally for about 1 week before the bug is seen.
	
	Workaround: This issue is difficult to detect because no message is displayed on the CMTS when the situation occurs. The only known workaround is to run a script that scans the MAC addresses of CMs, and if the situation is detected, reset the CM.

CSCeg24134	SNMP agent in ubr7200 routers running 12.2(15)BC2 and above will not return values for the MIB table ipNetToMediaTable, even if there are no snmp views configured. Workaround: IOS version 12.2(15)BC1 seems to work properly.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2f (continued)

Caveat ID Number	Description

CSCeg27950	FLAP-LIST is not aging properly in 12.2(15)BC2c. If tested with 12.2(15)BC2b, then it shows properly.
	The box was reloaded and all was working as desired for a day or so and then it was broken again.
	A recreate was performed with the same code and the same symptoms were seen.
	The lab config shows: "cable flap-list aging 1440" so the flap-list is not supposed to have line with more than 24 hours the following occurred:
	`MAC Address Upstream Ins Hit Miss CRC P-Adj Flap Time`
	`0040.7b74.cb4c Cable5/0/0/U0 0 24162 164 0 1168 1172 Oct 12 03:43:43`
	`000f.9f78.6d54 Cable5/0/0/U0 0 23780 188 0 440 442 Oct 9 13:51:52`
	`000a.739a.2c34 Cable5/0/0/U0 2 25332 526 0 279 293 Oct 12 06:48:13`
	`0020.40d8.8688 Cable5/0/0/U0 0 24575 380 0 177 192 Oct 12 05:01:26`
	`00a0.731f.6865 Cable5/0/0/U0 0 24094 220 0 30 33 Oct 10 07:39:27`
	`000a.735d.7b63 Cable5/0/0/U0 0 23944 208 0 21 25 Oct 12 08:40:46`
	There are no known workarounds.

CSCeg32660	Extra UGS grants are being sent by CMTS scheduler. This cause an issue with certain brands of eMTAs causing robotized voice. This issue occurs in a ubr7246vxr running 12.2(15)BC2a and 20ms interval voice traffic. There are no known workarounds.
CSCeg40945	The CMTS database may not correctly updated with the ip address of the CPE, and the following message is generated for the CPE mac address abcd.efgh.ijkl.mnop: `Failed to find CM with SID # 0, not to glean from thisDHCP packet DHCPGLEAN abcd.efgh.ijkl.mnop cmts glean failed` This issue occurs under the following conditions: – The Cisco UBR is configured for MPLS VPN – The CPE requesting an ip address is on one cable sub-interface x/0.n – The DHCP server is one another cable sub-interface y/0.p – The cable interfaces have to be different There are no known workarounds.
CSCeg68008	Reverse arp might fail on the CMTS for Ethernet (WAN/LAN) interfaces. This issue may occur anytime on the CMTS during normal operation. There are no known workarounds.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2f (continued)

Caveat ID Number	Description
CSCeg76058	Internal dhcp server on the CMTS in not working only in 12.2(15)BC2f throttle branch. Modems fail to complete dhcp - stay in init(d). The CMTS is fine with the external dhcp server. Release 12.3(9a)BC1 does not show this problem for modems, however, this release will fail for CPEs to come online with internal dhcp server. Workaround: Using an external dhcp server.
CSCin33783	Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an Gigabit Ethernet interface may prevent customer edge-to-customer edge (CE-to-CE) pings from going through. This issue is observed when Ethernet over Multiprotocol Label Switching (EoMPLS) is configured in VLAN mode on the Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1) on a Cisco 7200 series. Workaround: Configure EoMPLS in VLAN mode on a port adapter such as a Gigabit Ethernet or Fast Ethernet port adapter.
CSCin75000	MC28U may reset. Re-initialization of the card may lead to the NPE unexpectedly reloading. There are no known workarounds.
CSCsa44474	a UBR7200 router may reload due to a bus error There are no known workarounds.

Open Caveats for Release 12.2(15)BC2e

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2e and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC2e.

Closed and Resolved Caveats for Release 12.2(15)BC2e

The caveats listed in Table 15 are resolved in Cisco IOS Release 12.2(15)BC2e. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e

Caveat ID Number	Description
CSCdy01705	A Cisco router may experience high cpu utilization at process TTY Background when the command **logging synchronous** is configured under line con 0. Workaround: Remove the command **logging synchronous** from line con 0. However, this should only be performed during a scheduled maintenance window, as the router could pause indefinitely just after removal of the command and may require a manual reboot of the router.
CSCed27848	UBR with IOS 12.2(15)BC1 and 12.2(15)BC1a has a problem with loading startup-config after reload with BPI+ configuration and cable modems. When BPI+ is enabled in a cable modems' config file after reload CMTS doesn't load startup-config. This is version specific 12.2(15)BC1 and 12.2(15)BC1a seems to have this issue. There are no known workarounds.
CSCee61429	The MC28u, MC28x, MC16u, and MC16x real time clock drifts from the NPE clock. Due to a code omission in IOS 12.2(15)CX, 12.2(15)BC1a-e, and 12.2(15)BC2a-d, the real time clock on the MC28u, MC28x, MC16u, and MC16x Cable Line Cards for the uBR7246VXR is not kept in sync with the real time clock on the NPE. The estimated drift is approximately +/- 1.3 minutes per month, and is somewhat temperature sensitive. The linecard clock is updated each time the system is reloaded, but not afterwards. The linecard clock is not updated even if NTP is configured on the NPE. The drift can cause a problem where modems will eventually be in the reject(ts) state if the modem config file is set to contain a timestamp (see CSCef71411) and the drift is greater than 30 seconds. Workaround: If possible, write a script to periodically extract the current time from the NPE and login to the linecard using if-con/if-quit and set the time to the NPE value. Alternative workaround 1: Reload during a service window. Alternative workaround 2: Turn off timestamp.
CSCef04492	snmpwalk on cdrqCmtsCmStatusTable does not show consistent result. There are no known workarounds.

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef09586	If DHCP server in one of the configured VRF's has IP address that is matching broadcast address of the IP subnetwork used in another VRF (another subinterface), than cable modems will not come on-line and stay in init(d). This issue occurs if the user has DHCP server in VRF1 using IP address 10.2.16.15 and configure **ip address 10.2.16.1 255.255.255.240** on subinterface that belongs to VRF2. This issue has been noticed with following tested images: 12.2(11)BC2 and 12.2(15)BC1d. Workaround: Changing IP address of the DHCP server or changing IP address scope in another VRF will resolve this issue.
CSCef09770	Each flow appear in a different time with a different sid in docsIfCmtsServiceTable, but the docsIfCmtsServiceCreateTime are the same for all sids. There are no known workarounds.
CSCef19398	Momentary (about 1 second) of ping packet lost was observed when changing downstream modulation rate on another cable interface on the same line card. Once DS cable interface is reinitialized, ping operation returns to normal (successful reception of ping packets). There are no known workarounds.
CSCef20890	A Cisco ubr7246VXR running Cisco IOS Release 12.2(15)BC1 may reload unexpectedly due to a bus error. There are no known workarounds.
CSCef27943	The following error message is displayed at inappropriate times: `DSG tunnel MAC address already defined in DOCSIS` The following three valid configuration sequences have been incorrectly flagged with the above error message: 1. add/remove/readd of a DSG mapping on a cable bundle master interface. 2. mapping more than 1 IP address to a tunnel on a cable bundle master interface. 3. Configuring an RFC1112 based DSG tunnel and an non-DSG static IP multicast group which both use the same MAC address on a cable bundle master interface. Workaround: For the first sequence listed above, a shut/no shut will turn of the cable bundle master and will allow the DSG tunnel to be readded. No workaround exists for the other 2 sequences.
CSCef31956	This caveat improves reverse arp lookup on the CMTS for modem bringup. There are no known workarounds.

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef37495	Sync Pulse failure detection mechanism is not working for N+1/7200 solution. Workaround: Use Fast Failure Detection for crash detection.
CSCef46191	A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected. All other device services will operate normally. User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected. There are no known workarounds. The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef54205	If an MTA has multiple lines and both the lines are being used to make calls, call failures could happen in certain scenarios. Examples: Scenario 1: Line 1 has a call in progress, meanwhile, Line 2 makes a new call, then hangs up, and makes another new call, then hangs up, and so on. After sometime line 2 will not be able to make a call. Scenario 2: Line 1 is having a call, Line 2 makes a new call. Before Line 2 hangs up, Line 1 hangs up and makes another call. Same for Line 2, it hangs up and makes another call _before_ Line 1 hangs up, and vice versa. After sometime line 1 and 2 will not be able to make new calls. This issue occurs because activity count on the CMTS does not get decremented in each of the above scenarios (even if the call on a line goes away). As a result the activity count reaches its limit and new calls are not allowed. However, at any instance, if both lines are disconnected, the activity count will be reset again. Workaround: Increase the activity count on BTS to a large number. This way, even if the activity counts are not decremented at call termination, new calls will be allowed till the activity count is maxed out. When both the lines are terminated, the count will be reset automatically. In the case where the MTA contains 2 lines only, it should not have a big impact since it won't use up a lot of resources even if someone is trying to abuse the system by making multiple calls simultaneously. Moreover, it is a counter issue only, all the actual resources, such as service-flows, gates, etc, they are all freed up.
CSCef59093	Cisco uBR-MC28U cable interface line card may unexpectedly reload in an ubr7200 series CMTS running IOS release 12.2(15)BC2b. The issue only occurs with MC28U line card. MC16C in the same chassis works fine. There are no known workarounds.

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef68286	A cable modem termination system (CMTS) may record a traceback when you either remove a Fast Ethernet (FE) member interface of an EtherChannel interface by entering the **shutdown** interface configuration command or you add an FE member interface to an EtherChannel interface by entering the **no shutdown** interface configuration command. This issue is observed on a Cisco uBR7200 series when IP unicast traffic is sent in both the downstream and the upstream direction. Workaround: When new member FE interface is added to the EtherChannel interface, take the following steps: 1. Enter the **shutdown** interface configuration command on both the new FE member interface and the EtherChannel interface. 2. Add the FE member interface by entering the **channel-group** *port-channel-number* interface configuration command on the FE member interface. 3. Enter the **no shutdown** interface configuration command on the Etherchannel interface. When an FE member interface is remove from the EtherChannel interface, take the following steps: 1. Enter the **shutdown** interface configuration command on the EtherChannel interface. 2. Remove the FE member interface by entering the **no channel-group** *port-channel-number* interface configuration command on the FE member interface. 3. Enter the **no shutdown** interface configuration command on the Etherchannel interface.
CSCef70739	A “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error is displayed at the console and the “Active links” for the **show ip nbar resources** command will show 4 GB plus. This issue occurs when the NBAR feature is activated, i.e when “match protocol <protocol-name>” is included in a policy map, or “ip nbar protocol-discovery” is applied on an interface, the “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error may appear on the console. Workaround: Perform **no ip nbar resources** to reset active links back to zero.

Table 15 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef73242	Cisco ubr7200 series CMTS running IOS release 12.2(15)BC2b may not guarantee configured QoS levels on Downstream dynamic Service Flows in VoIP networks. The issue can be seen with very high SFIDs (between 32768 and 65535) and when cable modems are provisioned with non-zero Active QoS Timeout. Workaround: Increase the bandwidth for Best Effort (BE) flow.
CSCin82407	Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server. Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources. This advisory will be posted to http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

Open Caveats for Release 12.2(15)BC2c

All the caveats listed in Table 16 are open and reported in Cisco IOS Release 12.2(15)BC2c. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 16 Open Caveats for Cisco IOS Release 12.2(15)BC2c

Caveat ID Number	Description
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCed10546	Ping can use wrong interface ip address as source ip address. This issue only occurs if a load balancing with CEF is performed. There are no known workarounds.
CSCed27848	UBR with IOS 12.2(15)BC1 and 12.2(15)BC1a has a problem with loading startup-config after reload with BPI+ configuration and cable modems. When BPI+ is enabled in a cable modems' config file after reload CMTS does not load startup-config. This is version specific 12.2(15)BC1 and 12.2(15)BC1a seems to have this issue. There are no known workarounds.
CSCed64701	Unexpected packet loss at a certain rate and frame size and the overrun incrementing on the interface can be observed on the GigaEthernet Interfaces. There are no known workarounds.

Table 16 Open Caveats for Cisco IOS Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCee02297	A CPE behind a cable modem should be allowed to assume the IP address of a previous CPE behind the same cable modem. Currently, if a new CPE does have to assume its IP address behind a particular CM like this, one has to perform a "clear cable host" on the CMTS so that the CMTS releases the IP/MAC binding for the previous CPE with the CM its behind. There are no known workarounds.
CSCee52091	Demand for IPv6 is growing and some governments are requiring that their networks to support ipv6 natively. This DDTS is to request that support for IPv6 is enabled on cable interfaces. There are no known workarounds.
CSCee76997	A Software forced crash, PC 0x60659EFC when I/O card inserted. There are no known workarounds.
CSCee80483	UBR7246VXR running 12.2(15)BC2a crashes due to watchdog timeout. UBR7246VXR unexpectedly reloads due to watchdog timeout when a cable modem entry is cleared per the following snip: `clear cable modem X.X.X.X delete` UBR7200-3-BADARPDELETE: Tried to remove arp entry for X.X.X.X that is not dynamicProcess aborted on watchdog timeout, process = DHCPD Receive. +++++++++ X.X.X.X represents IP address of the cable modem. There are no known workarounds.
CSCef00276	UBR7200 reboots unexpectedly with an Bus error address 0xE2. There are no known workarounds.
CSCef04492	snmpwalk on cdrqCmtsCmStatusTable does not show consistent result. There are no known workarounds.
CSCef09574	Extended ping is OK with IOS 12.1.19ECx. After upgraded to 12.2.15.BC1, user with privilege level 14 could not execute **extended ping** command. Workaround: IOS 12.1.19ECx works fine.
CSCef19528	CMTS records alignment errors after "debug cable keyman" is turned on. Workaround: Do not turn "debug cable keyman" on.
CSCef19578	The **no debug cable map** command does not work to turn off the "debug cable map". Workaround: The undebug all (aliased to "u all") works.
CSCef20891	CMTS fails to send encrypted multicast traffic for CPEs that are behind BPI+ enabled modems. There are no known workarounds.

Table 16 Open Caveats for Cisco IOS Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCef24304	Router crashed with software forced crash. The trigger is unknown. From the log, it indicates that router unexpectedly reloads with watchdog timeout. There was no config changes or interruptions made to the router when this occurred. There are no known workarounds.

CSCin21618	A uBR7246 with an OC-12 SRP interface can crash with the following sequence of commands:
	`test pas oir 2 pull`
	`test pas oir 2 push`
	`test pas oir 1 pull`
	`test pas oir 1 push`
	Workaround: Do not “test pas oir” the high slot of a double wide card. “test pas oir 1 pull” followed by a push can be done repeatedly without error.

CSCin45061	Mobile host functionality does not work. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2c

The caveats listed in Table 17 are resolved in Cisco IOS Release 12.2(15)BC2c. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 17 Closed and Resolved Caveats for Release 12.2(15)BC2c

Caveat ID Number	Description
CSCeb46870	Service Assurance Agent (SAA) running on Cisco Routers with versions 12.2(10.7)T2 or later can sometime report wrong values for “Number of operations attempted” and “Number of operations skipped”. The issue is observed in a probe if that probe is running for more than 49 days. Workaround: Restart the probe which have the problem.
CSCec27338	Network Based Access Recognition (NBAR) is used to classify packet streams. When packet streams contain packets that are fragmented, it’s important that all the fragments for a packet traverse the same router running NBAR. If some packets are dropped or routed around a particular router running NBAR, then that can cause high CPU. This is a result of the fragment table getting too large when all fragments of a packet are not presented to NBAR. There are no known workarounds.

Table 17 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCed49726	When DMIC is enabled, the CMTS needs to download the config file from the provisioning server. if the CMTS cannot download the file, the modems cannot register. Work around: Configure the management network such that the CMTS can download the CM config file from the provisioning server.
CSCed61686	Using a local ToD Server when MPLS/VPN is configured was not routing ToD packets correctly. This fix allows Local ToD Time server to be configured with MPLS/VPN. There are no known workarounds.
CSCed86260	When two Cable interface are bundled, the ifInUcastPkts of the secondary cable interface is decreasing. There are no known workarounds.

CSCed89815	A bus error may occur on a Cisco router when **trace** command is enabled.When **show version** EXEC command is entered, the following error messages may be displayed:
	`System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY`
	0xXXXXXXXX represents the program counter at which the router reloads. 0xYYYYYYYY represents the address at which the router reloads.
	This issue is observed on a Cisco router that runs Cisco IOS Release 12.2(15)BC1.The platform would be UBR7200. The following is a sample command:
	`trace www.a.net`
	More information on Bus error can be gathered off the following link:
	http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
	There are no known workarounds.

CSCee26361	A DHCPACK or DHCPNACK with a chaddr == 0 is not forwarded by the Cisco DHCP stack to the cable CMTS code when the CMTS is a relay agent. The DHCP stack must forward such a reply to the CMTS code so that the CMTS can make a decision on an active or inactive lease on the DHCP server. There are no known workarounds.
CSCee29081	CMTS does nor receive the DHCP response to a DHCP lease query even though the response was sent from the DHCP server. CSCee26361 fixed this problem. What this DDTS is now adding is a check in CMTS code to not continue with dhcp gleaning if a response to a lease query is received by the CMTS. There are no known workarounds.

Table 17 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCee32609	The CMTS may report a CPU hog error when processing GetBulk SNMP requests. There are no known workarounds.

CSCee48935	Tracebacks on a UBR7200.
	IOS (tm) 7200 Software (UBR7200-K8P-M), Version 12.2(15)BC1b.
	When the issue occurs, a lot of cable modems in status init(r1) are seen.
	Workaround: Resetting the interface solves the problem.
	Log Buffer (1000000 bytes):
	`*May 6 07:10:37.886: %SYS-2-LINKED: Bad enqueue of 639A4B24 in queue 629DAFE0`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 45`
	`-Traceback= 6083B6F0 604B4530 6051DEC4 604D3E50 604B34C8 604B031C 604B0544 6056D2F4`
	
	`*May 6 07:10:37.886: %SYS-2-NOTQ: unqueue didn't find 6391FAC8 in queue 629DAFE0`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 45`
	`-Traceback= 6083B8F8 604B44A8 604D2AD0 604D3E20 604B34C8 604B031C 604B0544 6056D2F4`
	
	`*May 6 07:10:37.890: %SYS-2-LINKED: Bad enqueue of 6391FAC8 in queue 629DAFE0`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 45`
	`-Traceback= 6083B6F0 604B4530 6051DEC4 604D3E50 604B34C8 604B031C 604B0544 6056D2F4`
	
	`*May 6 07:10:38.238: %SYS-2-NOTQ: unqueue didn't find 63A15470 in queue 629DAFE0`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 45`
	`-Traceback= 6083B8F8 604B44A8 604D2AD0 604D3E20 604B34C8 604B031C 604B0544 6056D2F4`
	
	`*May 6 07:10:38.242: %SYS-2-LINKED: Bad enqueue of 63A15470 in queue 629DAFE0`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 45`
	`-Traceback= 6083B6F0 604B4530 6051DEC4 604D3E50 604B34C8 604B031C 604B0544 6056D2F4`

CSCee49594	The ENTITY-MIB does not recognize the NPE-G1 processor. There are no known workarounds.
CSCee55989	When SNMP query getnext/getbulk DOCS-QOS-MIB: docsQosCmtsMacToSrvFlowTable (docsQosCmtsIfIndex), NMS will see the infinite loop if the number of CMs is greater than 1000. All the platforms are affected. Workaround: Use cli to get the info. If only docsQosCmtsIfIndex is needed, use the CM mac address, snmp get exact cdxCmCpeIfIndex which is the same value as docsQosCmtsIfIndex.

Table 17 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCee64504	A CPUHOG may occur for about 4.5 seconds when you enter the **show running-config** command. This issue is observed on a Cisco uBR10000 series but may also occur on other platforms. Workaround: Do not enter the **show running-config** command. Rather, enter the **show config** command.
CSCee66672	High CPU might be seen when OIR cable linecard if CM onoff trap is enabled and throttled. Workaround: Disable the CM onoff trap before OIR. No cable enable-trap cmonoff-notification.
CSCee81149	With IOS 12.2(15)CX, it is possible to configure 125 KHz steps. With IOS 12.2(15)BC2a, it is not possible to configure 125 KHz steps. A change was made to minimum frequency step size since the original release of MC28u in 12.2(15)CX. This was done in order to support alternate suppliers of upconverter modules. This change restricts the step size to 250 Khz increments. That is why 168.125 Mhz is not accepted by 12.2(15)BC2a software. There are no known workarounds.
CSCef22962	If BPI is enabled, DSx messages with key sequence number 0 are rejected. There are no known workarounds except waiting until the key sequence number changes and retrying the command.

Open Caveats for Release 12.2(15)BC2b

All the caveats listed in Table 18 are open and reported in Cisco IOS Release 12.2(15)BC2b. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 18 Open Caveats for Cisco IOS Release 12.2(15)BC2b

Caveat ID Number	Description
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCed10546	Ping can use wrong interface ip address as source ip address. This issue only occurs if do load balancing with CEF is performed
CSCed27848	UBR with IOS 12.2(15)BC1 and 12.2(15)BC1a has a problem with loading startup-config after reload with BPI+ configuration and cable modems. When BPI+ is enabled in a cable modems' config file after reload CMTS doesn't load startup-config. This is version specific 12.2(15)BC1 and 12.2(15)BC1a seems to have this issue. There are no known workarounds.

Table 18 Open Caveats for Cisco IOS Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCed64701	Unexpected packet loss at a certain rate and frame size and the overrun incrementing on the interface can be observed on the GigaEthernet Interfaces. There are no known workarounds.
CSCed86260	When two Cable interface are bundled, the ifInUcastPkts of the secondary cable interface is decreasing. There are no known workarounds.
CSCee02297	A CPE behind a cable modem should be allowed to assume the IP address of a previous CPE behind the same cable modem. Currently, if a new CPE does have to assume its IP address behind a particular CM like this, one has to perform a “clear cable host” on the CMTS so that the CMTS releases the IP/MAC binding for the previous CPE with the CM its behind. There are no known workarounds.
CSCin21618	OC-12 CMTS got hanged with OIR on SRP interface. There are no known workarounds.
CSCin45061	Mobile host functionality does not work. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2b

The caveats listed in Table 19 are resolved in Cisco IOS Release 12.2(15)BC2b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2b

Caveat ID Number	Description
CSCed06848	With DMIC turned on, CMs may not be able to download IOS config files. If a CM is online and tries to download an IOS.cfg file from the same tftp server as specified in the DHCP offer, it will fail. The problem only happens with DMIC turned on and seen on CMs (e.g., Cisco CMs in routing mode), that try downloading a second config file after coming online. There are no known workarounds.

CSCed36625	On cable routers, including uBR7200s and uBR10ks, CPE OSs such as Linux and FreeBSD may appear to frequently change the mac address of their gateway IP address. Linux will show:
	
	`Dec 15 00:12:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	`Dec 15 00:13:26 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:a8 to 00:01:42:1d:4d:54 on dc0`
	`Dec 15 00:26:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	
	FreeBSD will show:
	
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:54 to 00:08:e2:33:0c:70 on ed0`
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:70 to 00:08:e2:33:0c:54 on ed0`
	
	This issue occurs when cable bundling is configured. Modems and CPEs on the bundle slave interface(s) will experience the problem. Those on the master interface will not experience it.
	
	The problem is that the L2 header for arp replies and arp requests are not consistent on a bundle slave. An arp reply will have a source mac in the L2 header of the bundle slave interface. A broadcast arp request will have a source mac of the bundle master and the arp request packets will have a mac source of the bundle master.
	
	Workaround: In theory, using a static arp entry on the CPE device binding the gateway IP address to the mac address of the CMTS slave interface will prevent the CPE from changing its arp entry for the gateway.

CSCed61110	Cisco ubr7200 series CMTS running IOS release 12.2(15)BC1 may experience a software-forced crash after a watchdot timiout in CMTS MAC Timer process. The failure occurred on a platform with NPE-G1. There are no known workarounds.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCed83867	uBR7246VXR with NPE-1G and MC28U blades with 'cable source-verify dhcp'enabled results in: 1. 100% CPU load and flooding the CNR with service queries, the contributor to high CPU load is identified to be 'DHCPD Receive' process. 2. The few mac-address in the arp entry shows all zeros Workaround: Turning off the "cable source-verify dhcp" option in the config will bring the CPU back down.
CSCed88709	When a service-policy that corresponds to a policy-map with no fair-queueing classes is applied outbound on a Cable interface and one class performs shaping the uBR7200 may drop outbound packets and generate error messages similar to `%LINK-4-BADQID: Interface Cable4/0, bad output queue ID specified (265). Packet dropped` when the shaping classes becomes active because of traffic rates that exceed the prescribed limits in the class. Workaround: Have at least one class with a fair-queueing configuration in the policy-map. This means using one of the "bandwidth", "priority", or "fair-queue" commands within the policy-map for at least one class.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description

CSCed95436	uBR7246VXR may run into a issue with the Total-Kbyte Value being to high when issuing the <Show Subscriber-Usage> command.
	This behavior has been observed on 12.2(15)BC1 and 12.2(15)BC1b.
	Example:
	`uBR7246VXR#show cable subscriber-usage over-consume`
	`Sfid Mac Address Enforce-rule Total-Kbyte Last-detect`
	`Last-penalty Pen`
	`Name Count time`
	`time Flag`
	`761 0000.0000.0002 RESA1-UP 4294967087 Mar10 21:55:01`
	`Mar10 22:55:01 Act`
	`762 0000.0000.0002 RESA1-DOWN 4294967270 Mar10 21:55:01`
	`Mar10 22:55:01 Act`
	
	`uBR7246VXR#show cable modem 0000.0000.0002 counters`
	`MAC Address US Packets US Bytes DS Packets DS Bytes`
	`0000.0000.0002 1631 219278 1467 1187222`
	
	`cable qos enforce-rule RESA1-UP`
	`penalty-period 60`
	`registered qos-profile 92`
	`enforced qos-profile 12`
	`monitoring-duration 120`
	`activate-rule at-byte-count 38400 upstream enforce`
	`enabled`
	
	`cable qos enforce-rule RESA1-DOWN`
	`penalty-period 60`
	`registered qos-profile 92`
	`enforced qos-profile 12`
	`monitoring-duration 120`
	`activate-rule at-byte-count 450000 downstream enforce`
	`enabled`
	
	`cable qos profile 12 max-burst 1544`
	`cable qos profile 12 max-downstream 575`
	`cable qos profile 12 max-upstream 128`
	
	`cable qos profile 92 max-burst 1544`
	`cable qos profile 92 max-downstream 1600`
	`cable qos profile 92 max-upstream 128`
	
	There are no known workarounds.

CSCee12282	A uBR7246VXR CMTS router with output QMC traffic-shaping enabled and active on a cable interface can leak processor pool memory under high load, i.e. when multiple particles are used for packet buffering. Workaround: Remove output QMC shaping command from cable interface to stop leak; reload router to reclaim memory.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCee16342	The CMTS may crash when the following command is issued: "show packetcable gate <gateid>" The crash would happen if the command is issued during the time duration when that particular gate is being deleted (e.g., as a result of call teardown) There are no known workarounds.
CSCee12868	docsIfCmtsCmStatusSignalNoise returns a wrong value. It should represent 10th dB rather than just dB. Workaround: Multiply the received number by 10.
CSCee20869	In order to protect from DOS service attacks on the CMTS, it is decided to add per SID basis throttling of lease queries and global rate limit for lease queries initiated by downstream traffic. This is meant to reduce the CPU utilization of DHCP Receive process & ISR context when "cable source-verify dhcp" and "no cable arp" is configured. There are n o known workarounds.
CSCee21114	When "source-verify dhcp" and "no cable arp" is configured, DHCP lease query response for dst address of pkts coming from the back-haul is dropped. CPE is unreachable from the back-haul until the CPE itself send an ARP or IP packet. Workaround: Do not configure "no cable arp".
CSCee23838	If a downstream packet received at the CMTS is destined for a modem whose ARP entry is incomplete or not present in the CMTS arp database, the CMTS goes into a loop of issuing out DHCP lease queries and receiving ACKs till an upstream packet for the modem populates the ARP database on the CMTS. Workaround: Disable "no cable arp" on the cable interface.
CSCee27443	Second service flow can not be created if Docsis 1.0+ vendor specific encodings are used for data transfer. This is regression issue which was triggered by CSCeb21271 and CSCdz66185. Workaround: For any TOS except 5 the second DS flow will be created BUT we will end up reserving bandwidth for those flows.
CSCee27994	The default ranging-backoff value should be changed from "auto" to values of 3 6. Workaround: Hard code the ranging-backoff values to 3 6.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCee37649	Under high load with BPI active, the ubr7200 may lock up, permitting no console access. Higher level protocols will be unresponsive (for example, the system will not respond to ARP requests). The system may still forward packets. Workaround: Take off the load for a period of time (physically disconnect all connected modems) until the system recovers. Alternative Workaround: Disable BPI on systems with constantly high CPU load.
CSCee46490	Customers and internal tech support have a need to monitor the status and collect debug information from the RF cards with on-board processors (e.g., MC520 and MC28U). This is currently done by using telnet or if-con to login to the line card and issue show commands to collect the data. Logging into the line card should only be done by the direction of a Cisco support person. New options to the existing “show controllers” CLI command will be added to collect line card data from the NPE. Workaround: Telnet or if-con to the line card.
CSCee47911	The number of errors on the “show interface cable x/y upstream z” has increased dramatically after upgrading to 12.2(15)BC2a. This problem is appearing on theMC28C. This does not appear to be affecting packet loss. There are no known workarounds.
CSCee55916	Users can logon to RF line cards with onboard processors without having “service internal” configured on the NPE/PRE. This issue occurs when the user executes the telnet CLI command to logon to an RF line card without “service internal” configured. There are no known workarounds.
CSCee55444	See CSCed06821 for modem security details which prevents modems from coming online and getting stuck in init(o). Modems which get an ip address which is not the same subnet as the primary ip address of the cable interface can get stuck in init(o). Workaround: Use the **ip source-interface loopback 0** command.
CSCin71529	When the cable QoS permission for the modems is disabled, the qos profile created by the modem may not be removed from the QoS profile table. Also, if a cable interface is shutdown or if one issues a “clear cable modem cax/y/z all delete” on the CMTS, the qos profile feature gets broken for deletion of qos profiles - the profile should be deleted, but it won't since the internal reference count of the profile is messed up. There are no known workarounds.

Open Caveats for Release 12.2(15)BC2a

All the caveats listed in Table 20 are open and reported in Cisco IOS Release 12.2(15)BC2a. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a

Caveat ID Number	Description
CSCdx62698	This problem was observed while doing spot checking for CMTS image. Workaround: To prevent CPE behind the Cable modem to accessing the CMTS, the interface specific access-group can be configured as a workaround.
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCea13693	When there are about 2800 cable modems connected to a cable interface, a few hundred cable modems will go offline in a short period of time. It is recommended to have no more than 2000 cable modems connected to a cable interface. There are no known workarounds.
CSCec09369	Under certain circumstances the reporting of CPU utilization could be inaccurate. This could occur if the timed scheduling of upstream traffic coincides exactly with the system clock that is used to calculate system timing for an extended period of time. There are no known workarounds.
CSCed06848	With DMIC turned on, CMs may not be able to download IOS config files. If a CM is online and tries to download an IOS.cfg file from the same tftp server as specified in the DHCP offer, it will fail. The problem only happens with DMIC turned on and seen on CMs (e.g., Cisco CMs in routing mode), that try downloading a second config file after coming online. There are no known workarounds.
CSCed10546	Ping can use wrong interface ip address as source ip address. This is happen only if we do load balancing with CEF There are no known workarounds.
CSCed12040	Cable source-verify needs to be modified to cater for internal changes within IOS. There are no known workarounds.
CSCed27848	UBR with IOS 12.2(15)BC1 and 12.2(15)BC1a has a problem with loading startup-config after reload with BPI+ configuration and cable modems. When BPI+ is enabled in a cable modems' config file after reload CMTS doesn't load startup-config. This is version specific 12.2(15)BC1 and 12.2(15)BC1a seems to have this issue. There are no known workarounds.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description

CSCed36625	On cable routers, including uBR7200s and uBR10ks, CPE OSs such as Linux and FreeBSD may appear to frequently change the mac address of their gateway IP address. Linux will show:
	`Dec 15 00:12:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	`Dec 15 00:13:26 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:a8 to 00:01:42:1d:4d:54 on dc0`
	`Dec 15 00:26:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	
	`FreeBSD will show:`
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:54 to 00:08:e2:33:0c:70 on ed0`
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:70 to 00:08:e2:33:0c:54 on ed0`
	
	This issue occurs when cable bundling is configured. Modems and CPEs on the bundle slave interface(s) will experience the problem. Those on the master interface will not experience it.
	
	The problem is that the L2 header for arp replies and arp requests are not consistent on a bundle slave. An arp reply will have a source mac in the L2 header of the bundle slave interface. A broadcast arp request will have a source mac of the bundlemaster and the arp request packets will have a mac source of the bundle master.
	
	Workaround: In theory, using a static arp entry on the CPE device binding the gateway IP address to the mac address of the CMTS slave interface will prevent the CPE from changing its arp entry for the gateway.

CSCed42120	Cisco ubr7200 series CMTS installed with NPE-G1 Network Processor Engine and running IOS release 12.2(15)BC1 may show high amount of uncorrectable FEC errors. The issue occurs only when upstream cable interfaces are configured with a non-default modulation profile optimized to use long grants for voice. IOS releases 12.2(15)BC1b, 12.2(15)CX, 12.2(15)CX1 show the same symptoms. Workaround: Use the default modulation profile.
CSCed44559	uBR7246 experiencing performance issue under IOS version ubr7200-k8p-mz.122-15.BC1a.bin Some indication of the performance issue is 1. high number of input errors and ignored on FastEthernet 2/0 2. high cpu spikes sometimes Because the input rate is rather lower than 100Mbps, customer complains the performance capability of uBR7246. There are no known workarounds.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed47892	CPU interrupt burst to 100% immediately from 50% The console will hang for 5 to 10 minutes. The CMTS stops forwarding traffic but does not crash. After the hang, normal operation resumes until the next hang. There are no known workarounds.
CSCed61110	Cisco ubr7200 series CMTS running IOS release 12.2(15)BC1 may experience a software-forced crash after a watchdot timiout in CMTS MAC Timer process. The failure occurred on a platform with NPE-G1. There are no known workarounds.
CSCed83867	uBR7246VXR with NPE-1G and MC28U blades with cable source-verify dhcp'enabled results in: 1. 100% CPU load and flooding the CNR with service queries, the contributor to high CPU load is identified to be 'DHCPD Receive' process. 2. The few mac-address in the arp entry shows all zeros Workaround: Turning off the "cable source-verify dhcp" option in the config will bring the CPU back down.
CSCed86260	When two Cable interface are bundled, the ifInUcastPkts of the secondary cable interface is decreasing. There are no known workarounds.
CSCed88709	When a service-policy that corresponds to a policy-map with no fair-queueing classes is applied outbound on a Cable interface and one class performs shaping the uBR7200 may drop outbound packets and generate error messages similar to `%LINK-4-BADQID: Interface Cable4/0, bad output queue ID specified (265). Packet dropped` when the shaping classes becomes active because of traffic rates that exceed the prescribed limits in the class. Workaround: Have at least one class with a fair-queueing configuration in the policy-map. This means using one of the **bandwidth**, **priority**, or **fair-queue** commands within the policy-map for at least one class.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed95436	uBR7246VXR may run into a issue with the Total-Kbyte Value being to high when issuing the <Show Subscriber-Usage> command. This behavior has been observed on 12.2(15)BC1 and 12.2(15)BC1b. ex. uBR7246VXR#show cable subscriber-usage over-consume Sfid Mac Address Enforce-rule Total-Kbyte Last-detect Last-penalty Pen Name Count time time Flag 761 0000.0000.0002 RESA1-UP 4294967087 Mar10 21:55:01 Mar10 22:55:01 Act 762 0000.0000.0002 RESA1-DOWN 4294967270 Mar10 21:55:01 Mar10 22:55:01 Act uBR7246VXR#show cable modem 0000.0000.0002 counters MAC Address US Packets US Bytes DS Packets DS Bytes 0000.0000.0002 1631 219278 1467 1187222 cable qos enforce-rule RESA1-UP penalty-period 60 registered qos-profile 92 enforced qos-profile 12 monitoring-duration 120 activate-rule at-byte-count 38400 upstream enforce enabled cable qos enforce-rule RESA1-DOWN penalty-period 60 registered qos-profile 92 enforced qos-profile 12 monitoring-duration 120 activate-rule at-byte-count 450000 downstream enforce enabled cable qos profile 12 max-burst 1544 cable qos profile 12 max-downstream 575 cable qos profile 12 max-upstream 128 cable qos profile 92 max-burst 1544 cable qos profile 92 max-downstream 1600 cable qos profile 92 max-upstream 128 This issue was discovered after a period of time. Currently amount of time and circumstances in which the event takes places are being explored. There are no known workarounds.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description

CSCee09491	The cmts running 12.1(19)EC1 has experienced that some cms were stucking in init(r1) state with continuous following messages.
	`Log messages:`
	`Mar 22 18:40:56 KST: %SYS-2-LINKED: Bad enqueue of 62783A24 in queue 61EA4ECC`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 40`
	`-Traceback= 60650134 60332F48 60380A3C 603351E0 60332700 60332928 603929F4 60392EDC 6063136C 60631358`
	`Mar 22 18:42:52 KST: %SYS-2-NOTQ: unqueue didn't find 6272FBC8 in queue 61EA4ECC`
	`-Process= "CMTS MAC Timer Process", ipl= 3, pid= 41`
	`-Traceback= 60650340 60332EB0 6035F284 60381914 6035EA88 6063136C 60631358`
	Workaround is to OIR the MC16c in question.

CSCee11283	ubr7246vxr(config-if)#cable up 0 power-adjust continue ? <2-15> Power level in dB The default “continue ranging” value in CMTS software to date is 1 dB. This value is an arbitrary value in the software and does not reflect Cisco RF Engineering best practices recommendation of a window of 3-6. The 1 dB window can unnecessarily cause cable modems to attempt to come online and then fall offline and repeat this cycle thus causing customers to have intermittent network connectivity. Workaround: Change the command on the CMTS to open the window by hand: cable up X power-adjust continue 4
CSCee12270	A uBR7256VXR CMTS router with cable bundling, subscriber management, NBAR, and output QMC traffic-shaping enabled can crash in cmts_safe_start with %ALIGN-1-FATAL access to addr=0x3 errors. There are no known workarounds.
CSCee12282	A uBR7246VXR CMTS router with output QMC traffic-shaping enabled and active on a cable interface can leak processor pool memory under high load, i.e. when multiple particles are used for packet buffering. Workaround: Remove output QMC shaping command from cable interface to stop leak; reload router to reclaim memory.
CSCin21618	OC-12 CMTS got hanged with OIR on SRP interface. There are no known workarounds.
CSCin36946	When a OIR pull is done on the Fastethernet interface which is part of a FastEtherchannel, the interface may still remain as member of the port-channel. And the packet input rate counter may not decrement to zero after the above OIR operation. There are no known workarounds.
CSCin45061	Mobile host functionality does not work. There are no known workarounds.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCin55008	After a OIR operation on the links which form part of the etherchannel, the channel group config on the links is lost. There are no known workarounds.
CSCeb61346	Changing the cable interface queueing configuration does not update the "show" and "running config" correctly. This issue occurs during change output policy on the 7200 There are no known workarounds, but the desired queueing will take effect, even though it does not show up in the "show" or "running config" correctly.
CSCed64701	Unexpected packet loss at a certain rate and frame size and the overrun incrementing on the interface can be observed on the GigaEthernet Interfaces. There are no known workarounds.
CSCee02297	A CPE behind a cable modem should be allowed to assume the IP address of a previous CPE behind the same cable modem. Currently, if a new CPE does have to assume its IP address behind a particular CM like this, one has to perform a "clear cable host" on the CMTS so that the CMTS releases the IP/MAC binding for the previous CPE with the CM its behind. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2a

The caveats listed in Table 21 are resolved in Cisco IOS Release 12.2(15)BC2a. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 21 Closed and Resolved Caveats for Release 12.2(15)BC2a

Caveat ID Number	Description
CSCed91527	The Request Collision counter does not appear to be incrementing on the MC8u card, when using the show controller command. There are no known workarounds.
CSCee06228	The SRP protocol on a ubr7246vxr running 12.2(15)BC1b may not fully initialize during the boot sequence if one side is wrapped. Workaround: Force a wrap using "srp ips request forced-switch <x>" and remove this forced wrap. Note this would have to be done manually after a reload/reboot.
CSCee17648	MAC Scheduler incorrectly Calculates max-unfrag-sz resulting in packet loss. Workaround: Modify Modulation profile so max burst option matches that of max-unfrag-sz.

Open Caveats for Release 12.2(15)BC2

All the caveats listed in Table 22 are open and reported in Cisco IOS Release 12.2(15)BC2. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2

Caveat ID Number	Description
CSCdx62698	This problem was observed while doing spot checking for CMTS image. Workaround: To prevent CPE behind the Cable modem to accessing the CMTS, the interface specific access-group can be configured as a workaround.
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCea13693	When there are about 2800 cable modems connected to a cable interface, a few hundred cable modems will go offline in a short period of time. It is recommended to have no more than 2000 cable modems connected to a cable interface. There are no known workarounds.
CSCec09369	Under certain circumstances the reporting of CPU utilization could be inaccurate. This could occur if the timed scheduling of upstream traffic coincides exactly with the system clock that is used to calculate system timing for an extended period of time. There are no known workarounds.
CSCed06848	With DMIC turned on, CMs may not be able to download IOS config files. If a CM is online and tries to download an IOS.cfg file from the same tftp server as specified in the DHCP offer, it will fail. The problem only happens with DMIC turned on and seen on CMs (e.g., Cisco CMs in routing mode), that try downloading a second config file after coming online. There are no known workarounds.
CSCed10546	Ping can use wrong interface ip address as source ip address. This is happen only if we do load balancing with CEF There are no known workarounds.
CSCed12040	Cable source-verify needs to be modified to cater for internal changes within IOS. There are no known workarounds.
CSCed27848	UBR with IOS 12.2(15)BC1 and 12.2(15)BC1a has a problem with loading startup-config after reload with BPI+ configuration and cable modems. When BPI+ is enabled in a cable modems' config file after reload CMTS doesn't load startup-config. This is version specific 12.2(15)BC1 and 12.2(15)BC1a seems to have this issue. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCed36625	On cable routers, including uBR7200s and uBR10ks, CPE OSs such as Linux and FreeBSD may appear to frequently change the mac address of their gateway IP address. Linux will show:
	`Dec 15 00:12:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	`Dec 15 00:13:26 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:a8 to 00:01:42:1d:4d:54 on dc0`
	`Dec 15 00:26:17 home /kernel: arp: 192.168.0.1 moved from 00:01:42:1d:4d:54 to 00:01:42:1d:4d:a8 on dc0`
	
	`FreeBSD will show:`
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:54 to 00:08:e2:33:0c:70 on ed0`
	`arp: 10.0.0.1 moved from 00:08:e2:33:0c:70 to 00:08:e2:33:0c:54 on ed0`
	
	This issue occurs when cable bundling is configured. Modems and CPEs on the bundle slave interface(s) will experience the problem. Those on the master interface will not experience it.
	
	The problem is that the L2 header for arp replies and arp requests are not consistent on a bundle slave. An arp reply will have a source mac in the L2 header of the bundle slave interface. A broadcast arp request will have a source mac of the bundlemaster and the arp request packets will have a mac source of the bundle master.
	
	Workaround: In theory, using a static arp entry on the CPE device binding the gateway IP address to the mac address of the CMTS slave interface will prevent the CPE from changing its arp entry for the gateway.

CSCed42120	Cisco ubr7200 series CMTS installed with NPE-G1 Network Processor Engine and running IOS release 12.2(15)BC1 may show high amount of uncorrectable FEC errors. The issue occurs only when upstream cable interfaces are configured with a non-default modulation profile optimized to use long grants for voice. IOS releases 12.2(15)BC1b, 12.2(15)CX, 12.2(15)CX1 show the same symptoms. Workaround: Use the default modulation profile.
CSCed44559	uBR7246 experiencing performance issue under IOS version ubr7200-k8p-mz.122-15.BC1a.bin Some indication of the performance issue is 1. high number of input errors and ignored on FastEthernet 2/0 2. high cpu spikes sometimes Because the input rate is rather lower than 100Mbps, customer complains the performance capability of uBR7246. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed47892	CPU interrupt burst to 100% immediately from 50% The console will hang for 5 to 10 minutes. The CMTS stops forwarding traffic but does not crash. After the hang, normal operation resumes until the next hang. There are no known workarounds.
CSCed61110	Cisco ubr7200 series CMTS running IOS release 12.2(15)BC1 may experience a software-forced crash after a watchdot timiout in CMTS MAC Timer process. The failure occurred on a platform with NPE-G1. There are no known workarounds.
CSCed83867	uBR7246VXR with NPE-1G and MC28U blades with 'cable source-verify dhcp'enabled results in: 1. 100% CPU load and flooding the CNR with service queries, the contributor to high CPU load is identified to be 'DHCPD Receive' process. 2. The few mac-address in the arp entry shows all zeros Workaround: Turning off the "cable source-verify dhcp" option in the config will bring the CPU back down.
CSCed86260	When two Cable interface are bundled, the ifInUcastPkts of the secondary cable interface is decreasing. There are no known workarounds.
CSCed88709	When a service-policy that corresponds to a policy-map with no fair-queueing classes is applied outbound on a Cable interface and one class performs shaping the uBR7200 may drop outbound packets and generate error messages similar to `%LINK-4-BADQID: Interface Cable4/0, bad output queue ID specified (265). Packet dropped` when the shaping classes becomes active because of traffic rates that exceed the prescribed limits in the class. Workaround: Have at least one class with a fair-queueing configuration in the policy-map. This means using one of the **bandwidth**, **priority**, or **fair-queue** commands within the policy-map for at least one class.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed95436	uBR7246VXR may run into a issue with the Total-Kbyte Value being to high when issuing the <Show Subscriber-Usage> command. This behavior has been observed on 12.2(15)BC1 and 12.2(15)BC1b. ex. uBR7246VXR#show cable subscriber-usage over-consume Sfid Mac Address Enforce-rule Total-Kbyte Last-detect Last-penalty Pen Name Count time time Flag 761 0000.0000.0002 RESA1-UP 4294967087 Mar10 21:55:01 Mar10 22:55:01 Act 762 0000.0000.0002 RESA1-DOWN 4294967270 Mar10 21:55:01 Mar10 22:55:01 Act uBR7246VXR#show cable modem 0000.0000.0002 counters MAC Address US Packets US Bytes DS Packets DS Bytes 0000.0000.0002 1631 219278 1467 1187222 cable qos enforce-rule RESA1-UP penalty-period 60 registered qos-profile 92 enforced qos-profile 12 monitoring-duration 120 activate-rule at-byte-count 38400 upstream enforce enabled cable qos enforce-rule RESA1-DOWN penalty-period 60 registered qos-profile 92 enforced qos-profile 12 monitoring-duration 120 activate-rule at-byte-count 450000 downstream enforce enabled cable qos profile 12 max-burst 1544 cable qos profile 12 max-downstream 575 cable qos profile 12 max-upstream 128 cable qos profile 92 max-burst 1544 cable qos profile 92 max-downstream 1600 cable qos profile 92 max-upstream 128 This issue was discovered after a period of time. Currently amount of time and circumstances in which the event takes places are being explored. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCee09491	The cmts running 12.1(19)EC1 has experienced that some cms were stucking in init(r1) state with continuous following messages.
	`Log messages:`
	`Mar 22 18:40:56 KST: %SYS-2-LINKED: Bad enqueue of 62783A24 in queue 61EA4ECC`
	`-Process= "CMTS MAC Protocol", ipl= 3, pid= 40`
	`-Traceback= 60650134 60332F48 60380A3C 603351E0 60332700 60332928 603929F4 60392EDC 6063136C 60631358`
	`Mar 22 18:42:52 KST: %SYS-2-NOTQ: unqueue didn't find 6272FBC8 in queue 61EA4ECC`
	`-Process= "CMTS MAC Timer Process", ipl= 3, pid= 41`
	`-Traceback= 60650340 60332EB0 6035F284 60381914 6035EA88 6063136C 60631358`
	Workaround is to OIR the MC16c in question.

CSCee11283	ubr7246vxr(config-if)#cable up 0 power-adjust continue ? <2-15> Power level in dB The default “continue ranging” value in CMTS software to date is 1 dB. This value is an arbitrary value in the software and does not reflect Cisco RF Engineering best practices recommendation of a window of 3-6. The 1 dB window can unnecessarily cause cable modems to attempt to come online and then fall offline and repeat this cycle thus causing customers to have intermittent network connectivity. Workaround: Change the command on the CMTS to open the window by hand: cable up X power-adjust continue 4
CSCee12270	A uBR7256VXR CMTS router with cable bundling, subscriber management, NBAR, and output QMC traffic-shaping enabled can crash in cmts_safe_start with %ALIGN-1-FATAL access to addr=0x3 errors. There are no known workarounds.
CSCee12282	A uBR7246VXR CMTS router with output QMC traffic-shaping enabled and active on a cable interface can leak processor pool memory under high load, i.e. when multiple particles are used for packet buffering. Workaround: Remove output QMC shaping command from cable interface to stop leak; reload router to reclaim memory.
CSCin21618	OC-12 CMTS got hanged with OIR on SRP interface. There are no known workarounds.
CSCin36946	When a OIR pull is done on the Fastethernet interface which is part of a FastEtherchannel, the interface may still remain as member of the port-channel. And the packet input rate counter may not decrement to zero after the above OIR operation. There are no known workarounds.
CSCin45061	Mobile host functionality does not work. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCin55008	After a OIR operation on the links which form part of the etherchannel, the channel group config on the links is lost. There are no known workarounds.
CSCeb61346	Changing the cable interface queueing configuration does not update the "show" and "running config" correctly. This issue occurs during change output policy on the 7200 There are no known workarounds, but the desired queueing will take effect, even though it does not show up in the "show" or "running config" correctly.
CSCed64701	Unexpected packet loss at a certain rate and frame size and the overrun incrementing on the interface can be observed on the GigaEthernet Interfaces. There are no known workarounds.
CSCee02297	A CPE behind a cable modem should be allowed to assume the IP address of a previous CPE behind the same cable modem. Currently, if a new CPE does have to assume its IP address behind a particular CM like this, one has to perform a "clear cable host" on the CMTS so that the CMTS releases the IP/MAC binding for the previous CPE with the CM its behind. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2

The caveats listed in Table 23 are resolved in Cisco IOS Release 12.2(15)BC2. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2

Caveat ID Number	Description
CSCdu13269	If the router is low on memory it may print out the foll. error messages. The router may become non functional. There are no known workarounds.
CSCdy66891	When a cable modem receives a docsis binary file with network access disabled and bpi enabled, the CMTS will show it in the "online(pt)" state instead of "online(d)". Workaround: Remove BPI from the docsis binary file.
CSCdz58997	Under Cisco IOS Release 12.2(11)BC1b, show cable modem phy shows DSpwr in wrong way. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCdz80580	A DPT-OC-12 port adapter (PA-SRP) may stop transmitting packets. This issue is observed on a Cisco uBR7200 series when a packet that is smaller than 8 bytes is transmitted on the PA-SRP. Workaround: Perform an online insertion and removal (OIR) of the PA-SRP.
CSCea53868	The CMTS may display the error below after an N+1 switch over. `%UBR7200-4-BAD_REGISTRATION: Cable modem <mac> on interface Cable x/y when online attempted re-registration with different QoS` There are no known workarounds.
CSCea61100	The iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical. entPhysicalTable.entPhysicalEntry.entPhysicalSerialNum will return an incomplete chassis serial number. Only integer values minus any leading zeros are returned by the mib. There are no known workarounds.
CSCea85575	Need way to find out how long a currently online cable modem has been online. There are no known workarounds.
CSCeb08941	There is no error/warning message if user issues “test cable ucc” on a non-existing cable modem. There are no known workarounds.
CSCeb27416	The CMTS may record a AAA related traceback with spurious memory access while running Bulk calls. There are no known workarounds.

CSCeb33495	In ubr7246 VXR/NPE-G1, after router crash, the ROM monitor may not recover from exception and stuck in infinite loop with the following error messages:
	`*** TLB (Load/Fetch) Exception ***`
	`Access address = 0x100`
	`  PC = 0xbfc0d968, SP = 0x87fffbf0, RA = 0xbfc0efc0`
	`  Cause Reg = 0x00000008, Status Reg = 0x30408003`
	`ROM Monitor Can Not Recover From Exception`
	`A Board Reset Is Issued`
	The only way to recovery it is power off/on.
	There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb34574	Executing the cable modem qos profile command may generate a misleading message indicating that the modem could not be found even though it is listed in the show cable modem command display. The problem occurs if the command fails for one of the following reasons. 1. The QoS profile specified by the command was not created by the CMTS. 2. The modem's existing QoS profile for it's primary SID was created by a modem registration request. Either of these conditions will cause the command to fail as described in the CMTS configuration guide. The show cable qos profile command can be used to determine if the specified profile was created by the CMTS. The show cable modem registration command can be used to determine which profile the modem is using. There are no known workarounds.
CSCeb38067	All the modems on legacy LC which uses asic version of BRCM3210 MAC chip, such as MC16C and MC28C, might go offline suddenly and stay offline forever until human intervention. When this problem happens, you need to shut/no shut or clear the affected interface to restore all cable modems to online. This problem impacts both 12.1EC and 12.2BC. There are no known workarounds.
CSCeb54552	After upgrade from EC train to BC2 train, ubr7200 face issue with modem staying off-line intermittently This was seen with an upstream that was configured with a fix initial ranging interval There are no known workarounds.
CSCeb56433	If the **traffic-shape...** command is configured on a ubr7200 CMTS interface, the following error message may be seen: `%LINK-4-BADQID: Interface Cable6/1, bad output queue ID specified (265). Packet dropped -Traceback= 60898D48 60944AD8 605819AC 613285E0 6132867C 606971C4 600FD8C4 60133F04` There are no known workarounds.
CSCeb63130	No DSD-REQ is sent to MTA to clean up DOCSIS service flow resource when CMTs receives gate-delete msg from CMS with gate state in RESERVED or COMMITTED. There are no known workarounds.
CSCeb63747	Modems may be online with a 0.0.0.0 ip address. To recover from this situation, ping from the CMTS to the modem. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb63785	CMTS will accept DSA-REQ intended to share the same resource ID that is in use by other service flow. There are no known workarounds.
CSCeb64909	During codec change, if MTA issue BW request with both adm/act bit set in qos set type TLV, CMTS does not compare it against the authorized flow spec, and can cause BW reject even if it is within authorized BW. Workaround: Do not use single phase DSC-REQ.
CSCeb70360	After users issue “test cable ucc cx/y <sid> <us_chid>” or “test cable ucc cx/y <sid> <us_chid> 0”, the CM offline counter is incremented by 1 whereas in fact the modem did not go offline at all. The offline counter can be retrieved by issuing “sh cab modem <mac> connectivity” in 12.2BC. Workaround: Use “test cable ucc cx/y <sid> <us_chid> 3” for those modems which support it. If a modem does not support the above, then there are no known workarounds.
CSCeb73924	When IGMP join is received from slave interface before configuring IGMP static group on master interface, multicast traffic is not forwarded to the master interface. Workaround: Remove and reapply the multicast static group configurations on the master.
CSCeb73924	When IGMP join is received from slave interface before configuring IGMP static group on master interface, multicast traffic is not forwarded to the master interface. Workaround: Remove and reapply the multicast static group configurations on the master
CSCeb82402	Pings from cable interface of a UBR running 12.1(13)EC4 are failing whenever interface in CEF switching mode has an access-list. Workaround: Use the **no ip route-cache cef** command on the interface fixes the problem.

CSCeb84099	In Cisco ubr7200 with MC16S card, after reload, one may see DSP image download failed for this MC16S card, such as:
	`*Feb 29 07:26:38.987: %UBR7200-3-DBDSPERR5: DSP failed to respond to Host Handshake`
	`*Feb 29 07:26:38.987: %UBR7200-5-DBDSPRECOVER1: Trying to switch to backup dsp image`
	`*Feb 29 07:26:40.483: %UBR7200-3-DBDSPERR5: DSP failed to respond to Host Handshake`
	After this happened, ubr7200 will crash, such as:
	`*** System received a Bus Error exception ***`
	`signal= 0xa, code= 0xc08, context= 0x62271434`
	`PC = 0x00000000, SP = 0x62364330, RA = 0x6056966c`
	`Cause Reg = 0x00000c08, Status Reg = 0x3400e103`
	Workaround: replace the problem MC16S card.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb85140	The CMTS may record a spurious traceback related to GC connection handle. There are no known workarounds.
CSCec01689	The router will reload when a L3 cache parity error happens. Typically this is due to cache parity expection in the L3 cache. This commit changes the parity exception handling mechanism on the NPE-400 on uBR7200, where the router will automatically recover from the parity error exception in most of the cases (it's estimated that the recovery can happen in 70% of the parity error occurrence instances) without reloading the box. This mechanism used to be only supported for NPE300. After this commit, it will only be supported on NPE300 and NPE400. There are no known workarounds.
CSCec02495	When the GBIC on a UBR/NPE-G1 is removed and reinserted the **show interface** command or the **show controllers** command may indicate that the newly inserted GBIC is missing or unknown. This is only cosmetic and will not affect the operation of the router. There are no known workarounds.
CSCec03980	The UGS information described in the CISCO-DOCSEXT-MIB does not show up in 12.2 BC code. There are no known workarounds.
CSCec04003	An UBR7246VXR seems to “freeze” frequently for some time, stops responding to management, forwarding traffic, and are very slow trying to access it using telnet. When we do a show proc cpu we see that: the highest CPU user is: `35  75661096  46089930  1641 81.06% 84.50% 85.08%  0 CMTS MAC Protoco` Workaround: Enable CEF switching if possible. CEF was enabled to solve the scaling those exact scaling problems that the virus appears to exacerbate Alternative Workaround: Configure service internal ip route-cache 30 2 3 or less severe ip route-cache 30 10 10 In order to reduce the route cache size Refer to the following for more information about these two workarounds: http://www.cisco.com/warp/public/707/advisory.html http://www.cisco.com/warp/customer/63/ts_codred_worm.shtml

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec08579	With N+1 enabled, the Protect CMTS may crash with the error below if the identical modulation profiles are not configured on Working and Protect CMTS: `"Null Init Mtn Burst Descriptor in MAC scheduler init"` Workaround: Configure Working and Protect CMTS with the same modulation profiles.
CSCec13012	When issuing the **Show Cable Subscriber-usage** command, the CMTS does not pause with the --More-- prompt between multiple screens of output. There are no known workarounds.
CSCec14844	On uBR7200/uBR7100, if there are too many CM/CPEs, there could be CPU HOG error messages when user issues “clear cab modem all delete” or “clear cab modem all reset”. Workaround: Lower the number of CM/CPEs.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec15728	On a uBR7100 CMTS Modular QoS via the CLI are not configurable in 122-15.BC1 feature set ubr7100-ik8s-mz in which this feature is supported. They are configurable in previous IOS's. ex. class-map match-any MAIL match protocol pop3 match protocol smtp match protocol nntp match protocol secure-pop3 match protocol secure-nntp class-map match-any MULTIMEDIA match protocol netshow match protocol streamwork match protocol vdolive match protocol cuseeme match protocol realaudio class-map match-any FILEXFER match protocol ftp match protocol secure-ftp match protocol nfs match protocol printer class-map match-any HTTP match protocol http match protocol secure-http match protocol gopher class-map match-any FILESHARE match protocol gnutella match protocol napster match protocol fasttrack class-map match-all FILESHARE-WAN match class-map FILESHARE match not access-group 190 class-map match-all HTTP-WAN match class-map HTTP match not access-group 190 class-map match-all MULTIMEDIA-WAN match class-map MULTIMEDIA match not access-group 190 class-map match-all FILEXFER-WAN match class-map FILEXFER match not access-group 190 class-map match-all MAIL-WAN match class-map MAIL match not access-group 190 These commands are no longer configurable: ubr7111-A(config)#class-map match-any MAIL ^ % Invalid input detected at '^' marker. This Problem has only been observed on a uBR7100 platforms with IOS 122-15.BC1. The problem does not occur on the ubr7200. Workaround: Use a previous IOS to use these features.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec16832	When a PCR value is defined for an ATM PVC on a uBR7246VXR running 12.2(11)BC3 images, the PCR definition is not accepted. CBR values are properly applied to the ATM circuit. This can be observed in the **sh atm pvc** command. There are no known workarounds.
CSCec17509	When a batch event message is sent after the call ends, the BCIDs in the message become bogus. There are no known workarounds.

CSCec17997	When a large number of modems are on a single upstream it takes them a long time to get to (r1) state. The root cause is that the algorithm for automatically adjusting the ranging backoff window was broken in BC. The work around is to fix the ranging backoff to a large value:
	`cable up 0 ranging 6 9`
	Additional improvement is reached by configuring this on all upstreams if all upstreams share the same frequency.
	Additional optimization is reached by decreasing the IM interval:
	`cable insertion interval automatic 20 250`
	There are no known workarounds.

CSCec21275	Need to hide the following commands: - debug cable capture-map - show cable map-capture There are no known workarounds.
CSCec21392	“no-persistence”, when set, is not displayed and saved in the running configuration. Workaround: Configure no-persistence again after router reload.
CSCec26636	User can configure spectrum group bands in the frequency range of 5-65 MHz. Current implementation allows user to assign a spectrum group to an upstream that may not be compatible with the upstream operating mode. For example, cable spectrum-group 1 band 20000000 40000000 cable spectrum-group 1 band 50000000 65000000 interface cablex/y cable downstream annex B cable upstrean <n> spectrum-group 1 In this case, spectrum group 1 should not be assigned to upstream that is operating in North American mode. Workaround: Correct the spectrum group definition.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCec27900	If the **show pci hardware** command is entered on a telnet session to a system running NPE-G1, the following output will be seen on the NPE-G1 console:
	
	`BCM1250 LDT Host Bridge, handle=0`
	`BCM1250 bridge, config=0x0`
	`(0x00):dev, vendor id = 0x0002166D`
	`(0x04):status, command = 0x00100107`
	`(0x08):class code, revid = 0x06000002`
	`(0x0C):hdr, lat timer, cls = 0x00010000`
	`(0x18):bus id registers = 0x000F0300`
	`(0x1C):secondary status = 0x0000F141`
	`(0x20):mem base/limit = 0x4FF04880`
	`(0x30):io upper limit/base = 0x00010001`
	`(0x34):capabilities ptr = 0x00000040`
	`(0x38):expansion rom bar = 0x00000000`
	`(0x3C):bridge ctrl = 0x00220000`
	`(0x40):LDT cmd, cap id, = 0x20000008`
	`(0x44):Link config/control = 0x00000020`
	`(0x48):Link frequency = 0x00000211`
	`(0x50):SRIcmd, srirxden, sritxden = 0x52211010`
	`(0x54):SRI tx numerator = 0x0000FFFF`
	`(0x58):SRI rx numerator = 0x0000FFFF`
	`(0x68):Error status/control = 0x00009249`
	`(0x6C):Tx ctrl, databufalloc = 0x00041515`
	`(0xC8):Tx buffer count max = 0x00FFFFFF`
	`(0xDC):Rx CRC expected = 0xFFEFE7AF`
	`(0xF0):Rx CRC received = 0xBEFCFEDE`
	
	`BCM1250 PCI Host Bridge:`
	`bus_no=0, device_no=0`
	`DeviceID=0x0001, VendorID=0x166D, Cmd=0x0146, Status=0x02A0`
	`Cls=0x06/0x00/0x00, Rev=0x02, LatencyTimer=0x2C,`
	`CacheLineSize=0x10`
	`BaseAddr0=0x60000008, BaseAddr1=0x00000000, MaxLat=0x00,`
	`MinGnt=0x00`
	`SubsysDeviceID=0x0000, SubsysVendorID=0xFFFF, ErrorAddr=0x00010401`
	
	This problem occurs on a Cisco uBR7246 series with a NPE-G1 running 12.2(15)BC.
	
	There are no known workarounds.

CSCec29381	If a CMTS, running 12.2(15)BC, receives an event-generation-object (in a gate-open message) containing attributes measuring more than 255 bytes in length, it ignores that attribute and does not generate an event message (RADIUS message). This is a severe issue for CALEA functionality because if the SDP string passed within the event-generation-object is greater than 255 bytes, no event message would be generated. Note that CALEA is NOT a packetable 1.0 functionality, so this issue does not affect packetable 1.0 deployments. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec30030	The CBT trace window display fft frequency is always less than the real frequency. This is repeatable. It is easy to see the problem if RBW is big. The second problem is when CBT trace window frequency span equals multiple of RBW. For example: `frequency span = 6000 KHz, RBW = 60 KHz hence  span = 100*RBW.` In this corner case, the last FFT point displayed in Trace window is very big. This is repeatable. There are no known workarounds.
CSCec31019	gdb is currently not supported on NPE-G1 in cable mainline branch. There are no known workarounds.
CSCec31356	With global command PacketCable authorize vanilla-docsis-modem enabled, UGS and UGS/AD request from DOCSIS1.0+ and non-packetcable compliant DOCSIS 1.1 modem are rejected. This causes no UGS BW request be accepted for these modems. There are no known workarounds.
CSCec31823	When a spectrum group is configured with frequencies above the north american freq-range and within the japanese freq-range, and when this spectrum group is assigned to an upstream, the cm's on that upstream will not make it past init(rc)state on cmts bootup. Changing the upstream configuration from a spectrum group to a fixed frequency and rebooting will work fine, as will changing the upstream config to a spectrum group that is contained within the north american range. Workaround: Once the cmts is in this broken state, changing the spectrum group or the upstream frequency in the running config, as specified above, will cause the modems to come on-line.
CSCec33788	A SNR Reading can not have a correct value if the measurement of that SNR is near a high collision area. The current code does not take to account where the SNR was measured. This problem happen more in current code, because the feature of automatic ranging backoff alogrithm is not working correct. With this feature turn on, the problem is not as gross, but the problem is still there Workaround: Use fixed backoffs for a known number of modems, and the problem is mitigate since this causing less collisions
CSCec34056	The CMTS may crash while doing “test pas oir”. Workaround: Unconfigure “cable modem remote-query” functionality.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec34520	If a MCxxU card is installed as first modem card in a system, several features/functionality will not work properly for legacy cards (MCxxC). - The output of “show interface <interface> mac-scheduler” will report zero average load. - Load balancing does not work in “utilization” mode. - HCCP may not or not completely work - Ageing functionality may not work properly. - Contention periods may not be updated. - Modem distance detection may not work properly. Workaround: Always install a legacy card (MCxxC) in a lower slot number than any MCxxU card.
CSCec36216	When enabling the cable dynamic-secret command on the Cisco CMTS in IOS 12.2 (15)BC1, certain cable modems may later become stuck in the state “init(o)” and be unable to come online. Disabling the cable dynamic-secret command brings these modems back online immediately. IMPORTANT: The modems which become stuck in init(o) are limited to certain brands / models, and are a repeatable subset of all modems on the CMTS. A list of modems by OUI, model, and SysDescr is enclosed at the end of this DDTS. These modems do not appear DOCSIS compliant. This issue occurs when Cable dynamic-secret is enabled on the cable interface IOS 12.2(15)BC1 on uBR7200, uBR7100, and uBR10K Specific brands and software versions of cable modems become stuck in state init(o) only when dynamic secret is enabled, and immediately come online when dynamic secret is disabled. All other modems come online and work normally. Lab investigation indicates that these modems are NOT DOCSIS COMPLIANT, and are storing the TFTP server IP address from the initial DHCP offer (before Dynamic Shared Secret was enabled) and requesting the new TFTP file name from the old server, the old server cannot find the encrypted filename, so the modem is stuck in init(o). Workaround: Power cycle the affected cable modem. Alternative workaround: Disable cable dynamic secret, use TFTP-enforce and cable source-verify instead.
CSCec36221	The CMTS may display the error below. `tod: Cant match output i/f for telco return` There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec36319	If cable intercept is configured on an MC28U/MC16U/MC28X/MC16X interface, when a CM starts to come online, a traceback will be generated. This may also happen randomly when there is data traffic. If the intercepted packets are not IP packets, the encapsulating IP packets' TOS field may also not be the default TOS value. This happens only with cable intercept command. It should not cause any serious problem besides generating the traceback because the spurious memory access is only due to read, not write. Only in rare cases should the potentially incorrect TOS value cause visible problems. For example, if the intercepted packets' TOS value is set to high priority/low latency while there happens to be other high priority/low latency traffic sharing the links with these intercepted packets. This problem exists since CSCdz45824. Again, this happens only if the intercepted packets are non-IP. Workaround: Avoid configuring cable intercept.
CSCec37571	A Cisco router may reload due to low memory. This problem occurs when BPI+ is in use. There are no known workarounds.
CSCec40125	Under heavy load, all of the modems on an upstream of the MC28u linecard may go offline. Modems are never seen in any kind of registration state by the CMTS, again. All incoming packets from that upstream are lost or corrupted. The problem can be corrected with a shut/no shut on the upstream. Please see Field Notice Number 27315 for a Workaround/Solution.
CSCec40145	Downstream MC28U line card hang can occur under extreme CPU load and high traffic conditions. There are no known workarounds.
CSCec44208	If you have an if-con session open from a Telnet NPE session and you try to if-con to the same TransAm line card from the main NPE console, you get the confirmation message, but when you reply "y" and hit CR several times, you don't get the LC console prompt. you can still use both logout commands to get back to NPE prompt. This issue also occurs if you have an if-con session from main NPE prompt and you try to if-con to same LC from a Telnet NPE session. There are no known workarounds.
CSCec46272	Tracebacks are from linecard SNMP after equalization being turned on and while polling SNMP docsIfSignalQualityEntry variables. There are no known workarounds.
CSCec48352	DSA-REQ from MTA trying to share the same resource is rejected even if it has not tried to commit QOS per service flow. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCec50122	A Cisco uBR7200 series CMTS running 12.2(15)BC1 IOS release may experience a spurious memory access errors
	`%ALIGN-3-SPURIOUS: Spurious memory access made at 0x604B1364 reading 0x24`
	`%ALIGN-3-TRACE:`
	`-Traceback= 604B1364 604B2B38 604AF960 604AFB88 6056AA60 00000000 00000000 00000000`
	`%ALIGN-3-TRACE:`
	`-Traceback= 604B1368 604B2B38 604AF960 604AFB88 6056AA60 00000000 00000000 00000000`
	There are no known workarounds.

CSCec50575	When “show cable l2-vpn” is executed, some amount of memory is leaked depending on the number of entries in the l2-vpn table. This issue occurs when l2-vpn entries are present. There are no known workarounds.
CSCec50650	The number of attributes in Radius header for QoS_Reserve and QoS_Commit event messages that are sending to CALEA Delivery Function (DF) is incorrect if the Session Description Protocol (SDP) attribute's length is greater than 247. There are no known workarounds.
CSCec52043	MC28U line card crash has been seen under conditions of extreme LC CPU LOAD/ACTIVITY. There are no known workarounds.
CSCec52178	Unexpected giant MAPs with MAP size equal to tens of bucket size are encountered under heavy traffic load. There are no known workarounds.
CSCec53031	DSCP from gate-set msg is not reflected as TOS byte on US packets from MTA such that TOS overwrite function does not work on ubr7200. There are no known workarounds.
CSCec55466	On a Cisco 7200 router with a NPE-G1 installed, modem control and flow control may not work properly on the AUX port, preventing modems or other RS-232 devices which rely on these signals from working properly. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCec56298	The default behavior for the cable dynamic-secret command is to scramble the filename during registration.
	
	The new CLI option, nocrypt, introduced with this DDTS permits the operator to not scramble these filenames. Thus, the SNMP query for the DOCSIS config file in use by a cable modem will return a non-scrambled filename.
	
	This option first became available in IOS 12.2(15)BC1b, and will be available in 12.2(15)BC2 and future releases.
	
	`uBR(config-if)#cable dynamic-secret ?`
	`  lock    Lock modems violating dynamic secret`
	`  mark    Mark modems violating dynamic secret`
	`  reject  Reject registration request from modems violating dynamic secret`
	
	`uBR(config-if)#cable dynamic-secret mark ?`
	`  nocrypt  Do not encrypt modem config file name`
	`  <cr>`
	`uBR(config-if)#cable dynamic-secret reject ?`
	`  nocrypt  Do not encrypt modem config file name`
	`  <cr>`
	
	`uBR(config-if)#cable dynamic-secret lock ?`
	`  <1-255>  Profile used to lock`
	`  nocrypt  Do not encrypt modem config file name`
	`  <cr>`
	
	`uBR(config-if)#cable dynamic-secret lock 15 ?`
	`  nocrypt  Do not encrypt modem config file name`
	`  <cr>`
	
	There are no known workarounds.

CSCec57848	Crash seen under heavy traffic on MC28U. There are no known workarounds.
CSCec65492	This problem has been observed for both cable interface and gigabit Ethernet interface. One reason is that the moving average algorithm for bit rate takes byte count even when it appears to be in error (negative). This may happen with other interface type also. There are no known workarounds.
CSCec66199	With DSC-REQ to toggle DOCSIS resource between admitted and active state, gate state is not changed to reflect that, and QOS-RESERVED is not sent as a result. There are no known workarounds.
CSCec71080	he fix for CSCdz74683 counts the additional two bytes added for the PHS header as payload, causing the rate limit code to consider them as payload in its calculations. This may trigger packet drops. Workaround: Disabling PHS (if acceptable).

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec74759	when running uBR7246VXR NPE300 with 12.2(15)BC1... RTP traffic get bad performance on UGS (packet loss). When using BE for the same traffic the Voip call is working ok. From the cable-monitor capture, we can see 300msec gap between some MAPs causing the RTP drops Workaround: On some CMTS the Internal FastEthernet 0/x by being shutdown will fix the gap problem.
CSCec81905	If a ubr7246VXR has more than five downstream interfaces in the chassis (e.g., 3 MC28 cards), calls will start failing on the sixth interface. Gates created for the MTAs connected to the sixth (and higher) interfaces will be stuck. There are no known workarounds.
CSCec85359	snmpwalk failed OID.1.3.6.1.2.1.10.127.1.3.7 This issue is observed on 7206VXR running IOS 12.1(13)EC3 and having PA-A3-8E1IMA interfaces. Workaround: OIR the linecard.
CSCec89236	'Invalid cable upstream <port#> ingress-noise-cancellation' message gets displayed on a VXR that has both transam and legacy card. Cable interface refers to legacy card. There are no known workarounds.
CSCed03026	When sending large amounts of downstream traffic and pushing the CLC cpu to 100% by turning off clc scheduler allocate and turning on clc debugs, cm's that went offline would not get passed init(i) state, even once the CLC cpu utilization was reduced. A CLC reload is required to bring the cm's online. There are no known workarounds.

CSCed06821	When the following IOS configurations are used together, some modems become stuck in the state “init (o)” and cannot come online. These modems will cycle through various registration states, but do not come online. The issue is specific to a minority of modem brands.
	`ip tftp-source interface <interface>`
	`- where <interface> is not the cable interface`
	`cable dynamic-secret <any setting>`
	The issue grows to all modem brands if an access lists prevents TFTP traffic between the modem and the <interface> specified above.
	Workaround: Remove the CMTS configuration:
	`ip tftp-source interface <interface> command.`
	`use FTP for logging and management files.`

CSCed12228	The slot column shows the wrong slot number in **show packetcable gate summary** command. For example, if the call is made from interface c4/1, it still show up as 4/0. It does not cause any problem with calls. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed12672	Mac clients behind cable modem sometimes randomly unable to get IP address via dhcp. Debugs on CMTS shows encapsulation failure for packets that are destined for that mac client. Work-around: Configuring static ip address on mac client made it to work.
CSCed12992	Load balancing CLI commands with “ugs” parameters will not be stored in NVRAM. Instead, the command will be replaced with “voice” instead of “ugs”. There are no known workarounds.
CSCed14904	A Cisco Universal Broadband Router may reload unexpectedly as a result of it's memory getting corrupted. This issue occurs only when using CMTS remote query feature. Workaround: Disable the CMTS remote query. If the CMTS remote query must be use, then there are no known workarounds.
CSCed17434	UBR7200 with NPE-G1 can crash running 15BC1a. There are no known workarounds.
CSCed20964	Cisco uBR-MC28U cable interface line card may crash in ubr7200 series CMTS running IOS release 12.2(15)CX with cable modems failing to register. There are no known workarounds.
CSCed24185	It is possible - though invalid - to configure a subinterface on a cable bundle slave interface. Operational impact is unknown. There are no known workarounds.

CSCed24602	When a NPE-G1 GigabitEthernet interface is configured for “no negotiation auto” and the link partner is in the shutdown (or not connected) state the interface will flap repeatedly with the following message
	`01:19:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up`
	`01:19:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down`
	This problem is described in CSCdx95364 and this DDTS seeks to have the fix ported to 12.2BC IOS for the ubr7200.
	Workaround: Configure the GigabitEthernet interface on the NPE-G1 to use “negotiation auto” mode.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed26241	Ubr7246VXR may modify DHCP BootP requests running 12.2(15)BC1. The BootP packet will be decreased in size and may cause the DHCP not to reply to the BootP requests. The behavior is not observed in 12.1(13)EC4. ex. Debugs debug ip dhcp server packet & debug ip udp With 12.1(13)EC4 (working) Dec 11 12:53:49.819: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67),length=308 Dec 11 12:53:49.819: BOOTP: opcode 1 on interface FastEthernet0/0.50, 0secs, 0 hops Dec 11 12:53:49.819: DHCPD: setting giaddr to 192.168.0.1. Dec 11 12:53:49.819: UDP: sent src=192.168.0.1(67), dst=10.0.0.1(67),length=328 Dec 11 12:53:49.819: DHCPD: BOOTREQUEST from 0002.de15.3ed8 forwarded to10.0.0.1. Dec 11 12:53:50.091: UDP: rcvd src=10.0.0.1(67), dst=192.168.0.1(67),length=308 Dec 11 12:53:50.091: DHCPD: forwarding BOOTREPLY to client 0002.de15.3ed8. Dec 11 12:53:50.091: DHCPD: creating ARP entry (10.0.0.1,0002.de15.3ed8). Dec 11 12:53:50.091: DHCPD: unicasting BOOTREPLY to client 0002.de15.3ed8(10.0.0.1). Dec 11 12:53:50.095: UDP: sent src=192.168.0.1(67), dst=10.0.0.1(68),length=328 With 12.2(15)BC1 (not working) .Dec 11 12:46:18.173: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67),length=308 .Dec 11 12:46:18.173: BOOTP: opcode 1 on interface FastEthernet0/0.50, 0 secs, 0 hops .Dec 11 12:46:18.173: DHCPD: setting giaddr to 192.168.0.1. .Dec 11 12:46:18.173: DHCPD: adding relay information option. .Dec 11 12:46:18.173: UDP: sent src=192.168.0.1(67), dst=10.0.0.1(67),length=249 .Dec 11 12:46:18.173: DHCPD: BOOTREQUEST from 0002.de15.3ed8 forwarded to 10.0.0.1. This issue was discovered after the ubr7246VXR was upgraded to 12.2(15)BC1 from 12.1(13)EC4. BootP clients (Qam Modulators) sent DHCP BootP requests through the CMTS (ingress FE, egress POS), no cable interfaces involved, on the LAN to the DHCP server. The packets are shortened and the DHCP server may drop the requests due to this fact. Workaround: Revert to 12.1(13)EC4.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed28844	When a gate transits to the “committed” state, then back to “reserved”, and to “committed” again, a new gate-open message is sent again, which is not desired. There are no known workarounds.
CSCed32192	If a load balancing modem exclude entry is changed from its default setting to “enforce”, the new setting is not reflected in the configuration. Workaround: Remove an existing entry, then reconfigure it with “enforce” flag.
CSCed44135	COPS connection may occasionally reset under certain conditions. This may cause interoperability issues. If COPS messages (e.g., gate control messages) are being received by the CMTS at a rate equal to or more frequently than the COPS keep-alive timer value, no keep-alive messages will be sent from the CMTS. Therefore, the PDP end of the COPS connection misses one or more keep-alives and closes the COPS connection. A new connection then needs to be established. There are no known workarounds.
CSCed45074	Downstream data lost in multi-DS bundle configuration. Condition: When destination of DS data crosses DS interfaces, data is lost for 10-30 seconds. There are no known workarounds.
CSCed46863	BUS exception occurred when **sh cable subscriber-usage over-consume** command was entered per the crashinfo. There are no known workarounds.
CSCed48419	IS-IS routing protocol support is no more present in latest 12.2BC codes. Its available in 12.1EC. Currently there is no workaround available for customers who want to run IS-IS and who are running NPE-G1 on their UBR7200s which requires 12.2BC code. There are no known workarounds.
CSCed56281	Although PPPoE client has connected behind CM, It is not outputted by “show interface cable x/x modem [SID]”. This issue occurs only MC16U and/or MC28U. MC16C and/or MC28C has no this defect. There is no affect for communicating of PPPoE client. This is a cosmetic problem. There are no known workarounds.
CSCed63206	The linecards reload unexpectedly. The issue is caused by an ipc-timeout bcz of buffer depletion. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed65148	A UBR7200 may experience a reload with the following given as the cause of the reload in the show version: `System returned to ROM by break at PC 0x607C35F0` There are no known workarounds.
CSCed67484	CSCed14039 fixed A WDT problem for the NPE-G1. A first set of diffs were ported from this DDTS to Cable BC release train in Nov., 2003. Later another set of diffs were committed to the same DDTS that fixes the problem at more of a root cause level. This DDTS was opened to port the 2nd commit against CSCec14039 to the Cable BU branches. There are no known workarounds.
CSCed73075	Customer reported a NPE-400 crash. The crash was identified to be missing of CSCec58486 in the Cable BU BC train. There are no known workarounds.
CSCed78236	SNMP GetBulk of docsQosMIBObjects.1 may cause CPUHOG error message. There are no known workarounds.
CSCed78829	Performance degradation was caused by changing NRNG_CR_ACF and NRNG_CR_TCF registers due to incorrect consideration for performance optimization. this affects only QPSK modulation. Software fix is simply checking for modualtion profiles. if all modulation rates are using qpsk, different set of values are applied to these registers. There are no known workarounds.
CSCed86429	**test cable dsc qos** command is broken for DS service flows. Workaround: Use the **test cable dsc message** command.
CSCed95046	Source verify is not performed for MC28U interfaces on ubr7200. There are no known workarounds.
CSCin20386	This was observed while doing spot checking for cable related CLI's. There are no known workarounds.
CSCin36963	The port-channel interface may report erratic values for Total drops, broadcasts and interface resets after a member link of the etherchannel fails. There are no known workarounds.
CSCin37450	The output drops counter of show interface port-channel does not increment when packets are dropped after traffic shaping. There are no known workarounds.
CSCin49029	MTS did not mark the CM which attempts for theft-of-service. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCin54561	Down Stream Multicast traffic is running at the CMTS and after doing a OIR at the cable interface the following Spurious memory access observed as below.
	
	It is observed that the problem is due to the CLI “cable match address <n>”
	
	Also the following error messages was continuously populating at the CMTS, after the OIR.
	
	`*Aug 25 02:41:02.803: %UBR7200-3-NOMORESIDS: Maximum number of SIDS have been allocated for interface Cable6/0`
	`*Aug 25 02:41:38.803: %UBR7200-3-NOMORESIDS: Maximum number of SIDS have been allocated for interface Cable6/0`
	`*Aug 25 02:42:14.919: %UBR7200-3-NOMORESIDS: Maximum number of SIDS have been allocated for interface Cable6/0`
	
	Workaround: Shut down the interface before executing the OIR.

CSCin54781	Two issues are seen setting docsIfQosProfMaxTransmitBurst: 1. Allows to set docsIfQosProfMaxTransmitBurst, but getone on docsIfQosProfMaxTransmitBurst does not return the set value. “Show cable qos profile” also does not show the set value. 2. Allows to set docsIfQosProfMaxTransmitBurst, when the Qos profile is in “active” state. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCin54933	A cable modem termination system (CMTS) may record a traceback when you either remove a Fast Ethernet (FE) member interface of an EtherChannel interface by entering the **shutdown** interface configuration command or you add an FE member interface to an EtherChannel interface by entering the **no shutdown** interface configuration command. This issue is observed on a Cisco uBR7200 series when IP unicast traffic is sent in both the downstream and the upstream direction. Workaround: When you add a new member FE interface to the EtherChannel interface, take the following steps: 1. Enter the **shutdown** interface configuration command on both the new FE member interface and the EtherChannel interface. 2. Add the FE member interface by entering the **channel-group** *port-channel-number* interface configuration command on the FE member interface. 3. Enter the **no shutdown** interface configuration command on the Etherchannel interface. When you remove an FE member interface from the EtherChannel interface, take the following steps: 1. Enter the **shutdown** interface configuration command on the EtherChannel interface. 2. Remove the FE member interface by entering the **no channel-group** *port-channel-number* interface configuration command on the FE member interface. 3. Enter the **no shutdown** interface configuration command on the Etherchannel interface.
CSCea17313	packet may not go through a port-channel interface configured for vrf forwarding. This is seen on 7500 routers. Workaround: Unconfigure and reconfigure the vrf forwarding on the port-channel interface (by executing **no ip vrf forwarding** and **ip vrf forwarding** commands).
CSCea39371	A Cisco 7500 series router may unexpectedly reload with a bus error. This issue is observed on a Cisco 7500 series router if Border Gateway Protocol (BGP), IP version 6 (IPv6), and distributed Cisco Express Forwarding (dCEF) are enabled concurrently. Workaround: Disable dCEF and enable central CEF instead.
CSCea55879	We need to create a know that will allow up to assign precedence 0-7 traffic to the same queue on an SRP interface. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCea64720	**copy** and **rename** embeds wrong timestamp to the destination files if NTP is configured. This defect is observed in flash and ATA flash cards. This defect is seen in 12.2(16). There are no known workarounds.
CSCea71679	Some IP addresses are not allowed for 'ip local pool' configuration. IP address configured for local pool was present as an IP address for some loopback interface on the router. Do not configure the IP address for the local pool.

CSCeb42687	Following error message will appear on NPE-G1:
	`*May 30 09:13:05.618: %SYS-3-INTPRINT: Illegal printing attempt from interrupt level.`
	`-Process= "<interrupt level>", ipl= 5`
	There are no known workarounds.

CSCeb60531	Whenever there are gate control messages being transmitted and received from a CMTS, the CMTS will not transmit a COPS Keep Alive message, even though it needs to. The CMTS will wait until the “batch” of gate control messages is complete (i.e, the call is set up) before it transmits its Keep Alive. Since it can be (in this case it was) outside the Keep Alive interval specified by the CMS, the CMS sends a Client-Close to the CMTS and establishes a new COPS connection. This can cause additional and undesirable call setup delays. This issue occurs under heavy COPS workload conditions, when many voice calls are being set up simultaneously and the CMS is using the COPS protocol to download call setup info to the router. There are no known workarounds.

CSCeb73339	A 7206vxr with NPE-G1 running 12.3(1) enterprise may crash at mgd_timer_complain_uninit while performing nat translations. An uninitialized timer message occurs and then a fatal alignment error followed by an Unexpected exception crash.
	`Example:`
	`%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 8.`
	`-Process= "IP Input", ipl= 0, pid= 49`
	`%ALIGN-1-FATAL: Illegal access to a low address`
	`Unexpected exception, CPU signal 10, PC = xxxxxxx`
	There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb75824	A Cisco 7200 series router with a Network Processing Engine (NPE-G1) may pause indefinitely on bootup if there is no Compact Flash Card in the disk2: device slot. This issue is observed only with an NPE-G1 on a Cisco 7200 series. It does not affect any other Cisco 7200 series NPE. Workaround: Insert a Compact Flash Card into the disk2: device slot and power-cycle the router. The Compact Flash Card does not need to contain any particular files; however, a copy of the desired Cisco IOS image is recommended.
CSCec08434	The Cisco 7200 series boothelper image for Cisco IOS Release 12.2(14)S2 may reload unexpectedly, and the router may return to the ROM monitor (ROMmon) mode. This issue is observed when you install a 2-port Token Ring Inter-Switch Link 100BASE-TX port adapter (PA-2FEISL-TX) or a 1-port ATM Enhanced OC-3 Packet-over-SONET (POS) port adapter in a Cisco 7200 series Network Processing Engine G-1 (NPE-G1) and you reload, reset, or power up the router with the boothelper image. Workaround: Remove the PA-2FEISL-TX or 1-port ATM Enhanced OC-3 POS port adapter when you reload, reset, or power up the router with the boothelper image. Once the router has booted up, you can reinstall the port adapters.
CSCec14039	A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message: `Last reset from watchdog reset` This problem is observed on a Cisco 7200 series that is configured with an NPE-G1 and that is running Cisco IOS Release 12.2(14)S3. The symptom may also occur in other releases. There are no known workarounds.
CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information about which radius server to use is downloaded via a protocol other than RADIUS. The problem only happens when no RADIUS server is configured on the router, and no RADIUS server has been configured on the router since it last reloaded. Workaround: Configure a dummy radius server, as in: **radius-server host *x.x.x.x*** Where “x.x.x.x” is an arbitrary ipv4 address.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec22929	A software-forced reload may occur on a Cisco 7200 series after an OIR of a PA-2T3+ port adaptor. This issue is observed when traffic enters through the interface of the port adapter. Workaround: Shut down the interface of the port adapter before you perform an OIR.

CSCec25534	The following message displays yet plenty of free memory seems to be available.
	`%NBAR-1-MAXMEMORYUSED: Reached maximum amount of memory allocated for stile`
	Memory calculation for NBAR maximum allocation limit is wrong when amount of free memory is over 214.8MB at router initialization. This causes a pre-mature warning message:
	`%NBAR-1-MAXMEMORYUSED: Reached maximum amount of memory allocated for stile`
	The Above message only informs you that you are low on NBAR memory. The router will continue classifying correctly. Mis-classification is not occurring until you see the error:
	`%NBAR-1-NOSTATEMEM: Memory for maintaining state used up`
	There are no known workarounds.

CSCec27821	A Network Processing Engine G-1 (NPE-G1) may forward unicast IP packets that have a Layer 2 multicast MAC address. This issue is observed on an NPE-G1 that is installed in a Cisco 7200 series. Workaround: Create an access control list (ACL) to filter the packets. Alternate workaround: Configure a static multicast MAC address mapping to the ports of the connected Layer 2 switch.
CSCec27847	A ubr7200 running a NPE-G1 has the built in GigE enabled, the GigE could possibly cause the upstream maps not to be generated, which could cause modems to drop, or packets to be lost. Workaround: Disable the built in GigE interface.
CSCec39692	Cisco UBR10K running 12.2(11)BC2 may crash. This issue is observed on a Cisco UBR10K Series when you execute **show config**. Workaround: If no change has been made since the router booted up, use “show run” to look at the running configuration. No workaround yet to look at the configuration stored in NVRAM.
CSCec87802	High cpu utilization mostly due to CEF Scanner. This issue is observed on a uBR10k series that is running IOS 12.2(15)BC1. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed13018	Native GE interface throttling is always bypassed. With newer version of BCM chips also the throttling is bypassed, whereas only for older revision it is needed. There are no known workarounds.
CSCed26897	Every frequency hop leads to an upstream re-init which in current SW can case a 300ms delay in servicing UGS. The problem is made more sever because frequency hopping on upstreams that have no modems on them is happening to frequently and a result cases a lot of UGS interruption There are no known workarounds.
CSCed29514	The C7200 NPE-G1 builtin GE (SBeth) MAC Filter accepts NULL DAs 00-00-00-00-00-00. This unintentional behavior may pose a denial of service security risk in customer environments if their networks are flooded with NULL DAs. This appears to be a Broadcomm silicon or documentation errata. The Broadcomm docs state that NULL DAs may be used for unused MAC Filter entries, implying that they are not accepted. This issue occurs when NULL DAs are presented to the NPE-G1 SBeth I/F. There are no known workarounds.
CSCed53018	PPPoE tunneled session is always dropped by LAC (which is acting as PPPoE concentrator at the same time) with 12.2(15)BC1 on ubr7246VXR. The PPPoE session is dropped due to cable source-verify leasetimer. No PPP TERM REQ is received from PPPoE client (that's CM), or CDN is received from LNS. Workaround: Do not use "cable source-verify dhcp" or use "cable source-verify" instead.
CSCed65223	The ifHCOutOctets counters are impossibly high for gig interfaces. The problem has seen on UBR10000 running 12.2(15)BC1. However, ifHCInOctets counters seem to be fine. There are no known workarounds.

Table 23 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed89735	An uncorrectable ECC parity error may occur on a Cisco 7200 series that is configured with an NPE-G1. This issue is observed rarely when you enter the **show sysctlr** or the **show tech** command on the NPE-G1. Workaround: Do not enter the **show sysctlr** or the **show tech** command.
CSCin43613	The Fast Ethernet (FE) switching performance on a Cisco 7200 series was altered by implementing the fix for: CSCdw00953 - TX-ISL 1 port FE PA wont go DOWN immediately after loss of carrier. The fix went into: 12.2(16)BX 12.3(1)BW 12.2(16)B 12.2(15)ZN 12.2(17)B 12.3(15) PI 12.2(16)S 12.3(15)PI 12.2(15)T 12.2(15) If you are running an IOS list above or later, you may see a performance change from earlier IOS. You regain the performance, you must load an IOS that contains this bug fix. This issue is observed on any FE switching path of a 7200 router. There are no known workarounds.

Open Caveats for Release 12.2(15)BC1g

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC1g and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC1g.

Closed and Resolved Caveats for Release 12.2(15)BC1g

The caveats listed in Table 24 are resolved in Cisco IOS Release 12.2(15)BC1g. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 24 Closed and Resolved Caveats for Release 12.2(15)BC1g

Caveat ID Number	Description

CSCsa81379	NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.
	
	If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.
	
	The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.
	
	Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.
	
	Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):
	
	`cnfFeatureAcceleration 1.3.6.1.4.1.9.9.99999.1.3`
	`cnfFeatureAccelerationEnable 1.3.6.1.4.1.9.9.99999.1.3.1`
	`cnfFeatureAvailableSlot 1.3.6.1.4.1.9.9.99999.1.3.2`
	`cnfFeatureActiveSlot 1.3.6.1.4.1.9.9.99999.1.3.3`
	`cnfFeatureTable 1.3.6.1.4.1.9.9.99999.1.3.4`
	`cnfFeatureEntry 1.3.6.1.4.1.9.9.99999.1.3.4.1`
	`cnfFeatureType 1.3.6.1.4.1.9.9.99999.1.3.4.1.1`
	`cnfFeatureSlot 1.3.6.1.4.1.9.9.99999.1.3.4.1.2`
	`cnfFeatureActive 1.3.6.1.4.1.9.9.99999.1.3.4.1.3`
	`cnfFeatureAttaches 1.3.6.1.4.1.9.9.99999.1.3.4.1.4`
	`cnfFeatureDetaches 1.3.6.1.4.1.9.9.99999.1.3.4.1.5`
	`cnfFeatureConfigChanges 1.3.6.1.4.1.9.9.99999.1.3.4.1.6`

Open Caveats for Release 12.2(15)BC1f

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC1f and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(15)BC1f.

Closed and Resolved Caveats for Release 12.2(15)BC1f

The caveats listed in Table 25 are resolved in Cisco IOS Release 12.2(15)BC1f. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC1f

Caveat ID Number	Description
CSCed61110	Cisco ubr7200 series CMTS running IOS release 12.2(15)BC1 may experience a software-forced crash after a watchdot timiout in CMTS MAC Timer process. The failure occurred on a platform with NPE-G1. There are no known workarounds.
CSCee64504	A CPUHOG may occur for about 4.5 seconds when you enter the **show running-config** command. This issue is observed on a Cisco uBR10000 series but may also occur on other platforms. Workaround: Do not enter the **show running-config** command. Rather, enter the **show config** command.
CSCef09586	If DHCP server in one of the configured VRF's has IP address that is matching broadcast address of the IP subnetwork used in another VRF (another subinterface) than cable modems will not come on-line and stay in init(d). If customer has DHCP server in VRF1 using IP address 10.2.16.15 and configure **ip address 10.2.16.1 255.255.255.240** on subinterface that belongs to VRF2, problem will occur. This issue has been noticed with following tested images: 12.2(11)BC2, 12.2(15)BC1d. Workaround: Changing IP address of the DHCP server or changing IP address scope in another VRF will resolve the problem.
CSCef20890	A Cisco ubr7246VXR running Cisco IOS Release 12.2(15)BC1 may unexpectedly reload due to a bus error. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC1f (continued)

Caveat ID Number	Description
CSCef46191	A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected. All other device services will operate normally. This issue occurs when user initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected. Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml
CSCin82407	Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server. Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources. This advisory will be posted to http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

Open Caveats for Release 12.2(15)BC1d

All the caveats listed in Table 26 are open and reported in Cisco IOS Release 12.2(15)BC1d. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 26 Open Caveats for Cisco IOS Release 12.2(15)BC1d

Caveat ID Number	Description
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCdy66891	When a cable modem receives a docsis binary file with network access disabled and bpi enabled, the CMTS will show it in the “online(pt)” state instead of “online(d)”. Workaround: Remove BPI from the docsis binary file.
CSCdz47210	No MIB object for “1st time online” in “show interface cable sid connectivity” output. There are no known workarounds.
CSCdz58997	Under Cisco IOS Release 12.2(11)BC1b, show cable modem phy shows DSpwr in wrong way. There are no known workarounds.

Table 26 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCea00322	Under rare circumstances, namely when the service provider tftp server is down of unreachable, a cable modem may still be able to come online against a CMTS if it obtains an illicit DOCSIS configuration file from a local tftp server. There are no known workarounds.
CSCea53868	The CMTS may display the error below after an N+1 switch over. `%UBR7200-4-BAD_REGISTRATION: Cable modem <mac> on interface Cable x/y when online attempted re-registration with different QoS` There are no known workarounds.
CSCea61100	The iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical. entPhysicalTable.entPhysicalEntry.entPhysicalSerialNum will return an incomplete chassis serial number. Only integer values minus any leading zeros are returned by the mib. There are no known workarounds.
CSCeb08941	There is no error/warning message if user issues “test cable ucc” on a non-existing cable modem. There are no known workarounds.
CSCeb27416	The CMTS may record a AAA related traceback with spurious memory access while running Bulk calls. There are no known workarounds.
CSCeb34574	Executing the cable modem qos profile command may generate a misleading message indicating that the modem could not be found even though it is listed in the show cable modem command display. The problem occurs if the command fails for one of the following reasons. 1. The QoS profile specified by the command was not created by the CMTS. 2. The modem's existing QoS profile for it's primary SID was created by a modem registration request. Either of these conditions will cause the command to fail as described in the CMTS configuration guide. The show cable qos profile command can be used to determine if the specified profile was created by the CMTS. The show cable modem registration command can be used to determine which profile the modem is using. There are no known workarounds.
CSCeb63785	CMTS will accept DSA-REQ intended to share the same resource ID that is in use by other service flow. There are no known workarounds.

Table 26 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCeb64909	During codec change, if MTA issue BW request with both adm/act bit set in qos set type TLV, CMTS does not compare it against the authorized flow spec, and can cause BW reject even if it is within authorized BW. Workaround: Do not use single phase DSC-REQ.
CSCeb70360	After users issue “test cable ucc cx/y <sid> <us_chid>” or “test cable ucc cx/y <sid> <us_chid> 0”, the CM offline counter is incremented by 1 whereas in fact the modem did not go offline at all. The offline counter can be retrieved by issuing “sh cab modem <mac> connectivity” in 12.2BC. Workaround: Use “test cable ucc cx/y <sid> <us_chid> 3” for those modems which support it. If a modem does not support the above, then there are no known workarounds.
CSCeb80293	With multiple cops connections set up to same CMS, any CMTS originating gate messages, such as gate-open, always sent to the first cops connection. There are no known workarounds.
CSCec02495	When the GBIC on a UBR/NPE-G1 is removed and reinserted the **show interface** command or the **show controllers** command may indicate that the newly inserted GBIC is missing or unknown. This is only cosmetic and will not affect the operation of the router. There are no known workarounds.
CSCec08579	With N+1 enabled, the Protect CMTS may crash with the error below if the identical modulation profiles are not configured on Working and Protect CMTS: `"Null Init Mtn Burst Descriptor in MAC scheduler init"` Workaround: Configure Working and Protect CMTS with the same modulation profiles.
CSCec13012	When issuing the command Show Cable Subscriber-usage, the CMTS does not pause with the --More-- prompt between multiple screens of output. There are no known workarounds.
CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information about which radius server to use is downloaded via a protocol other than RADIUS. The problem only happens when no RADIUS server is configured on the router, and no RADIUS server has been configured on the router since it last reloaded. Workaround: Configure a dummy radius server, as in: **radius-server host *x.x.x.x*** Where “x.x.x.x” is an arbitrary ipv4 address.

Table 26 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCec14844	On uBR7200/uBR7100, if there are too many CM/CPEs, there could be CPU HOG error messages when user issues “clear cab modem all delete” or “clear cab modem all reset”. Workaround: Lower the number of CM/CPEs.
CSCec17509	When a batch event message is sent after the call ends, the BCIDs in the message become bogus. There are no known workarounds.
CSCec34056	The CMTS may unexpectedly reload while doing “test pas oir”. Workaround: Unconfigure “cable modem remote-query” functionality.
CSCec36319	If cable intercept is configured on an MC28U/MC16U/MC28X/MC16X interface, when a CM starts to come online, a traceback will be generated. This may also happen randomly when there is data traffic. If the intercepted packets are not IP packets, the encapsulating IP packets’ TOS field may also not be the default TOS value. This happens only with cable intercept command. It should not cause any serious problem besides generating the traceback because the spurious memory access is only due to read, not write. Only in rare cases should the potentially incorrect TOS value cause visible problems. For example, if the intercepted packets' TOS value is set to high priority/low latency while there happens to be other high priority/low latency traffic sharing the links with these intercepted packets. This problem exists since CSCdz45824. Again, this happens only if the intercepted packets are non-IP. Workaround: Avoid configuring cable intercept.
CSCec40145	Downstream MC28U line card hang can occur under extreme CPU load and high traffic conditions. There are no known workarounds.
CSCec50575	When “show cable l2-vpn” is executed, some amount of memory is leaked depending on the number of entries in the l2-vpn table. This issue occurs when l2-vpn entries are present. There are no known workarounds.
CSCec52178	Unexpected giant MAPs with MAP size equal to tens of bucket size are encountered under heavy traffic load. There are no known workarounds.
CSCin20386	This was observed while doing spot checking for cable related CLI’s. There are no known workarounds.
CSCin36963	The port-channel interface may report erratic values for Total drops, broadcasts and interface resets after a member link of the etherchannel fails. There are no known workarounds.

Table 26 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCin37450	The output drops counter of show interface port-channel does not increment when packets are dropped after traffic shaping. There are no known workarounds.
CSCin49029	MTS did not mark the CM which attempts for theft-of-service. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC1d

The caveats listed in Table 27 are resolved in Cisco IOS Release 12.2(15)BC1d. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 27 Closed and Resolved Caveats for Release 12.2(15)BC1d

Caveat ID Number	Description
CSCed12672	Mac clients behind cable modem sometimes randomly are unable to get IP address via dhcp. Debugs on CMTS shows encapsulation failure for packets that are destined for that mac client. Workaround: Configure the static ip address on the mac client.

CSCed68043	ARP Filter counters do not clear. uBR10k and uBR7246 platforms are affected.
	This issue occurs when ARP Filters are enabled and there is arp traffic that is being filtered. The counters in the following example show command will not clear:
	`sqi-vxr2#sho cable arp-filter c3/0`
	`ARP Filter statistics for Cable3/0:`
	`  Replies Rcvd: 4 total. 4 unfiltered, 0 filtered`
	`  Requests Sent For IP: 4 total. 2 unfiltered, 2 filtered`
	`  Requests Forwarded: 168 total. 14 unfiltered, 154 filtered`
	There are no known workarounds.

CSCed83867	uBR7246VXR with NPE-1G and MC28U blades with 'cable source-verify dhcp'enabled results in: 1. 100% CPU load and flooding the CNR with service queries, the contributor to high CPU load is identified to be 'DHCPD Receive' process. 2. The few mac-address in the arp entry shows all zeros Workaround: Turning off the "cable source-verify dhcp" option in the config will bring the CPU back down.

Table 27 Closed and Resolved Caveats for Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCed88709	When a service-policy that corresponds to a policy-map with no fair-queueing classes is applied outbound on a Cable interface and one class performs shaping the uBR7200 may drop outbound packets and generate error messages similar to `%LINK-4-BADQID: Interface Cable4/0, bad output queue ID specified (265). Packet dropped` when the shaping classes becomes active because of traffic rates that exceed the prescribed limits in the class. Workaround: Have at least one class with a fair-queueing configuration in the policy-map. This means using one of the **bandwidth**, **priority**, or **fair-queue** commands within the policy-map for at least one class.
CSCee12282	A uBR7246VXR CMTS router with output QMC traffic-shaping enabled and active on a cable interface can leak processor pool memory under high load, i.e. when multiple particles are used for packet buffering. Workaround: Remove output QMC shaping command from cable interface to stop leak; reload router to reclaim memory.
CSCee20869	In order to protect from DOS service attacks on the CMTS, it is decided to add per SID basis throttling of lease queries and global rate limit for lease queries initiated by downstream traffic. This is meant to reduce the CPU utilization of DHCP Receive process & ISR context when “cable source-verify dhcp” and “no cable arp” is configured. There are n o known workarounds.
CSCee21114	When “source-verify dhcp” and “no cable arp” is configured, DHCP lease query response for dst address of pkts coming from the back-haul is dropped. CPE is unreachable from the back-haul until the CPE itself send an ARP or IP packet. Workaround: Do not configure “no cable arp”.
CSCee23838	If a downstream packet received at the CMTS is destined for a modem whose ARP entry is incomplete or not present in the CMTS arp database, the CMTS goes into a loop of issuing out DHCP lease queries and receiving ACKs till an upstream packet for the modem populates the ARP database on the CMTS. Workaround: Disable “no cable arp” on the cable interface.
CSCee37649	Under high load with BPI active, the ubr7200 may lock up, permitting no console access. Higher level protocols will be unresponsive (for example, the system will not respond to ARP requests). The system may still forward packets. Workaround: Take off the load for a period of time (physically disconnect all connected modems) until the system recovers. Alternative Workaround: Disable BPI on systems with constantly high CPU load.

Open Caveats for Release 12.2(15)BC1c

All the caveats listed in Table 28 are open and reported in Cisco IOS Release 12.2(15)BC1c. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 28 Open Caveats for Cisco IOS Release 12.2(15)BC1c

Caveat ID Number	Description
CSCdx62698	This problem was observed while doing spot checking for CMTS image. Workaround: To prevent CPE behind the Cable modem to accessing the CMTS, the interface specific access-group can be configured as a workaround.
CSCdy10666	Remote-query unconfiguring does not work properly. There are no known workarounds.
CSCdy66891	When a cable modem receives a docsis binary file with network access disabled and bpi enabled, the CMTS will show it in the “online(pt)” state instead of “online(d)”. Workaround: Remove BPI from the docsis binary file.
CSCdz04902	Forcing a QoS profile through the command “cable modem <x> qos pro <y>” does not persist after a modem is flapping. Since the qos profile forcing is considered as an option to “punish” customers who abuse BW then it has to be in affect even if the modem flaps. There are no known workarounds.
CSCdz45824	TOS bits in duplicated call content don't match that of original call content. This may result in lower delivery reliability of duplicated call content which is contrary to requirement of same or better reliability. This issue occurs under normal operating conditions for CALEA call content. There are no known workarounds.
CSCdz47210	No MIB object for “1st time online” in “show interface cable sid connectivity” output. There are no known workarounds.
CSCdz58997	Under Cisco IOS Release 12.2(11)BC1b, show cable modem phy shows DSpwr in wrong way. There are no known workarounds.
CSCdz73188	ubr7200 system restarted by bus error when it was trying to create an entry for a file system. There are no known workarounds.
CSCea00322	Under rare circumstances, namely when the service provider tftp server is down of unreachable, a cable modem may still be able to come online against a CMTS if it obtains an illicit DOCSIS configuration file from a local tftp server. There are no known workarounds.

Table 28 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCea13693	When there are about 2800 cable modems connected to a cable interface, a few hundred cable modems will go offline in a short period of time. It is recommended to have no more than 2000 cable modems connected to a cable interface. There are no known workarounds.
CSCea43086	Performing a “clear interface cable 0” on a Cisco CM will break the functionality introduced in CSCdz04902. This problem does not happen if the CM is reloaded. There are no known workarounds.
CSCea53868	The CMTS may display the error below after an N+1 switch over. `%UBR7200-4-BAD_REGISTRATION: Cable modem <mac> on interface Cable x/y when online attempted re-registration with different QoS` There are no known workarounds.
CSCea61100	The iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical. entPhysicalTable.entPhysicalEntry.entPhysicalSerialNum will return an incomplete chassis serial number. Only integer values minus any leading zeros are returned by the mib. There are no known workarounds.
CSCeb08941	There is no error/warning message if user issues “test cable ucc” on a non-existing cable modem. There are no known workarounds.
CSCeb27416	The CMTS may record a AAA related traceback with spurious memory access while running Bulk calls. There are no known workarounds.
CSCeb34574	Executing the cable modem qos profile command may generate a misleading message indicating that the modem could not be found even though it is listed in the show cable modem command display. The problem occurs if the command fails for one of the following reasons. 1. The QoS profile specified by the command was not created by the CMTS. 2. The modem's existing QoS profile for it's primary SID was created by a modem registration request. Either of these conditions will cause the command to fail as described in the CMTS configuration guide. The show cable qos profile command can be used to determine if the specified profile was created by the CMTS. The show cable modem registration command can be used to determine which profile the modem is using. There are no known workarounds.

Table 28 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCeb63785	CMTS will accept DSA-REQ intended to share the same resource ID that is in use by other service flow. There are no known workarounds.
CSCeb64909	During codec change, if MTA issue BW request with both adm/act bit set in qos set type TLV, CMTS does not compare it against the authorized flow spec, and can cause BW reject even if it is within authorized BW. Workaround: Do not use single phase DSC-REQ.
CSCeb70360	After users issue “test cable ucc cx/y <sid> <us_chid>” or “test cable ucc cx/y <sid> <us_chid> 0”, the CM offline counter is incremented by 1 whereas in fact the modem did not go offline at all. The offline counter can be retrieved by issuing “sh cab modem <mac> connectivity” in 12.2BC. Workaround: Use “test cable ucc cx/y <sid> <us_chid> 3” for those modems which support it. If a modem does not support the above, then there are no known workarounds.
CSCeb80293	With multiple cops connections set up to same CMS, any CMTS originating gate messages, such as gate-open, always sent to the first cops connection. There are no known workarounds.
CSCec02495	When the GBIC on a UBR/NPE-G1 is removed and reinserted the **show interface** command or the **show controllers** command may indicate that the newly inserted GBIC is missing or unknown. This is only cosmetic and will not affect the operation of the router. There are no known workarounds.
CSCec08579	With N+1 enabled, the Protect CMTS may crash with the error below if the identical modulation profiles are not configured on Working and Protect CMTS: `"Null Init Mtn Burst Descriptor in MAC scheduler init"` Workaround: Configure Working and Protect CMTS with the same modulation profiles.
CSCec13012	When issuing the command Show Cable Subscriber-usage, the CMTS does not pause with the --More-- prompt between multiple screens of output. There are no known workarounds.
CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information about which radius server to use is downloaded via a protocol other than RADIUS. The problem only happens when no RADIUS server is configured on the router, and no RADIUS server has been configured on the router since it last reloaded. Workaround: Configure a dummy radius server, as in: **radius-server host *x.x.x.x*** Where “x.x.x.x” is an arbitrary ipv4 address.

Table 28 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCec14844	On uBR7200/uBR7100, if there are too many CM/CPEs, there could be CPU HOG error messages when user issues “clear cab modem all delete” or “clear cab modem all reset”. Workaround: Lower the number of CM/CPEs.
CSCec17509	When a batch event message is sent after the call ends, the BCIDs in the message become bogus. There are no known workarounds.
CSCec34056	The CMTS may unexpectedly reload while doing “test pas oir”. Workaround: Unconfigure “cable modem remote-query” functionality.
CSCec36319	If cable intercept is configured on an MC28U/MC16U/MC28X/MC16X interface, when a CM starts to come online, a traceback will be generated. This may also happen randomly when there is data traffic. If the intercepted packets are not IP packets, the encapsulating IP packets’ TOS field may also not be the default TOS value. This happens only with cable intercept command. It should not cause any serious problem besides generating the traceback because the spurious memory access is only due to read, not write. Only in rare cases should the potentially incorrect TOS value cause visible problems. For example, if the intercepted packets' TOS value is set to high priority/low latency while there happens to be other high priority/low latency traffic sharing the links with these intercepted packets. This problem exists since CSCdz45824. Again, this happens only if the intercepted packets are non-IP. Workaround: Avoid configuring cable intercept.
CSCec40145	Downstream MC28U line card hang can occur under extreme CPU load and high traffic conditions. There are no known workarounds.
CSCec50575	When “show cable l2-vpn” is executed, some amount of memory is leaked depending on the number of entries in the l2-vpn table. This issue occurs when l2-vpn entries are present. There are no known workarounds.
CSCec52178	Unexpected giant MAPs with MAP size equal to tens of bucket size are encountered under heavy traffic load. There are no known workarounds.
CSCin20386	This was observed while doing spot checking for cable related CLI’s. There are no known workarounds.
CSCin36963	The port-channel interface may report erratic values for Total drops, broadcasts and interface resets after a member link of the etherchannel fails. There are no known workarounds.

Table 28 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCin37450	The output drops counter of show interface port-channel does not increment when packets are dropped after traffic shaping. There are no known workarounds.
CSCin49029	MTS did not mark the CM which attempts for theft-of-service. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC1c

The caveats listed in Table 29 are resolved in Cisco IOS Release 12.2(15)BC1c. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 29 Closed and Resolved Caveats for Release 12.2(15)BC1c

Caveat ID Number	Description
CSCec87802	High cpu utilization mostly due to CEF Scanner. This issue is observed on a uBR10k series that is running IOS 12.2(15)BC1. There are no known workarounds.

CSCed06821	When the following IOS configurations are used together, some modems become stuck in the state “init (o)” and cannot come online. These modems will cycle through various registration states, but do not come online. The issue is specific to a minority of modem brands.
	`ip tftp-source interface <interface>`
	`- where <interface> is not the cable interface`
	`cable dynamic-secret <any setting>`
	The issue grows to all modem brands if an access lists prevents TFTP traffic between the modem and the <interface> specified above.
	Workaround: Remove the CMTS configuration:
	`ip tftp-source interface <interface> command.`
	`use FTP for logging and management files.`

CSCed14904	A Cisco Universal Broadband Router may reload unexpectedly as a result of it's memory getting corrupted. This issue occurs only when using CMTS remote query feature. Workaround: Disable the CMTS remote query. If the CMTS remote query must be use, then there are no known workarounds.

Table 29 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCed27956	A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Table 29 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCed38527	A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.
CSCed67484	CSCed14039 fixed A WDT problem for the NPE-G1. A first set of diffs were ported from this DDTS to Cable BC release train in Nov., 2003. Later another set of diffs were committed to the same DDTS that fixes the problem at more of a root cause level. This DDTS was opened to port the 2nd commit against CSCec14039 to the Cable BU branches. There are no known workarounds.

Table 29 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCed73075	Customer reported a NPE-400 crash. The crash was identified to be missing of CSCec58486 in the Cable BU BC train. There are no known workarounds.
CSCin43613	The Fast Ethernet (FE) switching performance on a Cisco 7200 series was altered by implementing the fix for: CSCdw00953 - TX-ISL 1 port FE PA wont go DOWN immediately after loss of carrier. The fix went into: 12.2(16)BX 12.3(1)BW 12.2(16)B 12.2(15)ZN 12.2(17)B 12.3(15) PI 12.2(16)S 12.3(15)PI 12.2(15)T 12.2(15) If you are running an IOS list above or later, you may see a performance change from earlier IOS. You regain the performance, you must load an IOS that contains this bug fix. This issue is observed on any FE switching path of a 7200 router. There are no known workarounds.

Open Caveats for Release 12.2(15)BC1b

All the caveats listed in Table 30 are open and reported in Cisco IOS Release 12.2(15)BC1b. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 30 Open Caveats for Cisco IOS Release 12.2(15)BC1b

Caveat ID Number	Description
CSCec06867	If the IP address of a DHCP CPE is changed to a currently unused static IP address, this new IP address will not be allowed into the CMTS host tables and into the CMTS ARP table. And traffic destined to this static IP address will be dropped by the CMTS.

Closed and Resolved Caveats for Release 12.2(15)BC1b

The caveats listed in Table 31 are resolved in Cisco IOS Release 12.2(15)BC1b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 31 Closed and Resolved Caveats for Release 12.2(15)BC1b

Caveat ID Number	Description
CSCea48939	Active Links counter not being decremented properly. The display for “show ip nbar resources” shows Active Links higher than Total Links. Sometimes it shows negative links and sometimes goes to zero. There are no known workarounds.
CSCeb82402	Pings from cable interface of a UBR running 12.1(13)EC4 are failing whenever interface in CEF switching mode has an access-list. Workaround: Using the **no ip route-cache cef** command on the interface fixes the problem.
CSCec10116	MPLS VPN PE router replies with packets which source address taken from global routing table on ICMP Echo Requests sent in VRF to net or broadcast address of a VRF interface via MPLS backbone. There are no known workarounds.
CSCec21392	When set, “no-persistence” is not displayed and saved in the running configuration. Workaround: Configure “no-persistence” again after the router reloads.
CSCec33788	A SNR Reading can not have a correct value if the measurement of that SNR is near a high collision area. The current code does not take to account where the SNR was measured. This problem happen more in current code, because the feature of automatic ranging backoff alogrithm is not working correct. With this feature turn on, the problem is not as gross, but the problem is still there Workaround: Use fixed backoffs for a known number of modems, and the problem is militated since this causing less collisions
CSCec81905	If a ubr7246VXR has more than five downstream interfaces in the chassis (e.g., 3 MC28 cards), calls will start failing on the sixth interface. Gates created for the MTAs connected to the sixth (and higher) interfaces will be stuck. There are no known workarounds.

Open Caveats for Release 12.2(15)BC1a

All the caveats listed in Table 32 are open and reported in Cisco IOS Release 12.2(15)BC1a. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 32 Open Caveats for Cisco IOS Release 12.2(15)BC1a

Caveat ID Number	Description
CSCec06867	If the IP address of a DHCP CPE is changed to a currently unused static IP address, this new IP address will not be allowed into the CMTS host tables and into the CMTS ARP table. And traffic destined to this static IP address will be dropped by the CMTS.

Closed and Resolved Caveats for Release 12.2(15)BC1a

The caveats listed in Table 33 are resolved in Cisco IOS Release 12.2(15)BC1a. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 33 Closed and Resolved Caveats for Release 12.2(15)BC1a

Caveat ID Number	Description
CSCdt10018	The cable provider wants to manage the modems additional from the uBR7223 by using commands like **#sh cable modem remote-query**. However, every cable-subinterface is a member of a vrf-tunnel the modems and are not reachable from the uBR (using SNMP-traps).
CSCea61448	Processor may crash when entering **cable service class** cli commands. Corrupted Program Counter crash can be seen when entering **cable service class** CLI commands. There are no known workarounds.
CSCeb54552	After upgrade from EC train to BC2 train, ubr7200 face issue with modem staying off-line intermittently. This was seen with an upstream that was configured with a fix initial ranging interval. There are no known workarounds.
CSCeb73924	When IGMP join is received from slave interface before configuring IGMP static group on master interface, multicast traffic is not forwarded to the master interface. Workaround: Remove and reapply the multicast static group configurations on the master
CSCec03980	The UGS information described in the CISCO-DOCSEXT-MIB does not show up in 12.2 BC code. There are no known workarounds.

Table 33 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCec04003	An UBR7246VXR seems to “freeze” frequently for some time, stops responding to management, forwarding traffic, and are very slow trying to access it using telnet. When we do a show proc cpu we see that: the highest CPU user is: `35 75661096 46089930 1641 81.06% 84.50% 85.08% 0 CMTS MAC Protoco` Workaround: Enable CEF switching if possible. CEF was enabled to solve the scaling those exact scaling problems that the virus appears to exacerbate Alternative Workaround: Configure service internal ip route-cache 30 2 3 or less severe ip route-cache 30 10 10 In order to reduce the route cache size Refer to the following for more information about these two workarounds: http://www.cisco.com/warp/public/707/advisory.html http://www.cisco.com/warp/customer/63/ts_codred_worm.shtml

Table 33 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description

CSCec15728	On a uBR7100 CMTS Modular QoS via the CLI are not configurable in 122-15.BC1 feature set ubr7100-ik8s-mz in which this feature is supported. They are configurable in previous IOS's.
	Example:
	`class-map match-any MAIL`
	`  match protocol pop3`
	`  match protocol smtp`
	`  match protocol nntp`
	`  match protocol secure-pop3`
	`  match protocol secure-nntp`
	`class-map match-any MULTIMEDIA`
	`  match protocol netshow`
	`  match protocol streamwork`
	`  match protocol vdolive`
	`  match protocol cuseeme`
	`  match protocol realaudio`
	`class-map match-any FILEXFER`
	`  match protocol ftp`
	`  match protocol secure-ftp`
	`  match protocol nfs`
	`  match protocol printer`
	`class-map match-any HTTP`
	`  match protocol http`
	`  match protocol secure-http`
	`  match protocol gopher`
	`class-map match-any FILESHARE`
	`  match protocol gnutella`
	`  match protocol napster`
	`  match protocol fasttrack`
	`class-map match-all FILESHARE-WAN`
	`  match class-map FILESHARE`
	`  match not access-group 190`
	`class-map match-all HTTP-WAN`
	`  match class-map HTTP`
	`  match not access-group 190`
	`class-map match-all MULTIMEDIA-WAN`
	`  match class-map MULTIMEDIA`
	`  match not access-group 190`
	`class-map match-all FILEXFER-WAN`
	`  match class-map FILEXFER`
	`  match not access-group 190`
	`class-map match-all MAIL-WAN`
	`  match class-map MAIL`
	`  match not access-group 190`
	These commands are no longer configurable:
	`ubr7111-A(config)#class-map match-any MAIL`
	`                                   ^`
	`% Invalid input detected at '^' marker.`
	This problem has only been observed on a uBR7100 platforms with IOS 122-15.BC1 and does not occur on the ubr7200.
	Workaround: Use a previous IOS to use these features. Previous IOS do not have this problem and can be used to run this feature.

Table 33 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCec16832	When a PCR value is defined for an ATM PVC on a uBR7246VXR running 12.2(11)BC3 images, the PCR definition is not accepted. CBR values are properly applied to the ATM circuit. This can be observed in the **sh atm pvc** command. There are no known workarounds.

CSCec17997	When a large number of modems are on a single upstream it takes them a long time to get to (r1) state. The root cause is that the algorithm for automatically adjusting the ranging backoff window was broken in BC. The work around is to fix the ranging backoff to a large value:
	`cable up 0 ranging 6 9`
	Additional improvement is reached by configuring this on all upstreams if all upstreams share the same frequency.
	Additional optimization is reached by decreasing the IM interval:
	`cable insertion interval automatic 20 250`
	There are no known workarounds.

CSCec25534	The following message displays yet plenty of free memory seems to be available.
	`%NBAR-1-MAXMEMORYUSED: Reached maximum amount of memory allocated for stile`
	Memory calculation for NBAR maximum allocation limit is wrong when amount of free memory is over 214.8MB at router initialization. This causes a pre-mature warning message:
	`%NBAR-1-MAXMEMORYUSED: Reached maximum amount of memory allocated for stile`
	The Above message only informs you that you are low on NBAR memory. The router will continue classifying correctly. Mis-classification is not occurring until you see the error:
	`%NBAR-1-NOSTATEMEM: Memory for maintaining state used up`
	There are no known workarounds.

CSCec29381	If a CMTS, running 12.2(15)BC, receives an event-generation-object (in a gate-open message) containing attributes measuring more than 255 bytes in length, it ignores that attribute and does not generate an event message (RADIUS message). This is a severe issue for CALEA functionality because if the SDP string passed within the event-generation-object is greater than 255 bytes, no event message would be generated. Note that CALEA is NOT a packetable 1.0 functionality, so this issue does not affect packetable 1.0 deployments. There are no known workarounds.

Table 33 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCec36216	When enabling the cable dynamic-secret command on the Cisco CMTS in IOS 12.2(15)BC1, certain cable modems may later become stuck in the state init(o) and be unable to come online. Disabling the cable dynamic-secret command brings these modems back online immediately. IMPORTANT: The modems which become stuck in init(o) are limited to certain brands / models, and are a repeatable subset of all modems on the CMTS. This occurs when cable dynamic-secret is enabled on the cable interface IOS 12.2(15)BC1 on uBR7200, uBR7100, and uBR10K. Specific brands and software versions of cable modems become stuck in state init(o) only when dynamic secret is enabled, and immediately come online when dynamic secret is disabled. All other modems come online and work normally. Lab investigation indicates that these modems are NOT DOCSIS COMPLIANT, and are storing the TFTP server IP address from the initial DHCP offer (before Dynamic Shared Secret was enabled) and requesting the new TFTP file name from the old server, the old server cannot find the encrypted filename, so the modem is stuck in init(o). Workaround: a) Power cycle the affected cable modem b) Further work around are being evaluated by Cisco engineering at this time for the various modems. c) Disable cable dynamic secret, use TFTP-enforce and cable source-verify instead.
CSCec37571	A Cisco router may reload due to low memory. This problem occurs when BPI+ is in use. There are no known workarounds.
CSCec50650	The number of attributes in Radius header for QoS_Reserve and QoS_Commit event messages that are sending to CALEA Delivery Function (DF) is incorrect if the Session Description Protocol (SDP) attribute's length is greater than 247. There are no known workarounds.

Open Caveats for Release 12.2(15)BC1

All the caveats listed in Table 34 are open and reported in Cisco IOS Release 12.2(15)BC1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 34 Open Caveats for Cisco IOS Release 12.2(15)BC1

Caveat ID Number	Description
CSCec06867	DHCP CPE IP address cant be changed until ARP timeout
CSCec07002	All modems on some upstreams offline when 6000+ modems on CMTS

Closed and Resolved Caveats for Release 12.2(15)BC1

The caveats listed in Table 35 are resolved in Cisco IOS Release 12.2(15)BC1. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 35 Closed and Resolved Caveats for Release 12.2(15)BC1

Caveat ID Number	Description
CSCdu13269	Attempt to free Unassigned memory, System reloads
CSCdu53656	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCdz46435	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_srcad
CSCdz71127	corrupted packet can cause input queue wedge - reg to CSCdx02283
CSCdz74683	rate-limiting should happen after PHS is taken into account
CSCdz85694	SYS-2-INTSCHED:may_suspend when changing GigE config on NPE-G1
CSCea02355	rare ip packets may cause input queue wedge
CSCea08892	change buffer allocations in VXR
CSCea14372	CMTS should calculate the dynamic map advance based on max delay
CSCea21911	CMTS Crashes randomly under load

Table 35 Closed and Resolved Caveats for Release 12.2(15)BC1 (continued)

Caveat ID Number	Description
CSCea28131	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCea29514	NPE-G1:Aux port do not work after changing configuration
CSCea41560	show cable modem verbose shows wrong value for active classifiers
CSCea55917	LC-HA:BPI broken for dynamic service flows
CSCea56592	OIR causes Q Wedge with bundle when OIR of different card types
CSCea57826	NPE-G1:GE Rx input stuck
CSCea60814	Internal configuration file editor does no longer work
CSCea64738	make <cable int> optional in clear cable modem command
CSCea71170	LC-HA: First switch-over from W->P fails when call is in session
CSCea78353	Intermittent packet drop by CEF when interface is cable bundle master
CSCea81983	Pktcbl: should delete associate DS SF when receiving US SF DSD
CSCea88356	ubr7200/MC16B:Calibration bad for 3.2MHz channel width
CSCea92361	7200/16s:DSP stops responding with continuous SNMP query. (ACK 39)
CSCea92806	NPEG1 crashed during PA-MC-E3 OIR
CSCea93586	OIR causes trace backs at cmts_ds_trafshap_out
CSCeb01067	NPE-G1:Add support for MRVL88E1111 PHY and remove debugs
CSCeb02553	Upstream port in shared spectrum group can go down and stay down
CSCeb09043	CMTS stops generating Initial Maintenance opportunities
CSCeb11987	Pktcbl: em-n-02182 remove Call Answer and Disconnect EM
CSCeb12127	Traceback from cmts_check_us_input_power_level_range
CSCeb12966	Pktcbl: remove media_cnx object per ECN dqos-n-02185
CSCeb13881	Alignment error and traceback at cmts_rx_interrupt, cmts_mac2
CSCeb14298	Pktcbl: clfr information missing/broken in CMTS DSC-REQ
CSCeb14562	Gig intf on NPE-G1 bounces when adding bridging on subintf
CSCeb21271	CSCdz66185 limits the number of DOCSIS 1.0+ modems allowed on a DS
CSCeb22301	NPE-G1 breaks into ROMMON or boot-mode when boot up
CSCeb29707	Interface counters show output drops when no drops in serv.flow count
CSCeb38067	all cms offlined in MC16C in 12.1(10)EC1 and 12.1(13)EC3.
CSCeb38851	Traceback and Alignment errors in DMIC routines

Table 35 Closed and Resolved Caveats for Release 12.2(15)BC1 (continued)

Caveat ID Number	Description
CSCeb40414	CLI for modulation profile does not check validity if first digit 0
CSCeb44085	PacketCable: Gate Open is not being sent
CSCeb44118	Packetcable: Radius information is not being send
CSCeb45272	CMTS crash during modem registration
CSCeb45392	Add protection for a NULL pointer in cmts_bind_cm_to_upstream
CSCeb46162	PacketCable: Bogus gate id lookup error when service flow timeout
CSCeb51330	Traceback and traffic stop after OIR in int-bundling env
CSCeb56680	Modem entry can exist on multiple interfaces
CSCeb58771	fair_enqueue called from process without int protection
CSCeb59740	ubr7200 may crash with FIFO queueing on DOCSIS interface
CSCeb63130	CMTS does not send DSD after receiving gate-delete
CSCeb63747	Modems online with 0.0.0.0 IP address
CSCeb82492	load balancing: threshold stability cmd wrong in NVRAM
CSCeb84099	MC16S:cmts crash at Bus Error after DSP failed to respond
CSCeb85140	ALIGN-3-SPURIOUS traceback with pktcbl_handle_commit_msg
CSCin20408	CMTS displays invalid CLI under show cable tech-support output
CSCin29936	ciscoEnvMonSupplySource returns incorrect values
CSCin31951	SNMP: Traceback at timer_start while config session timeout to max va
CSCin36943	Show Version displays erratic number of interfaces after OIR of FE

Open Caveats for Release 12.2(11)BC3d

There are no open caveats specific to Cisco IOS Release 12.2(11)BC3d that require documentation in the release notes.

Closed and Resolved Caveats for Release 12.2(11)BC3d

The caveat listed in Table 36 is resolved in Cisco IOS Release 12.2(11)BC3d. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 36 Closed and Resolved Caveats for Release 12.2(11)BC3c

Caveat ID Number	Description
CSCeb78345	Initial maintenance slots not created under some circumstances

Open Caveats for Release 12.2(11)BC3c

Except for the caveats listed as closed and resolved in Table 37, Cisco IOS Release 12.2(11)BC3c contains the same open caveats as Cisco IOS Release 12.2(11)BC3b, which are listed in Table 38.

Closed and Resolved Caveats for Release 12.2(11)BC3c

The caveats listed in Table 37 are resolved in Cisco IOS Release 12.2(11)BC3c. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 37 Closed and Resolved Caveats for Release 12.2(11)BC3c

Caveat ID Number	Description
CSCdz71127	corrupted packet can cause input queue wedge - reg to CSCdx02283 Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available. Cisco has made software available, free of charge, to correct the problem. This advisory is available at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
CSCea02355	rare ip packets may cause input queue wedge Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available. Cisco has made software available, free of charge, to correct the problem. This advisory is available at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
CSCeb09043	CMTS stops generating Initial Maintenance opportunities

Open Caveats for Release 12.2(11)BC3b

All the caveats listed in Table 38 are open and reported in Cisco IOS Release 12.2(11)BC3b. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 38 Open Caveats for Cisco IOS Release 12.2(11)BC3b

Caveat ID Number	Description
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdy10666	Remote-query: Inconsistencies observed while unconfiguring/re-config
CSCdy12874	UBR7200+PPPoE: CMTS hanged on OIR with PPPoE configuration
CSCdy68181	7200/N+1:Modems ping drop after switch over to Protect
CSCea06194	Memory allocation errors on Working CMTS

Table 38 Open Caveats for Cisco IOS Release 12.2(11)BC3b (continued)

Caveat ID Number	Description
CSCea13693	Cable modems going off when number of online CM is more than 2500
CSCea48727	two bus errors at cmts_high_prio_tx_safe, at invalid address
CSCea52884	big % of modem flap after upgrade to BC2 from EC
CSCea53868	re-registration with different QoS error after N+1 switch over
CSCeb26840	Cable DS CIR Problem
CSCeb29377	cable modem remains offline until shut/no shut is made on upstream
CSCeb29707	Interface counters show output drops when no drops in serv.flow count
CSCin14761	Cable Intf accounting does not increment for ip multicast pkts
CSCin16705	Configuring mac-address at the cable interface causes cable link dow
CSCin20386	show interfaces cable downstream CLI shows incorrect value for DnIf
CSCin21618	OC-12 CMTS got hanged with OIR on SRP interface
CSCin28359	Spurious memory access observed pas_eeprom_compare after OIR
CSCin36963	Port-channel interface reports erratic interface counter values

Closed and Resolved Caveats for Release 12.2(11)BC3b

The caveats listed in Table 39 are resolved in Cisco IOS Release 12.2(11)BC3b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 39 Closed and Resolved Caveats for Release 12.2(11)BC3b

Caveat ID Number	Description
CSCea30518	CMTS crashing in cmts_update_srv_flow_pak_stats
CSCea50842	Range check missing in UCC-RSP handling
CSCea90978	Cable modem US DS counters not retained after CM resets/flapped

Open Caveats for Release 12.2(11)BC3

All the caveats listed in Table 40 are open and reported in Cisco IOS Release 12.2(11)BC3. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 40 Open Caveats for Cisco IOS Release 12.2(11)BC3

Caveat ID Number	Description
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdy09392	7200/16S: sh cable modem xxxx cnr does not show CNR (ACK40)
CSCdy10666	Remote-query: Inconsistencies observed while unconfiguring/re-config
CSCdy12874	UBR7200+PPPoE: CMTS hanged on OIR with PPPoE configuration
CSCdy68181	7200/N+1:Modems ping drop after switch over to Protect

Table 40 Open Caveats for Cisco IOS Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCea06194	Memory allocation errors on Working CMTS
CSCea08892	change buffer allocations in VXR
CSCea13693	Cable modems going off when number of online CM is more than 2500
CSCea14372	CMTS should calculate the dynamic map advance based on max delay
CSCea19174	static CPE added in bundle forwarding table w/ source-verify dhcp
CSCea29697	CMTS rejects CM REG-REQ due to MIC failure, when configured encrypt
CSCea30518	CMTS crashing in cmts_update_srv_flow_pak_stats
CSCea41560	show cable modem verbose shows wrong value for active classifiers
CSCea45540	Invalid Service template with state of 145 seen for DS QoS on CMTS
CSCea48727	two bus errors at cmts_high_prio_tx_safe, at invalid address
CSCea51028	NPE-G1 crash by watchdog
CSCea51119	NPE-G1 crashed due to memory corruption
CSCea52884	big % of modem flap after upgrade to BC2 from EC
CSCea53868	re-registration with different QoS error after N+1 switch over
CSCea56592	OIR causes Q Wedge with bundle when OIR of different card types
CSCin14761	Cable Intf accounting does not increment for ip multicast pkts
CSCin14866	access-list match counter behaves improperly for tcp-ack pkts
CSCin16705	Configuring mac-address at the cable interface causes cable link dow
CSCin20386	show interfaces cable downstream CLI shows incorrect value for DnIf
CSCin20408	CMTS displays invalid CLI under show cable tech-support output
CSCin21618	OC-12 CMTS got hanged with OIR on SRP interface
CSCin28359	Spurious memory access observed pas_eeprom_compare after OIR
CSCin36963	Port-channel interface reports erratic interface counter values

Closed and Resolved Caveats for Release 12.2(11)BC3

The caveats listed in Table 41 are resolved in Cisco IOS Release 12.2(11)BC3. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 41 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC3

Caveat ID Number	Description
CSCdx00274	PA-FE input stuck with burst traffic
CSCdx35070	Change the default unique word (uw) to 16 for 16qam short/long burst
CSCdx63927	ubr7200 memory corruption
CSCdy57048	MPLS/Tag switching results in invalid TCP packet
CSCdz03063	NPE-G1:CPU hang up to 1 min after insert and/or remove compact flash
CSCdz15209	7206VXR may crash and go to ROMMON with NPE-G1 and I/O on bootup.

Table 41 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCdz35936	PPPoE termination does not work with CEF switching
CSCdz47039	NPE-G1: high packet drops between gig intf when CBFWQ and no congest
CSCdz48152	ARP fails after configuring no cable arp
CSCdz55120	cdxIfUpChannelCmRegistered does not include OnlineNetAccessDisabled
CSCdz60543	TEK_INVALID_INVALID_KEY_SEQUENCE_NUMBER for cm 0000.0000.0000
CSCdz61789	Crashes at cmts_print_sid_subint due to sid freed for UGS
CSCdz63050	NPE-G1:Output drop and bad length count up
CSCdz63364	Upstream state is not updated when an interface is shut down
CSCdz73107	Optimize cmts bundle aging process
CSCdz74634	PktCbl: Corner cases can leave Resv or Com gates w/out serv-flows
CSCdz74952	PktCbl: Only 1 gate-open should be sent per gate.
CSCdz86533	Spectrum-group enabled upstreams shutdown when hop occurs
CSCdz87887	MC16S with NPE-G1 hangs when a particular CLI command is entered
CSCdz88353	Traffic forwarded to CM/CPE when in Reject(m) state
CSCea01292	Need to port CSCdv34236 to flo_t_pokemon
CSCea02922	Minislot-size 2 is missing from the CLI
CSCea03469	no router bgp can crash a badly configured router in BGP-CLNS
CSCea06194	Memory allocation errors on Working CMTS
CSCea09938	Protect CMTS crash at cmts_hccp_become_active
CSCea09965	Crash with illegal access to rx_pakp NULL tail pointer.
CSCea10610	PKTCBL: wrong SDP downstream attribute code in EM
CSCea11519	%LINK-0-REENTER: Fatal re-entrancy, Level 3
CSCea12937	Giga interface of ubr7200 giving Duplex mismatch error
CSCea16841	Gate-set-err not sent when received extra gate-set for same gate
CSCea18034	Add service flow and slot info to show packetcable gate summary CLI
CSCea19339	QoSCommit does not meet Pkt. Cable specifications, extra parameter
CSCea23522	CMTS crashes on OIR
CSCea23696	CMTS Crash observed after show int c3/1 sid command
CSCea29384	PPPoE packet header get corrupted
CSCea30263	After OIR of bundle master modems on slave intfs loose connectivity
CSCea48330	MC16S hangs when used with NPE-G1, under certain CLI commands
CSCea49435	Voice sfid on online(d) modem does not work
CSCin29873	Inconsistent ouput shown by show env last
CSCin32094	UBR7200:Cmts crashed on <show int cx/y sid n counter>
CSCin33046	CPE1 mac got replaced by CPE2 mac with Sub-interface and IFB scenario

Table 41 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCdx77088	Software forced crash - watchdog timeout in pool_process
CSCdz55178	QoS profile name of more then 32 chars will crash the router

Open Caveats for Release 12.2(11)BC2

All the caveats listed in Table 42 are open in Cisco IOS Release 12.2(11)BC2. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 42 Open Caveats for Cisco IOS Release 12.2(11)BC2

Caveat ID Number	Description
CSCdw01790	Cable MPLS VPN Arp entry in global table for VPN modem
CSCdx00274	PA-FE input stuck with burst traffic
CSCdx25516	CM can spoof QoS once with no cable qos permission modem.
CSCdx35070	Change the default unique word (uw) to 16 for 16qam short/long burst
CSCdx58924	Dynamic modulation profile switchover does not work correctly
CSCdx59958	Multi-cast fails for the CPE connected behind the slave interface
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdx90989	DOCSIS CPE Configurator has Java error on Pentium IV Windows PC
CSCdy04675	SRP Topology timer is improperly initialized
CSCdy09392	7200/16S: sh cable modem xxxx cnr does not show CNR
CSCdy12874	UBR7200+PPPoE: CMTS hanged on OIR with PPPoE configuration
CSCdy41190	show cable modem <MAC> verbose shows a wrong QOS Prodfile Index
CSCdy52237	FEC Codeword length change causes invalid UCDs
CSCdy60025	Bit fields for ToS overwrite of reversed compared to EC
CSCdy68181	7200/N+1:Modems ping drop after switch over to Protect
CSCdy77073	Higher amount of CPEs at CPE counter
CSCdy89339	source-verify dhcp does not stop traffic for ip 0.0.0.0
CSCdz07946	can not define MQC priority command on RP
CSCdz15526	Optimization in shutting subinterface
CSCdz19454	Need a way to determine which modems cpe with static ips are behind
CSCdz23695	CPE database not updated with static IP address of new CPE until ARP
CSCdz25290	CMTS Software forced crash with PacketCable calls
CSCdz28905	unable to clear cable host
CSCdz33772	Incorrect counters in show ip mroute count output w/ mroute-cache
CSCdz35936	PPPoE termination does not work with CEF switching
CSCdz36601	Traceback at c10k_ttcm_turboacl_deconfigure_qos_acl for PBR acls

Table 42 Open Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
CSCdz39744	IPC errors during boot up
CSCdz42303	2 Modems are assigned the same SID after switchover
CSCdz42719	successive shut/no shut corrupts ARP table on CMTS
CSCdz44917	OC12 SRP Card Crash During Bootup
CSCdz48152	ARP fails after configuring no cable arp
CSCdz50750	PRE Crash at cmts_remove_bundle_entry during N+1 switchover
CSCdz54017	Modems stuck in init(rc) on 3 interfaces
CSCdz55120	cdxIfUpChannelCmRegistered does not include OnlineNetAccessDisabled
CSCdz57190	hosts on the slaves loose multicast if pim configured on other cable
CSCdz57216	PRE crash when forwarding a high volume of multicast traffic
CSCdz58277	Memory leak when modems fail to register with BPI enabled
CSCdz58321	Traceback when router boots up
CSCdz58875	POS connectivity failure, IPM overrun problem
CSCdz60543	TEK_INVALID_INVALID_KEY_SEQUENCE_NUMBER for cm 0000.0000.0000
CSCdz61789	Crashes at cmts_print_sid_subint due to sid freed for UGS
CSCdz63364	Upstream state is not updated when an interface is shut down
CSCin14761	Cable Intf accounting does not increment for ipmulticast pkts
CSCin14866	access-list match counter behaves improperly for tcp-ack pkts
CSCin16705	Configuring mac-address at the cable interface causes cable link dow
CSCin19059	CMTS crashed while doing OIR with many features configured at CLC
CSCin20386	show interfaces cable downstream CLI shows incorrect value for DnIf
CSCin20408	CMTS displays invalid CLI under show cable tech-support output
CSCin22969	cable master Int. configs also reflects at Slave Int in a Bundle
CSCin25027	cable source-verify dhcp failed with shut/no shut at cable interface
CSCin27393	SRP card flaps and tracebacks seen in show logging
CSCin28359	Spurious memory access observed pas_eeprom_compare after OIR

Closed and Resolved Caveats for Release 12.2(11)BC2

The caveats listed in Table 43 are resolved in Cisco IOS Release 12.2(11)BC2. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 43 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC2

Caveat ID Number	Description
CSCdw66742	GSR snmp ifindex persist does not keep the index values
CSCdx27083	Fast switching intermittently broken on CMTS
CSCdx58979	SNR was not displayed in show cable modem verbose output
CSCdx86517	NBAR protocol discovery may originates Spurious Accesses
CSCdy09508	linkUp trap is not sent for Cable interface upon card reinsert
CSCdy17114	Memory allocation failure in public buffer pools
CSCdy27344	upstream stuck in shutdown
CSCdy46139	ALL FF mac entry shown in cable bundle forwarding table
CSCdy48881	Secondary (supernet) address not deleted properly
CSCdy51773	enabling CDP under fast ethernet of ubr10k causes an interface reset
CSCdy58361	CMTS crash on watchdog timeout, process = CMTS MAC Protocol
CSCdy65160	Attempt to monitor uninitialized watched boolean (address 0)
CSCdy68134	Memory leaks when cable modulation profile is changed
CSCdy70193	Crash in timer_start64, cmts_update_lease_time, cmts_dhcp_glean
CSCdy72163	BC release Lacks fixes for CSCdt44322, dt59452, du28934. Patch it.
CSCdy73203	Through SSH Session Successful DOCSIS Pings Will Return FFFF Values
CSCdy73261	Pktcable: Several extra EM messages are generated with one voice call
CSCdy74329	AAA updates acct-delay-time attribute blindly
CSCdy75095	CMTS crash when service flow log id wrapped around in heavy system
CSCdy76407	Protect CMTS Crash During Show HCCP Detail
CSCdy76674	source-verify leasetimer config shows up on sub-interface
CSCdy76724	PRE Crash at sch_handle_headsail_pak, ip_fastswitch_wrapper
CSCdy77927	show cable host does not work for ubr10k (works for 7200)
CSCdy80368	scheduler allocate does not work on native GE ports on NPE-G1
CSCdy83321	Working CMTS crash during switch-over from Protect
CSCdy83754	ToS based rate-limiting not working
CSCdz01140	Overlapping IP address assignment can cause denial of service
CSCdz03584	crash when configuring more than 6 OUIs with int config file editor
CSCdz06164	CMTS: IP connectivity failure to Cable Modem and CPE
CSCdz06773	modems stuck in init(rc) in 1st cable bundle, 2nd ok
CSCdz07186	Internal config file editor does not support BPI objects
CSCdz08304	NPE-G1 - Static hosts behind CM can loose IP connectivity

Table 43 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
CSCdz11970	QOS profile max-burst range restore to 65535 for CLI
CSCdz14740	Back out CSCdy65174 - entPhysicalDescr is incorrect
CSCdz14783	Traceback occurs during switchover
CSCdz15213	PXF crashes when tag-switching enabled
CSCdz16916	Static hosts behind CM w/ multiple IP on one MAC loose connectivity
CSCdz17448	wrong range in docsIfQosProfMaxTransmitBurst in rfmib v4
CSCdz18615	CMTS - Need to un-hide the show int Cable X/Y modem 0 command
CSCdz19054	ifAlias entries are empty for ubr10k
CSCdz20869	Reload via SNMP makes the CMTS not to see the CPEs anymore
CSCdz22575	Pktcbl: CALEA support for call data
CSCdz23109	Uncorrectable FEC errors increment too fast on certain upstreams
CSCdz25778	min reserved rate sfids misbehave under interface congestion
CSCdz32296	SNR unknown, spec group assigned, freq not assigned
CSCdz42057	cdxCmtsCmRegistered shows wrong count
CSCin13783	Bundling crash on bootup and after LC switch-over
CSCin18551	DOCSIS11:Spurious memory access with cmts_msched_admit_rtps_srv func
CSCin19062	After OIR, some of the cable features are removed from the running-c
CSCin19295	IPC failure for TCCplus card and Traceback observed at CMTS
CSCin19758	GENERAL-3-EREVENT: No current_if_info and Traceback at CMTS
CSCin20365	Tracebacks seen while configuring badipsource buffer to high valu
CSCin20444	CMTS got hanged while doing clear cable host ? after done with sour

Open Caveats for Release 12.2(11)BC1b

There are no open caveats specific to Cisco IOS Release 12.2(11)BC1b that require documentation in the release notes.

Closed and Resolved Caveats for Release 12.2(11)BC1b

The caveat listed in Table 44 is resolved in Cisco IOS Release 12.2(11)BC1b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 44 Closed and Resolved Caveats for Release 12.2(11)BC1b

Caveat ID Number	Description
CSCdz16916	Static hosts behind CM w/ multiple IP on one MAC loose connectivity

Open Caveats for Release 12.2(11)BC1a

All the caveats listed in Table 45 are open in Cisco IOS Release 12.2(11)BC1a. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 45 Open Caveats for Release 12.2(11)BC1a

Caveat ID Number	Description
CSCdz15213	PXF crashes when tag-switching enabled
CSCdz16916	Static hosts behind CM w/ multiple IP on one MAC loose connectivity
CSCdz11970	QOS profile max-burst range restore to 65535 for CLI
CSCdy17114	Memory allocation failure in public buffer pools

Closed and Resolved Caveats for Release 12.2(11)BC1a

All the caveats listed in Table 46 are resolved in Cisco IOS Release 12.2(11)BC1a. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 46 Closed and Resolved Caveats for Release 12.2(11)BC1a

Caveat ID Number	Description
CSCdz06164	CMTS: IP connectivity failure to Cable Modem and CPE
CSCdz08304	Static hosts behind CM can loose IP connectivity

Open Caveats for Release 12.2(11)BC1

All the caveats listed in Table 47 are open in Cisco IOS Release 12.2(11)BC1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 47 Open Caveats for Release 12.2(11)BC1

Caveat ID Number	Description
CSCdw01790	Cable MPLS VPN Arp entry in global table for VPN modem
CSCdx25516	CM can spoof QoS once with no cable qos permission modem.
CSCdx58924	Dynamic modulation profile switchover does not work correctly
CSCdx58979	SNR was not displayed in show cable modem verbose output
CSCdx59958	Multi-cast fails for the CPE connected behind the slave interface
CSCdx62568	Cannot config cable match addr on sub-int for encrypted multicast
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdx73158	Modems Show Online on both Working & Protect Line Card
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdy04675	SRP Topology timer is improperly initialized
CSCdy09508	linkUp trap is not sent for Cable interface upon card reinsert

Table 47 Open Caveats for Release 12.2(11)BC1 (continued)

Caveat ID Number	Description
CSCdy27344	upstream stuck in shutdown
CSCdy52237	FEC Codeword length change causes invalid UCDs
CSCdy56613	During PRE switch-over, the secondary comes up then gets rebooted
CSCdy60025	Bit fields for ToS overwrite of reversed compared to EC
CSCdy83321	Working CMTS crash during switch-over from Protect
CSCin13783	Alignment error in c10k_mdfs_delete_midb_event()
CSCin14761	Cable Intf accounting does not increment for ipmulticast pkts
CSCin19059	CMTS crashed while doing OIR with many features configured at CLC

Closed and Resolved Caveats for Release 12.2(11)BC1

All the caveats listed in Table 48 are resolved in Cisco IOS Release 12.2(11)BC1. This table describes only severity 1 and 2 caveats and select severity 3 caveats

Table 48 Closed and Resolved Caveats for Release 12.2(11)BC1

Caveat ID Number	Description
CSCdt55744	crash in handle_key_req in 12.1(9.5)EC
CSCdw66742	GSR snmp ifindex persist does not keep the index values
CSCdw79462	CM did not become online in init(o) state w/bundling
CSCdw79462	CM did not become online in init(o) state w/bundling
CSCdw86707	Need the ability to disable the overheat auto-shutdown in conf t
CSCdx36497	[PDSN-R1.1]MALLOCFAIL/Block overrun on SIP w/high traffic rates
CSCdx37957	SNMP: Unerrored MIB decrementing (transmission.127.1.1.4.1.2)
CSCdx58550	Process= <interrupt level>, ipl=4, pid=47, bad enqueue
CSCdx73117	PRE Crash during N+1 switchover
CSCdx84066	show cable modem cable x upstream y summ display upstream y-1 info
CSCdx92196	Upstream admission control cant be turned off
CSCdx93143	sfids with minimum rate have worse performance than BE service flows
CSCdy00568	AWACS2/16S: Acterna power display inaccuracy
CSCdy01346	per modem and host access-lists do not work in 12.2(8)Bc1
CSCdy06163	PRE Crash After N+1 Switch Over
CSCdy06170	Traceback & Alignment errors.
CSCdy08691	DSP timeout & Acterna stop running when change mod.profile in CLI
CSCdy08808	CMTS crashes while changing modulation profile due to memory corrupt
CSCdy09508	linkUp trap is not sent for Cable interface upon card reinsert
CSCdy10672	TLB exception in cmts_cm_lookup
CSCdy13053	Standby linecard may crash after fail-back with spectrum management

Table 48 Closed and Resolved Caveats for Release 12.2(11)BC1 (continued)

Caveat ID Number	Description
CSCdy16384	RPF command may not be propagated to Toaster
CSCdy17477	After DHCP, CPE continues to show up as a static CPE
CSCdy17492	Line CON 0 and VTYs cannot be cleared
CSCdy17744	docsIfCmtsCmStatusSignalNoise returns in dB and not TenthdB
CSCdy18348	PRE Crash at cmts_find_bundle_entry & cmts_bundle_pkt
CSCdy18483	16S: three extra protective measures to prevent flash corruption
CSCdy20256	IP TOS overwrite not working on non-primary Upstream SFID on DOC1.1
CSCdy20580	Traceback seen while CLI with Acterna
CSCdy21165	Cable bundle entries do not timeout even when CPE/CM goes away
CSCdy21326	CM failed came online with - cable tftp-enforce functionality
CSCdy21713	Bundle fwding table timeouts can cause problem in adjacency creation
CSCdy22443	Spectrum manag. show command may crash during line card fail-over
CSCdy22616	Line Crash while adding it into a redundancy group on a live system
CSCdy32329	SW workaround to pass manufacturing test
CSCdy39316	Race condition in turbo acl compile and ACL delete can lead to crash
CSCdy41669	DOCSIS1.1: Fragmented packets with extended headers can cause crash
CSCdy43737	Multicast packets not forwarded on cable bundle slave interfaces
CSCdy43737	Multicast packets not forwarded on cable bundle slave interfaces
CSCdy46809	Crash in cmts_show_cm
CSCdy48881	Secondary (supernet) address not deleted properly
CSCdy50129	crash while sending icmp unreachable on cmts. (send_unreachable)
CSCdy51773	enabling CDP under fast ethernet of ubr10k causes an interface reset
CSCdy52470	Crash after %SYS-2-NOTQ: unqueue did not find 0 in queue 622FF200
CSCdy57548	Error message %SYS-2-LINKED Bad enqueue message
CSCdy57847	Traceback when doing no cable source-verify dhcp
CSCdy58361	CMTS crash on watchdog timeout, process = CMTS MAC Protocol
CSCdy65160	Attempt to monitor uninitialized watched boolean (address 0)
CSCdy70193	Crash in timer_start64, cmts_update_lease_time, cmts_dhcp_glean
CSCdy72163	BC release Lacks fixes for CSCdt44322, dt59452, du28934. Patch it.
CSCdy73261	Pktcable: Several extra EM messages are generated with one voice call
CSCdy75095	CMTS crash when service flow log id wrapped around in heavy system
CSCdy76407	Protect CMTS Crash During Show HCCP Detail
CSCdy76724	PRE Crash at sch_handle_headsail_pak, ip_fastswitch_wrapper

Open Caveats for Release 12.2(8)BC2a

There are no open caveats specific to Cisco IOS Release 12.2(8)BC2a that require documentation in the release notes.

Closed and Resolved Caveats for Release 12.2(8)BC2a

All the caveats listed in Table 49 are resolved in Cisco IOS Release 12.2(8)BC2a. This table describes only severity 1 and 2 caveats and select severity 3 caveats

Table 49 Closed and Resolved Caveats for Release 12.2(8)BC2a

Caveat ID Number	Description
CSCdy10672	TLB exception in cmts_cm_lookup

Open Caveats for Release 12.2(8)BC2

All the caveats listed in Table 50 are open in Cisco IOS Release 12.2(8)BC2. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 50 Open Caveats for Release 12.2(8)BC2

Caveat ID Number	Description
CSCdw01790	Cable MPLS VPN Arp entry in global table for VPN modem
CSCdx25516	CM can spoof QoS once with no cable qos permission modem.
CSCdx58560	Display slave vcci info for bundled subints in sh hard pxf cpu sub
CSCdx58924	Dynamic modulation profile switchover does not work correctly
CSCdx58979	SNR was not displayed in show cable modem verbose output
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdx73158	Modems Show Online on both Working & Protect Line Card
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdx93047	Crash when adding Cable Source-verify DHCP to sub-interface
CSCdx93143	sfids with minimum rate have worse performance than BE service flows
CSCdy06165	Traceback at cmts_glean,cmts_arp_glean, ip_arp_merge
CSCdy08808	CMTS crashes while changing modulation profile due to memory corrupt
CSCdy09508	linkUp trap is not sent for Cable interface upon card reinsert
CSCdy10672	TLB exception in cmts_cm_lookup
CSCdy11548	Fancy queueing commands missing from cmts policy-map config
CSCdy15858	Change Modulation Profile Defaults: FEC codeword size
CSCdy17492	Line CON 0 and VTYs cannot be cleared
CSCdy18348	PRE Crash at cmts_find_bundle_entry & cmts_bundle_pkt

Table 50 Open Caveats for Release 12.2(8)BC2 (continued)

Caveat ID Number	Description
CSCin13206	Schooner:%SCHED-3-UNEXPECTEDEVENT: Process received unknown event
CSCin14535	Traceback and Spurious Accesses observed at CMTS

Closed and Resolved Caveats for Release 12.2(8)BC2

All the caveats listed in Table 51 are resolved in Cisco IOS Release 12.2(8)BC2. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 51 Closed and Resolved Caveats for Cisco IOS Release 12.2(8)BC2

Caveat ID Number	Description
CSCdx31307	KA timeout does not trigger callback to cops client
CSCdw50718	SNMP - snmp-set smonVlanIdStatsTable elem causes crash
CSCdx00185	CM may get IP address for PC
CSCdx57717	pppoe failed with Bundling Cable Interfaces
CSCdx57217	Error in remapping sid after HCCP revert
CSCdx63414	Protect Line Card Crash during N+1 Swith over
CSCdx46444	automore broken when doing show cable modem remote-query
CSCdx74408	get perform snmp query using hidden community string cable-docsis
CSCdx73117	PRE Crash during N+1 switchover
CSCdx67901	cdxIfUpChannelInputPowerLevel always returns zero as a value
CSCdx69628	With Bundling, CMTS proxy the arp for CPEs on same CM
CSCdx81007	sho cable modem registered - CLI output shows wrong CPE information
CSCdx78866	Line Card Trace backs lead to keepalive failures
CSCdx77075	CMTS got hanged after issued sho run int Cx/y with OIR operation
CSCdx82328	Alternating ping fail failure after Worker LC is reset
CSCdx37675	Many important events do not generate syslog or SNMP trap message
CSCdx92261	access-group out command on sub interfaces not synced to Protect
CSCdx89411	Traceback at cmts_dhcp_inq_reply, cmts_dhcp_glean
CSCdx94008	ACL on per-modem or per-host basis broken
CSCdx58560	Display slave vcci info for bundled subints in sh hard pxf cpu sub
CSCdy02319	%ERR-1-FPGA: FP FPGA bad access Error message on PRE
CSCdy06163	PRE Crash After N+1 Switch Over
CSCdy08691	DSP timeout & Acterna stop running when change mod. profile in CLI
CSCdy06170	Traceback & Alignment errors

Open Caveats for Release 12.2(8)BC1

All the caveats listed in Table 52 are open in Cisco IOS Release 12.2(8)BC1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 52 Open Caveats for Cisco IOS Release 1.2.2(8)BC1

Caveat ID Number	Description
CSCdx57696	Traceback & Crash Observed
CSCdx57717	pppoe failed with Bundling Cable Interfaces
CSCdx58924	Dynamic modulation profile switchover does not work correctly
CSCdx58979	SNR was not displayed in show cable modem verbose output
CSCdx61268	CM status does not change, it looks always online

Closed and Resolved Caveats for Release 12.2(8)BC1

All the caveats listed in Table 53 are resolved in Cisco IOS Release 12.2(8)BC1. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 53 Closed and Resolved Caveats for Cisco IOS Release 12.2(8)BC1

Caveat ID Number	Description
CSCdx16713	Erroneous upstream IP packet causes buffer inconsistency

Open Caveats for Release 12.2(4)BC1b

All the caveats listed in Table 54 are open in Cisco IOS Release 12.2(4)BC1b. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 54 Open Caveats for Release 12.2(4)BC1b

Caveat ID Number	Description
CSCdw69389	Crash at cmts_ds_trafshap_out, cal_queue_dequeue, cmts_ds_pak_handle

Closed and Resolved Caveats for Release 12.2(4)BC1b

All the caveats listed in Table 55 are resolved in Cisco IOS Release 12.2(4)BC1b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 55 Closed and Resolved Caveats for Release 12.2(4)BC1b

Caveat ID Number	Description
CSCdw59858	Timer Wheel Timer: crash occurred in tw_timer_replenish()
CSCdw77623	Client ip address and tty name not set in cmd author request to tac+

Table 55 Closed and Resolved Caveats for Release 12.2(4)BC1b (continued)

Caveat ID Number	Description
CSCdw78350	Spectrum-group configured gone after reload
CSCdw79462	CM did not become online in init(o) state w/bundling

Open Caveats for Release 12.2(4)BC1a

There are no open caveats specific to Cisco IOS Release 12.2(4)BC1a that require documentation in the release notes.

Closed and Resolved Caveats for Release 12.2(4)BC1a

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(4)BC1a. Table 56 describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 56 shows the severity 1 and severity 2 caveats that exist for Cisco IOS Release 12.2(4)BC1.

Table 56 Closed and Resolved Caveats for Release 12.2(4)BC1a

Caveat ID Number	Description
CSCdw65903	An error can occur with management protocol processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats for Release 12.2(4)BC1

Table 57 shows the severity 1 and severity 2 caveats that exist for Cisco IOS Release 12.2(4)BC1.

Table 57 Open Caveats for Release 12.2(4)BC1

Caveat ID Number	Description
CSCdu81936	Received gratuitous ARP overwrites the interface's MAC address in the router's ARP table (see http://www.cisco.com/warp/public/707/IOS-arp-overwrite-vuln-pub.shtml for complete details)

Closed and Resolved Caveats for Release 12.2(4)BC1

Cisco IOS Release 12.2(4)BC1 is the first release in the 12.2 BC train for the Cisco uBR7100 series routers but Table 58 shows the closed or resolved caveats that existed in previous releases that are also resolved in this release.

Table 58 Closed and Resolved Caveats for Release 12.2(4)BC1

Caveat ID Number	Description
CSCdu26491	Multicast packets are not forwarded on cable bundle slave interfaces
CSCdu59266	CPEs in the same IP subnet can not communicate due to proxy ARP problem
CSCdu64806	CMTS can crash when giving the **no cable monitor** command.
CSCdu66833	Slave interface in cable bundle is shut down on reload
CSCdu79200	UBR crashes with Bus Error at PC 0x6033FE48
CSCdu85209	Customer spoofing CMTS gateway address
CSCdv15300	DHCP refresh on UBR7200 doesn't refresh CEF Adjacency
CSCdv46107	Incorrect radius accounting records for PPPoE connection
CSCdv54518	Fast switching onto PPPoE sessions over cable interface is broken
CSCdv69507	The **dhcp** option is missing from the **cable source-verify** command.
CSCdv71609	Traceback with %ALIGN-3-SPURIOUS during configuration
CSCdv78225	SNR formula is incorrect
CSCdv85525	Enabling PIM sparse-mode multicast brings all cable modems offline
CSCdv86213	CMTS with clockcard boot crash in add physical entity entry
CSCdv90735	The CEF adjacency table is not updated
CSCdw03863	Crash with watchdog timeout in IGMP Input process

Open Caveats for Release 12.2(4)XF1

No severity 1 or severity 2 caveats exist for Cisco IOS Release 12.2(4)XF1 for the Cisco uBR7100 series routers.

Closed and Resolved Caveats for Release 12.2(4)XF1

Cisco IOS Release 12.2(4)XF1 was the first release in the 12.2 XF train for the Cisco uBR7100 series routers, but Table 59 shows the closed or resolved caveats that existed in previous releases that are also resolved in this release.

Table 59 Closed and Resolved Caveats for Release 12.2(4)XF1

Caveat ID Number	Description
CSCdw03863	Crash with watchdog timeout in IGMP Input process

Related Documentation

The following sections describe the documentation available for the Cisco uBR7100 series. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 T and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2 T**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2 T**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in "Caveats" in these release notes, see *Caveats for Cisco IOS Release 12.2 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 T.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2 T**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2 T**: **Caveats**

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

The following documents are available for the Cisco uBR7100 series universal broadband routers on Cisco.com and the Documentation CD-ROM:

- *Cisco uBR7100 Series Hardware Installation Guide*
- *Cisco uBR7100 Series Software Configuration Guide*
- *Cisco uBR7100 Series Power Supply Installation*
- *Broadband Cable Command Reference Guide*
- *Cisco CMTS Feature Guide*

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Documentation Home Page: Broadband Access: Cable:
Cisco uBR7100 Series Universal Broadband Routers

Note The *Broadband Command Consolidation* is available on Cisco.com through the following path: **Technical Documents: Documentation Home Page: Broadband/Cable Solutions**

On the Documentation CD-ROM:

Cisco Product Documentation: Broadband Access: Cable: **Cisco uBR7100 Series Universal Broadband Routers**

Note The *Broadband Command Consolidation* is available on the Documentation CD-ROM through the following path: **Cisco Product Documentation: Broadband/Cable Solutions**

Tips Information about features of the Cisco uBR7100 series universal broadband router, as well as software release notes, are available on Cisco.com at:
http://www.cisco.com/univercd/cc/td/doc/product/cable/index.htm

Feature Modules

Feature modules describe new software enhancements, committed as features, supported by Cisco IOS Release 12.2(15)BC2i, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, and configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature-module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2 T**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2 T**: **New Feature Documentation**

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/cgi-bin/Support/FeatureNav/FN.pl

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM:

Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Release 12.2 Documentation Set

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the paper documents were printed.

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can email your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.